

# Chapter 16

## Data breach notification

- 16.1 This chapter discusses the practice of data breach<sup>1434</sup> notification and the merits of introducing a mandatory data breach notification requirement into the Privacy Act.
- 16.2 The chapter begins by explaining the meaning of a data breach and explaining the practice of breach notification. It then outlines the current legal framework and reform proposals in New Zealand and in other common law jurisdictions. The chapter closes by explaining, in more detail, the aspects that make up a data breach notification scheme, and poses a number of policy questions that we seek responses to.
- 16.3 Currently, the holders of personal information, both public and private sector agencies, are under no legal obligation to notify individuals or the Office of the Privacy Commissioner when individuals' personal information is compromised, notwithstanding that notification is said to provide individuals the opportunity to minimise the negative consequences that can come from a data breach, such as identity theft or fraud or discriminatory treatment. The fact that notification does not always occur is not surprising given the lack of incentives for companies to notify affected individuals including the potential costs to its financial bottom line and reputation.
- 16.4 The security of an individual's personal information is becoming increasingly important as more and more information of a sensitive or private nature is being collected and retained by both public and private sector agencies. Given the mass of information that is now being collected and held by organisations, it is inevitable that at certain times private information of individuals will be accessed, found, or otherwise inappropriately acquired. The question is what, if anything, agencies should be required to do in such cases.

---

<sup>1434</sup> We use the terms “data breach” throughout this chapter as it is often colloquially associated with the topic in mass media and much of the literature we have reviewed. Other references include “security breach”, “information security breach”, “data security breach”, and “privacy breach” (the last being the term used by the New Zealand Office of the Privacy Commissioner).

WHAT IS  
DATA BREACH  
NOTIFICATION?

- 16.5 Simply put, a data breach is the “unauthorised access to or collection, use or disclosure of, personal information.”<sup>1435</sup> Breach notification “is the practice of notifying affected individuals when their personal information has become available to unauthorised individuals or organisations.”<sup>1436</sup>
- 16.6 Data breaches take on a multitude of forms ranging from the innocent loss of a file to a more egregious act aimed at damaging another individual. Some involve individuals’ intentional acts to usurp the personal details of others, whereas others may be more innocent and involve nothing more than an employee mistakenly accessing personal information on a company’s shared computer work space. Data breaches can involve loss or theft of personal information or equipment on which personal information is stored (including CDs, USB keys, and other portable storage devices), inappropriate access controls allowing unauthorised use, equipment failure, human error, unforeseen circumstances such as a fire or flood, a hacking attack, or through “blagging” offences where personal information is obtained by deceiving the organisation which holds it.<sup>1437</sup>
- 16.7 Data breach notification laws are a ubiquitous feature of the US privacy law landscape. They were pioneered in California in 2003<sup>1438</sup> and exist in approximately 45 other States and the District of Columbia.<sup>1439</sup> Many US laws only relate to the private sector. Moreover, they exist without the support of broad-based privacy laws such as New Zealand’s Privacy Act. Voluntary notification guidelines exist in many countries, which apply in some cases to both public and private sector agencies, and require notification in a range of situations. Voluntary guidelines exist in Australia,<sup>1440</sup> Canada,<sup>1441</sup> New Zealand,<sup>1442</sup> and in the United Kingdom.<sup>1443</sup>
- 16.8 Amongst the US laws and various guidelines, distinctions exist particularly in regard to:<sup>1444</sup>
- who is covered (for example, whether they apply to both the public and private sectors);

1435 Office of the Privacy Commissioner *Information Paper to accompany Privacy Breach Guidance Material* (Wellington, February 2008) 1.

1436 Office of the Privacy Commissioner *Information Paper to accompany Privacy Breach Guidance Material* (Wellington, February 2008) 1.

1437 Information Commissioner’s Office *Guidance on Data Security Breach Management* (London, March 2008) 1.

1438 California Civil Code § 1798.29.

1439 [www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws](http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws) (accessed 9 November 2009).

1440 Office of the Privacy Commissioner (Cth) *Guide to Handling Personal Information Security Breaches* (Sydney, August 2008).

1441 Office of the Privacy Commissioner of Canada *Key Steps in Responding to Privacy Breaches* (Ottawa, 2007).

1442 Office of the Privacy Commissioner *Key Steps for Agencies in Responding to Privacy Breaches and Privacy Breach Checklist* (Wellington, February 2008).

1443 Information Commissioner’s Office *Guidance on Data Security Breach Management* (London, March 2008).

1444 Fred Cate “Information Security Breaches – Looking Back and Thinking Ahead” (The Centre for Information Policy Leadership, 2008) 4.

- what types of information are covered (for example, whether medical information is included and whether it includes combinations of information);
- the circumstances that must exist to “trigger” notification (for example, acquisition of personal information or acquisition and a serious risk of harm to an individual);
- the timing, content, and method of notification;
- any other parties that need to be notified, such as relevant regulators including Privacy Commissioners;
- whether data encryption will be an exemption to the requirement to notify;
- the penalties for non-compliance; and
- whether or not a civil cause of action is available against agencies that fail to notify.

We discuss some of these aspects of breach notification laws in more detail below.

#### DATA BREACH CASES

- 16.9 The number of data breaches that occur in New Zealand each year is difficult to gauge. While breaches are reported from time to time in the media, and the Privacy Commissioner has reported to us that notifications are received in her office, there are no accurate data available. Overseas experience in comparable jurisdictions would suggest that data breaches occur regularly (whether or not all are detected).
- 16.10 In New Zealand recent high profile data breach examples include the Treasury losing a CD in the post that contained the personal and company tax details of numerous individuals;<sup>1445</sup> the mobile phone network provider 2degrees’ website suffering teething problems making it possible to see the personal details of previous visitors to its site;<sup>1446</sup> and Massey University’s intranet suffering a fault in its security system thereby potentially exposing the sensitive information of students to anyone who accessed the site.<sup>1447</sup> Instances of police officers inappropriately accessing the national intelligence computer have also been recorded.<sup>1448</sup>
- 16.11 Numerous large scale data breaches have been recorded overseas, most notably in the United Kingdom and the United States. High profile cases in the United Kingdom include Her Majesty’s Revenue and Custom Service losing two CDs containing 25 million records containing financial and other details of people in receipt of child benefits (including names, addresses, dates of birth, and national insurance numbers).<sup>1449</sup> Another case involved the United Kingdom Ministry of Defence losing a laptop computer containing the sensitive personal details of 600,000 recruits or potential recruits.<sup>1450</sup> It was also found that the CD contained the further personal

1445 “Treasury Loses CD with Tax Information” (20 September 2009) [www.tvnz.co.nz](http://www.tvnz.co.nz) (accessed 18 February 2010).

1446 “Security Flaw Hits 2degrees Website” (5 August 2009) [www.stuff.co.nz](http://www.stuff.co.nz) (accessed 18 February 2010).

1447 Albany Students’ Association “Massey Uni Experiences Serious Breach of Security” (1 April 2009) Press release, available at [www.scoop.co.nz](http://www.scoop.co.nz) (accessed 18 February 2010).

1448 Ian Steward “Police Computer Violations Exposed” (7 December 2009) *The Press* Christchurch [www.stuff.co.nz](http://www.stuff.co.nz) (accessed 18 February 2010).

1449 Richard Thomas and Mark Walport *Data Sharing Review Report* (London, July 2008) 9.

1450 UK Information Commissioner *Enforcement Notice to Secretary of State Defence* (14 July 2008) 1.

information of up to another 400,000 individuals, totalling approximately 1,000,000 people.<sup>1451</sup> Similar large data breach incidents occur in the US. Daily, stories of large data breaches appear on the internet and in other media.<sup>1452</sup>

## THE CASE FOR DATA BREACH NOTIFICATION

- 16.12 In this part of the chapter we lay out some of the justifications given to support the need for breach notification, as well as some of the criticisms that have been made in response.

### Common rationales

#### *Identity theft and identity fraud*

- 16.13 Data breaches can involve all types of information, from the benign to the particularly sensitive. Some information is inherently sensitive and its loss can be costly and devastating to the individuals concerned. Other information may be relatively insignificant on its own, but can become more sensitive when viewed in combination with other information. Certain types of information may, if found in the wrong hands, put other people in danger of harm, including physical, financial, and reputational harm.<sup>1453</sup> The loss of medical records containing personal medical history could lead to discriminatory treatment or ostracism. Exposing an individual's physical address may expose them to threats of physical harm or threats to their personal privacy. The loss of bank account details could result in financial harm including fraud and identity theft.
- 16.14 The link between breaches of personal data and identity fraud and identity theft has been the primary justification submitted in the US in support of notification laws. Given the vast range of highly personal information that is now being collected and held by both public and private sector agencies, the possibility of that data being breached, and subsequently being used in identity fraud is said to be growing.<sup>1454</sup> Identity crime in the New Zealand context is discussed in chapter 17.
- 16.15 Notification is said to be necessary and justified as it enables the individuals whose information has been compromised to take steps to mitigate and control the negative effects that can result from a breach. This could involve changing bank account numbers and passwords, monitoring credit reports and bank account transactions, or taking steps to retrieve the information that was lost. Notification of a data breach is said to be particularly necessary given that an individual is usually unaware of its occurrence, unlike the case of car theft for example, where the owner is usually immediately aware that their vehicle is missing. Notifying an individual in cases where an agency knows or suspects information has been compromised would partially overcome this problem.

1451 UK Information Commissioner *Enforcement Notice to Secretary of State Defence* (14 July 2008) 2.

1452 See for example two databases containing lists of data breaches and the number of customers affected in each case at [www.datalossdb.org](http://www.datalossdb.org) (accessed 27 October 2009) and [www.privacyrights.org/ar/ChronDataBreaches.htm](http://www.privacyrights.org/ar/ChronDataBreaches.htm) (accessed 27 October 2009).

1453 Uniform Law Conference of Canada *Report of the Joint Criminal/Civil Section Working Group on Identity Theft: A discussion Paper* (Charlottetown, 2007) 14.

1454 However some challenge this premise. See, for example, Fred Cate "Information Security Breaches – Looking Back and Thinking Ahead" (The Centre for Information Policy Leadership, 2008) 4.

*Reducing other harms*

- 16.16 While the risk of identity theft and identity fraud have been the primary justifications for mandatory breach laws in the US, those outside of the US tend to focus on the full range of harms in their justifications. These include stalking, embarrassment, ostracism, or discrimination that could result from the release or loss of information held by an organisation. Notification enables individuals to take steps to mitigate these harms.

*The “right to know”*

- 16.17 As well as providing practical benefits to individuals affected by data breaches, a requirement to notify can also be justified as a matter of principle on the basis of a “right to know.”<sup>1455</sup> This principle dictates that individuals are owed a moral obligation from any agency that is collecting, storing, or using those individuals information, to be informed if it is compromised in any way. Simply put “individuals whose personal information has been exposed to potential unauthorized use as a result of a security breach deserve to be notified”.<sup>1456</sup>
- 16.18 If an organisation is benefiting from or required to use the personal information of an individual it is right for society to expect that that information is reasonably protected and to expect to be notified when that information is compromised. In relation to private organisations which benefit from the personal data of individuals it is right to expect that they are prepared to let individuals know when their information is compromised. In relation to agencies of the state, the argument is stronger given the particularly sensitive information the state holds about individuals that they are at times required by law to provide. Proper information handling practices in both the public and private sector should be encouraged.
- 16.19 A further aspect of the “right to know” is the notion that individuals should not be the “last to know” about a data breach involving their personal information, for example by reading of the breach in the newspaper. Prompt notification enables potentially embarrassing or damaging consequences to be mitigated through early response action taken by the individual concerned.

*Policy development, research, and sector oversight*

- 16.20 As well as benefiting affected individuals, it has also been said that breach notification can “enable law enforcement, researchers, and policy makers to better understand which firms and sectors are best (or worst) at protecting consumer and employee data.”<sup>1457</sup> In this regard notification assists in understanding the privacy and security environment and aids the development of policy in this area.

1455 Sasha Romanosky, Rahul Telang, Alessandro Acquisti “Do Data Breach Disclosure Laws Reduce Identity Theft?” (Carnegie Mellon University, 2008) 2.

1456 Canadian Internet Policy and Public Interest Clinic “Approaches to Security Breach Notification: A White Paper” (University of Ottawa, 2007) 22.

1457 Sasha Romanosky, Rahul Telang, Alessandro Acquisti “Do Data Breach Disclosure Laws Reduce Identity Theft?” (Carnegie Mellon University, 2008) 2.

This would be so particularly if the Privacy Commissioner had a function of publicly notifying breaches (even in an anonymised form) as it would alert everyone to the size of the problem.

## Data breach law criticisms

### *Ineffectiveness of data breach laws*

- 16.21 While supporters of mandatory data breach notification rely on the preceding justifications to argue that data breach laws are necessary, some criticise the laws as an inappropriate response to the problem of data breaches and identity theft.
- 16.22 There is little evidence to date that mandatory breach notification laws have led to a reduction of data breach incidents.<sup>1458</sup> This could suggest that mandatory breach notification laws are an ineffective way to encourage agencies to adequately protect information, or may otherwise be due to the relative youth of mandatory breach laws worldwide.
- 16.23 In the case of identity theft, one of the few studies conducted on the link between data breach notification laws and identity theft concluded that the effect of these laws on the reduction of identity theft was marginal.<sup>1459</sup> The authors compared the extent of identity fraud in US States that have data breach notification laws with those that do not. They concluded that “we find that the adoption of data breach disclosure laws have marginal effect on the incidences of identity thefts and reduce the rate by just under 2 per cent on average.”<sup>1460</sup> This is important to note as it brings in to question the justification for breach laws based on the perceived link between data breaches and identity theft and fraud.

### *Outmoded response*

- 16.24 A possible reason for the marginal effect on identity theft or the lack of effect in reducing breach incidents can be found in the criticisms of data breach laws by Fred H Cate. In his work on data breach laws, he criticises the approach being taken to protect data breaches and identity theft as a “twentieth century approach to twenty first century information flows and challenges.”<sup>1461</sup> Largely in response to the US data breach laws, he questions whether or not data breach notifications are really an appropriate response given the ubiquitous use and exchange of digital data that occurs in the world today. He considers that notifications

---

1458 Canadian Internet Policy and Public Interest Clinic “Approaches to Security Breach Notification: A White Paper” (University of Ottawa, 2007) 22.

1459 Sasha Romanosky, Rahul Telang, Alessandro Acquisti “Do Data Breach Disclosure Laws Reduce Identity Theft?” (Carnegie Mellon University, 2008) 11.

1460 Sasha Romanosky, Rahul Telang, Alessandro Acquisti “Do Data Breach Disclosure Laws Reduce Identity Theft?” (Carnegie Mellon University, 2008) 16.

1461 Fred Cate “Information Security Breaches – Looking Back and Thinking Ahead” (The Centre for Information Policy Leadership, 2008) 19.

were designed for a time when “data processing was infrequent, highly centralised, and clearly structured.”<sup>1462</sup> Now, in relation to this “bottomless ocean of information” he states that:<sup>1463</sup>

notices are too slow, too cumbersome, and too poorly timed to provide meaningful protection for information security, and requiring them as a broad response to security threats promises to inundate individuals with notices they are ill-equipped and unlikely to act on.

- 16.25 Cate does note that a number of proposals, including the New Zealand guidelines, “reflect many of the practical lessons from the broad and diverse U.S. experiences about the advantages and limits of notice”<sup>1464</sup> and avoid many of the criticisms he poses (which are directed particularly at the EU and US approaches). However, his general point cannot be entirely dismissed.

### *Unnecessary burdens*

- 16.26 Some critics of data breach laws have suggested that they are costly and constitute a regulatory burden on organisations with little concomitant benefit to consumers. It is also said that these laws can be costly and time consuming for individuals who receive data breach notifications and may take unnecessary and often inappropriate responses.<sup>1465</sup> Some figures quoted suggest that the probability of a single data breach being misused is very small, bringing into question the need to notify in many cases.<sup>1466</sup>

## NEW ZEALAND Legal requirements

- 16.27 Neither the Privacy Act, the Privacy Principles, nor any of the codes require mandatory breach notification. This means that agencies are not required to notify individuals whose personal information has been compromised, no matter how sensitive the information, and no matter how serious the risk of harm that could be suffered as a result.
- 16.28 The Privacy Commissioner has made clear however that failure to notify affected individuals could be a factor that is taken into account if a complaint is received concerning a breach of principle 5.<sup>1467</sup> Principle 5 requires holders of personal information protect information by such security safeguards as it is reasonable in the circumstances to take. If an individual was to become aware that their

<sup>1462</sup> Fred Cate “Information Security Breaches – Looking Back and Thinking Ahead” (The Centre for Information Policy Leadership, 2008) 19.

<sup>1463</sup> Fred Cate “Information Security Breaches – Looking Back and Thinking Ahead” (The Centre for Information Policy Leadership, 2008) 2.

<sup>1464</sup> Fred Cate “Information Security Breaches – Looking Back and Thinking Ahead” (The Centre for Information Policy Leadership, 2008) 1.

<sup>1465</sup> Canadian Internet Policy and Public Interest Clinic “Approaches to Security Breach Notification: A White Paper” (University of Ottawa, 2007) 22.

<sup>1466</sup> Canadian Internet Policy and Public Interest Clinic “Approaches to Security Breach Notification: A White Paper” (University of Ottawa, 2007) 22.

<sup>1467</sup> *4<sup>th</sup> Supplement to Necessary and Desirable*, recommendation 23A, para 2.5.

own personal information had been compromised and make a complaint, the Privacy Commissioner may take a failure to notify that individual into account in considering whether the organisation involved took all reasonable steps.<sup>1468</sup>

### The guidelines

- 16.29 In August 2007, the Office of the Privacy Commissioner issued voluntary data breach guidelines – *Key Steps for Agencies in Responding to Privacy Breaches and Privacy Breach Checklist* (“the guidelines”) – for consultation. The guidelines were finalised and released in February 2008.<sup>1469</sup>
- 16.30 The guidelines state that a privacy breach is “the result of the unauthorised access to or collection, use or disclosure of, personal information.” “Unauthorised access” is access that contravenes the terms of the Privacy Act.<sup>1470</sup> The guidelines are separated into four steps:
- breach containment and preliminary assessment;
  - evaluation of the risks associated with the breach;
  - notification; and
  - prevention.
- 16.31 As the list above illustrates, these guidelines go further than requiring notification as a response, making them more comprehensive than various US State requirements. The guidelines present a proactive approach and stress that breach prevention and data security is the most effective means of protecting the privacy of individuals. Notification is one aspect of a wider set of recommendations aimed at the protection and security of personal information.
- 16.32 The guidelines do not require notification in all cases, and outline a series of “threshold” questions that must be considered before recommending that affected individuals be notified. Matters that should be taken into account include the nature of the information that has been breached, particularly the level of sensitivity of that information, its context, whether or not the information is encrypted, anonymised, or otherwise inaccessible, and how the information can be used and whether this includes fraudulent or harmful purposes. As well as this, an organisation should consider who is affected by the breach, and finally, assess whether harm could foreseeably result, either to an individual, the organisation in question, or the public. Importantly, the guidelines note that the “key consideration in deciding whether to notify affected individuals should be whether notification is necessary in order to avoid or mitigate harm to an

---

1468 See for example Case Note 211257 [2009] NZPrivCmr 16 – concerning complaints lodged with the Privacy Commissioner after a member of a government agency lost a file on the street containing a list that included personal information about a large group of people. In this case, the Privacy Commissioner found that while there was a breach of principle 5, there was no interference with privacy because the individuals involved suffered no harm. In the case the agency took steps to mitigate any harm that could have resulted from the breach, by expediently notifying the affected individuals and the Privacy Commissioner's Office, seeking and receiving legal undertakings from media outlets who obtained the files not to publish their details and getting the original file back with the help of the police.

1469 Office of the Privacy Commissioner *Key Steps for Agencies in Responding to Privacy Breaches and Privacy Breach Checklist* (Wellington, February 2008).

1470 Office of the Privacy Commissioner *Key Steps for Agencies in Responding to Privacy Breaches and Privacy Breach Checklist* (Wellington, February 2008) 1.

individual whose personal information has been inappropriately accessed, collected, used or disclosed.”<sup>1471</sup> More detailed comments about the guidelines are included later in the chapter where appropriate.

- 16.33 The guidelines are relatively new and it is not yet possible to tell what effect they are having on data protection practices in either the public or private sector (if any). It may be that mandatory notification laws should only be considered an option after there has been a proper opportunity to assess the effectiveness of the voluntary guidelines.

#### OTHER JURISDICTIONS

- 16.34 Mandatory notification laws exist in nearly every US State,<sup>1472</sup> and almost 30 of these are based on the original Californian model.<sup>1473</sup> Various attempts to enact a federal breach notification law have, to date, been unsuccessful. Financial institutions throughout the US are subject to mandatory notification obligations under the *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice* issued by the Department of the Treasury.<sup>1474</sup>
- 16.35 The EU has recently amended its e-data Directive covering its telecoms sector (including phone, email, SMS, and internet use) to include a mandatory notification requirement.<sup>1475</sup> Calls to require mandatory notification across all sectors were not followed, but the European Commission has stated publicly that it will consider this in the future.<sup>1476</sup> An all-sector mandatory notification law has also recently been enacted in Germany.<sup>1477</sup>
- 16.36 No mandatory breach notification laws exist in Australia at either a federal or a state level but the Australian Law Reform Commission (ALRC) recently recommended that “the Privacy Act should be amended to include a new Part on data breach notification.”<sup>1478</sup> This recommendation was supported by the Australian Office of the Privacy Commissioner.<sup>1479</sup> The Australian Government is yet to respond to this aspect of ALRC’s report.<sup>1480</sup>

1471 Office of the Privacy Commissioner *Key Steps for Agencies in Responding to Privacy Breaches and Privacy Breach Checklist* (Wellington, February 2008) 6.

1472 Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) para 51.14.

1473 [www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws](http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws) (accessed 9 November 2009).

1474 Department of the Treasury (US) *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice* (2005).

1475 EC Directive 2009/136/EC.

1476 Viviane Reding, Member of the European Commission Responsible for Information Society and Media “Securing Personal Data and Fighting Data Breaches” (Speech to EDPS-ENISA Seminar, Brussels, 23 October 2009).

1477 Bundesdatenschutzgesetz [Federal Data Protection Act], 20 December 1990, BGBl. I at 2954, as amended. The German law requires that affected individuals must be notified of any unlawful or unauthorised access of personal information if the incident threatens significant harm to the individual.

1478 Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) para 51.73.

1479 Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) para 51.51.

1480 However it has signalled that it will respond in due course. See Australian Government *First Stage Response to the Australian Law Reform Commission Report 108 – Australian Law Reform Commission For Your Information: Australian Privacy Laws and Practice* (October 2009).

- 16.37 No mandatory breach notification laws exist in the United Kingdom where mandatory breach laws were rejected by the authors of the *Data Sharing Review Report*<sup>1481</sup> and the UK Government.<sup>1482</sup>
- 16.38 No mandatory breach law exists in Canada (with the exception of Ontario<sup>1483</sup>), but the House of Commons Standing Committee on Access to Information, Privacy and Ethics has recommended that a mandatory notification regime be added to Canada's Personal Information Protection and Electronic Documents Act 2000 (PIPEDA).<sup>1484</sup> This recommendation was supported by the Canadian Government<sup>1485</sup> and Privacy Commissioner.<sup>1486</sup> Two sets of voluntary breach notification guidelines exist in Canada at the Federal level. One set is issued by the Treasury Board of Canada and applies to the Privacy Act 1985 and the other is issued by the Canadian Privacy Commissioner<sup>1487</sup> and applies to PIPEDA.<sup>1488</sup> The New Zealand guidelines are explicitly based on the guidelines issued by the Privacy Commissioner of Canada.

## OPTIONS FOR REFORM

### Our view

- 16.39 The Law Commission currently hold no firm view as to the need for mandatory breach notification but are interested in your views. We have laid out a series of questions below that would be helpful if the decision is taken to recommend that mandatory breach notification requirements should be enacted in New Zealand law.

### Mandatory vs voluntary notification

- 16.40 Earlier in the chapter we outlined some of the commonly stated justifications for notifying individuals. Here we briefly outline the case for and against a *mandatory* notification regime.
- 16.41 If matters are left to voluntary notification, there are incentives not to notify. Notifying individuals in response to a data breach is likely to involve costs for organisations, both in terms of the actual costs of making the notification and costs to its reputation, as well as potential penalties from regulators and the possibility of costly civil claims brought against the organisation by affected individuals.<sup>1489</sup>

1481 The *Data Sharing Review Report* was commissioned by the UK Government to undertake a review of the framework for the use of personal information in both the public and private sectors. See Richard Thomas and Mark Walport *Data Sharing Review Report* (London, July 2008) recommendation 11.

1482 Ministry of Justice (UK) *Response to the Data Sharing Review Report* (London, November 2008) 11.

1483 In Ontario mandatory notification is required in relation to health records under the Personal Health Information Act 2004 (Ontario), s 12.

1484 House of Commons Standing Committee on Access to Information, Privacy and Ethics (Can) *Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics – Statutory Review of the Personal Information Protection and Electronic Documents Act* (Ottawa, May 2007). See recommendations 23–25.

1485 Industry Canada *Government Response to the Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics – Statutory Review of the Personal Information Protection and Electronic Documents Act* (Ottawa, October 2007) 10.

1486 Jennifer Stoddart, Privacy Commissioner of Canada, to Richard Simpson, Industry Canada “Letter in response to Industry Canada’s consultation regarding the review of the *Personal Information Protection and Electronic Documents Act* (PIPEDA)” (15 January 2008) Letter.

1487 Office of the Privacy Commissioner of Canada *Key Steps in Responding to Privacy Breaches* (Ottawa, 2007).

1488 The Privacy Act in Canada (R.S., 1985, c. P-21) only applies to public sector agencies. PIPEDA covers private organisations and businesses.

1489 It would be possible to sue on the tort of breach of privacy provided there is a “highly offensive” publication.

There is certainly little incentive to notify in cases where a breach would otherwise remain unknown to the affected individuals or public at large.<sup>1490</sup> There might also be insurance consequences: for example, companies might be reluctant to notify for fear of it being perceived as an admission of liability, thereby prejudicing rights to claim from their insurers. Proponents of breach notification argue that a mandatory notification requirement, backed up by adequate sanctions, is required to compel organisations to notify affected individuals in the absence of market based incentives to do otherwise. It has been stated that:<sup>1491</sup>

A firm may not have an incentive to notify consumers of breaches when the cost of the notification exceeds the expected damage to the firm. That is, even if the costs of notifying a customer is smaller than the damage that will be mitigated, a firm has no incentive to bear this costs if the damage it will be spared is less than the costs of telling the customer... Second a firm may run the risk of damage as a result of notification.

Mandatory notification laws “level out the playing field” and make sure that considerations relating to insurance liability, and possible ramifications to a company’s bottom line, do not encourage behaviour contrary to the public interest.

- 16.42 Mandatory laws are also said to provide the market with information about an organisation’s information handling practices, making companies more transparent in the way they handle the information of customers and other individuals.<sup>1492</sup>
- 16.43 Such laws are also said to encourage firms to adopt and further secure safe document management practices, thereby “disinfecting”<sup>1493</sup> themselves of improper and unsafe security practices that are likely to result in personal information being compromised. Aside from a possible link between data breaches and data theft or fraud, it is not unreasonable to assume that mandatory laws provide some incentive for organisations to review their practices, given the negative publicity and consequences that can result after notifying about a breach. The negative publicity that can stem from data breaches is said to provide an incentive for organisations to encourage practices and processes that keep data secure. This point was central to the Australian Law Commission’s reasoning in recommending the mandatory breach notification laws be introduced into the Australian Federal Privacy Act.<sup>1494</sup>
- 16.44 These benefits must be seen against some of the criticisms that are voiced in relation to mandatory breach notification laws. These include:
- the nominal effect that breach notification has been alleged to have had on reducing identity fraud;

1490 Canadian Internet Policy and Public Interest Clinic “Approaches to Security Breach Notification: A White Paper” (University of Ottawa, 2007) 23.

1491 Michael Turner “Towards a Rational Personal Data Breach Notification Regime” (Information Policy Institute, 2006) 12.

1492 Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) para 51.81.

1493 The term disinfectant relates to one of the rationales cited in support of data breach laws, “sunlight as disinfectant”. See, for example, Sasha Romanosky, Rahul Telang, Alessandro Acquisti “Do Data Breach Disclosure Laws Reduce Identity Theft?” (Carnegie Mellon University, 2008) 2.

1494 Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) para 51.73.

- the fact that, at least where there is a low threshold for notification, mandatory notification can lead to breach fatigue whereby the effectiveness of notices lessens as individuals are inundated by breach notifications; and
- the regulatory burden for public and private sector organisations and added costs that could be involved.

Q170 Should the Privacy Act include a mandatory breach notification requirement, or is a voluntary notification model more appropriate?

## Substantive requirements

16.45 If a mandatory rules approach is adopted, developing the final notification package would need to involve consideration of the following factors.

### *Definition of data breach*

16.46 In each US State the data breach laws prescribe the types of information that must be compromised before the obligation to notify arises. Specific definitions are required in the majority of cases in the absence of any generally applicable privacy law. Some guidelines, including those issued by the Office of the Privacy Commissioner, rely on the definition of personal information (or its equivalent) that exists in the privacy laws that support the guideline. In the New Zealand case, the guidelines relate to “personal information” as defined in the Privacy Act.<sup>1495</sup>

16.47 A data breach (or privacy breach as it is synonymously called) is defined in the New Zealand guidelines as “the result of unauthorised access to, or collection, use or disclosure of, personal information.”<sup>1496</sup> Such activity is unauthorised if it occurs in contravention of the Privacy Act or its codes.<sup>1497</sup> This would include loss, theft, or mistaken disclosure.

16.48 The ALRC defined a data breach as a situation when specified personal information has been, or is reasonably believed to have been, acquired by an unauthorised person.<sup>1498</sup> The ALRC recommended the adoption of a definition of “specified personal information” built on the definitions of “personal information” and “sensitive information” included in the Australian Privacy Act.<sup>1499</sup> The report recommends that the Act should prescribe the combinations of information that will constitute ‘specified personal information’ for the purposes of the notification regime. The report lists examples including driver’s licence or proof of age; Medicare number or other unique identifier, such as tax file number; and sensitive information (as defined in the Australian Privacy Act). This combinational approach is also found in the California data breach

<sup>1495</sup> Privacy Act 1993, s 2.

<sup>1496</sup> Office of the Privacy Commissioner *Key Steps for Agencies in Responding to Privacy Breaches and Privacy Breach Checklist* (Wellington, February 2008) 1.

<sup>1497</sup> Office of the Privacy Commissioner *Key Steps for Agencies in Responding to Privacy Breaches and Privacy Breach Checklist* (Wellington, February 2008) 2.

<sup>1498</sup> Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) para 51.83.

<sup>1499</sup> Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) para 51.83.

law (and the many US laws based on it).<sup>1500</sup> The ALRC made clear that any definition needs to cover more than sensitive financial information on the basis that financial harm “is not the only consequence that can flow from an unauthorised acquisition of personal information. Discrimination, stalking, and other harmful consequences potentially could flow from a security breach.”<sup>1501</sup>

- 16.49 The Californian Statute defines personal information as “an individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: social security number, driver’s licence number..., account number, credit or debit card number in combination with any security code..., medical information, and health insurance information.”<sup>1502</sup> The definition excludes publicly available information that is lawfully made available to the general public from government records.<sup>1503</sup>

Q171 How should a data breach be defined? Should a data breach requirement be applicable to all types of personal information, or should a more purposive definition be developed for the purposes of the breach notification regime?

#### *Notification threshold*

- 16.50 One of the purposes of data breach notification is to give individuals an opportunity to mitigate any harm that could arise as a result of a data breach. The notification threshold that is set should balance the risks of breach-fatigue and undue stress to individuals with the benefit of giving individuals the opportunity to take steps when their personal information has been affected. Setting the threshold at a meaningful level can also avoid unnecessary stress and wasted time that an individual can expend as a consequence of a data breach notice. Setting the notification threshold at an appropriate level was “highlighted as the critical issue” for submitters to the ALRC’s review of privacy.<sup>1504</sup>
- 16.51 The Canadian Internet Policy and Public Interest Clinic (CIPPIC) stated that “the trigger for notification should be based on a an objective test applied by organizations and subject to review by the applicable Privacy Commissioner. The test should be designed to avoid notification obligations where the breach does not expose individuals to a real risk of identity theft, but to apply in all situations where such a risk is created.”<sup>1505</sup>

1500 California Civil Code § 1798.29 (e).

1501 Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) para 51.98.

1502 California Civil Code § 1798.29(e).

1503 California Civil Code § 1798.29(f).

1504 Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) para 51.48.

1505 Canadian Internet Policy and Public Interest Clinic “Approaches to Security Breach Notification: A White Paper” (University of Ottawa, 2007) 25.

- 16.52 In California, the obligation to notify affected individuals is triggered when unencrypted personal computerised information “was, or is reasonably believed to have been, acquired by an unauthorized person.”<sup>1506</sup> This is qualified in the case of good faith acquisitions made by employees in an organisation, provided that there is no further unauthorised disclosure.<sup>1507</sup> The standard required in California is known as the “acquisition standard” as no assessment needs to be made to consider whether there is any risk of the data being misused or compromised. The Californian standard sets the notification requirement threshold at a relatively low level. Even if an organisation believes that there is no risk at all to the individual concerned, it is still under an obligation to notify. It would for example, require notification in any case where an e-mail was sent to an unintended addressee, or where a USB key containing data was accidentally disposed of. It is also of note that the Californian threshold is technology-specific in that it only relates to personal information that is computerised.
- 16.53 The ALRC recommended that the threshold for its notification regime be a *real risk of serious harm*.<sup>1508</sup> This is higher than the acquisition standard and requires the risk of harm to the affected person or persons be considered in deciding whether or not a notification should be made. The ALRC note that setting the trigger threshold at such a level should reduce the risk of breach fatigue and “also should reduce the compliance burden on agencies and organisations.”<sup>1509</sup>
- 16.54 The New Zealand guidelines suggest that affected individuals be notified of ‘material breaches’ which requires considering whether harm could foreseeably result from the breach.<sup>1510</sup> In doing so, organisations are recommended to consider the sensitivity of the information, whether or not there is a risk that the information could be used in identity theft or fraud, and what harm (financial, physical, and personal/ reputational) could foreseeably result for the individual, the organisation and the public at large.<sup>1511</sup>
- 16.55 One model advanced by American commentators sets up a twin-track or split-threshold model where the level of risk of harm to the individual dictates who should be notified.<sup>1512</sup> Affected individuals will be notified only when there is a real risk that their personal information will be misused. In cases where there is a risk that information has been acquired, but nothing more, notification is only made to the regulatory body. This lower threshold would trigger the need to investigate further. The regulatory body will then audit the investigation

---

1506 California Civil Code § 1798.29 (a).

1507 California Civil Code § 1798.29(d).

1508 Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) para 51.83.

1509 Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) para 51.86.

1510 Office of the Privacy Commissioner *Key Steps for Agencies in Responding to Privacy Breaches and Privacy Breach Checklist* (Wellington, February 2008) 5.

1511 Office of the Privacy Commissioner *Key Steps for Agencies in Responding to Privacy Breaches and Privacy Breach Checklist* (Wellington, February 2008) 6.

1512 Paul M Schwartz and Edward J Janger “Notification of Data Security Breaches” (Online, 2007). Available online at [www.paulschwartz.net/pdf/datasec\\_schwartz-janger.pdf](http://www.paulschwartz.net/pdf/datasec_schwartz-janger.pdf) (accessed 14 January 2010).

by the individual organisation and could step in if it believes an organisation erroneously decided not to notify. A similar dual notification model is reflected in the recommendations made by the CIPPIC.<sup>1513</sup>

Q172 In what circumstances should organisations be required to notify individuals that their personal information has been compromised? Should the legislation list the factors to be taken into account in deciding whether to notify? If so, what factors should the legislation list? Should there be different thresholds for notification to the individual and notification to the regulator?

### *The decision-maker*

- 16.56 Both the model recommended by the ALRC<sup>1514</sup> and the New Zealand guidelines<sup>1515</sup> vest responsibility to decide whether a notification needs to be made with the organisation itself. This is also the case in all US States.<sup>1516</sup> Vesting the initial decision with the organisation enables it to develop its own standards and make judgements based on facts that it is most aware of. CIPPIC stated that the organisation itself should make the decision on the basis that it is in the best position to “calculate the associated risks of a breach of its information security”.<sup>1517</sup>
- 16.57 The ALRC recommended that the decision reached by the organisation should be subject to oversight by the Privacy Commissioner who should be notified of data breaches that meet the threshold.<sup>1518</sup> The ALRC recommended that the decision to notify should be made in consultation with the Privacy Commissioner, and that the Privacy Commissioner should have the ultimate power to compel an organisation to notify if he or she believed, contrary to the view of the organisation, that the serious harm threshold was met.<sup>1519</sup> Notifying the Office of the Privacy Commissioner may be beneficial for agencies in terms of gaining further guidance concerning the breach and advice to ensure better practices in the future.<sup>1520</sup>

1513 Canadian Internet Policy and Public Interest Clinic “Approaches to Security Breach Notification: A White Paper” (University of Ottawa, 2007) 26.

1514 Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) para 51.87.

1515 Office of the Privacy Commissioner *Key Steps for Agencies in Responding to Privacy Breaches and Privacy Breach Checklist* (Wellington, February 2008) 6.

1516 Canadian Internet Policy and Public Interest Clinic “Approaches to Security Breach Notification: A White Paper” (University of Ottawa, 2007) 17.

1517 Canadian Internet Policy and Public Interest Clinic “Approaches to Security Breach Notification: A White Paper” (University of Ottawa, 2007) 26.

1518 Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) para 51.83.

1519 Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) para 51.88.

1520 Office of the Privacy Commissioner *Key Steps for Agencies in Responding to Privacy Breaches and Privacy Breach Checklist* (Wellington, February 2008) 8.

- 16.58 In Canada, the House of Commons Standing Committee on Access to Information, Privacy and Ethics recommended that in the case of certain defined breaches of personal information, organisations should notify the Privacy Commissioner of the breach. The Committee recommended that upon being notified of a breach of personal information, the Privacy Commissioner must make a determination as to whether or not affected individuals and others should be notified, and if so in what manner.<sup>1521</sup> With this approach the decision to notify rests with the Privacy Commissioner. This recommendation was subsequently rejected.<sup>1522</sup>
- 16.59 Consideration should also be given to who should be required to notify in cases where data held by an affiliated third party, such as a contractor, is compromised. The Privacy Commissioner's guidelines suggest that it is usually appropriate for the organisation who has a direct link to the customer to notify but notes that there may be situations where it is a more appropriate task for the third party to do so.<sup>1523</sup>

Q173 Who should decide whether a notification must be made in response to a data breach?

Q174 Should the Privacy Commissioner have the power to compel an organisation to notify affected individuals?

### *Who to notify*

- 16.60 The New Zealand guidelines, the US data breach laws, and the recommendations made by the ALRC all mandate notifying individuals whose personal information is compromised. The benefits of notifying individuals in these cases have previously been canvassed in the chapter.
- 16.61 It is also timely to consider whether the Privacy Commissioner or other interested parties should be notified, and if so at what stage in the process. In relation to the Privacy Commissioner, this decision will need to be made in light of the response to the policy question above – that which asks who should make the decision to notify. If it is the Privacy Commissioner, then their office will necessarily be contacted in each case. However, even if the decision is to be made by the agency itself, there may still be some merit in advising the Privacy Commissioner in each case, both for the agency concerned (for example in terms of guidance) and for policy development in the area (including trying to understand the extent of the problem).

1521 House of Commons Standing Committee on Access to Information, Privacy and Ethics (Can) *Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics – Statutory Review of the Personal Information Protection and Electronic Documents Act* (Ottawa, May 2007) 45.

1522 This recommendation was subsequently rejected by the Canadian Government in its official response, on the basis that the organisation itself would be well positioned to understand and assess the risks involved with notification. See *Government Response to the Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics, Statutory Review of the Personal Information Protection and Electronic Documents Act (PIPEDA), Fourth Report* (Ottawa, October 2007).

1523 Office of the Privacy Commissioner *Key Steps for Agencies in Responding to Privacy Breaches and Privacy Breach Checklist* (Wellington, February 2008) 7.

- 16.62 It would also be possible to include a requirement that, in certain cases, agencies notify other interested parties. Such parties could include financial regulatory bodies, credit card companies, insurers, organisations on behalf of whom the information was held, or law enforcement agencies such as the police.
- 16.63 Notifying credit card companies could ensure action is taken to monitor accounts and be on notice of suspect behaviour. The benefits of notifying particular bodies would differ from case to case.

Q175 In the case of a data breach should the agency be required to notify the Privacy Commissioner's Office? If so, should this be in every case, or only when the "notification threshold" is met?

Q176 Should other agencies be notified? If so, in what circumstances?

## Process requirements

### *Timing*

- 16.64 In its white paper on data breach laws, CIPPIC suggests that:<sup>1524</sup>

Security breach notification should be undertaken as soon as possible and without unreasonable delay after the occurrence of the breach, except where a law enforcement agency has made a written request for a delay. Delays for law enforcement purposes should be specified periods of time, and for not longer than 60 days at a time.

- 16.65 The New Zealand guidelines suggest notification should occur as soon as reasonably possible following assessment and evaluation of the breach and includes a similar extension provision for law enforcement purposes.

Q177 At which point should notification be required?

Q178 Should delays in notifying be allowed for law enforcement or any other purposes?

### *Method of notification*

- 16.66 The CIPPIC paper recommends that notification should "generally be by regular mail, but electronic and substitute notice should be permitted when certain conditions are met."<sup>1525</sup>

1524 Canadian Internet Policy and Public Interest Clinic "Approaches to Security Breach Notification: A White Paper" (University of Ottawa, 2007) 18.

1525 Canadian Internet Policy and Public Interest Clinic "Approaches to Security Breach Notification: A White Paper" (University of Ottawa, 2007) 28.

16.67 The New Zealand guidelines are similar. Notification should be direct – by phone, letter, email or in person. Substituted notification is provided for in cases where an individual’s contact details are unknown, or where a particularly large number of individuals are affected and direct contact would result in further harm or is prohibitive in cost for the organisation. Multiple methods of notification are also included as an option.<sup>1526</sup> In California substituted service is allowed if the cost of notification would be over US\$250,000, or where the number of affected people exceeds 500,000.<sup>1527</sup>

Q179 Should the method of notification be prescribed, or stated in terms of the objective to be achieved?

### *Content of the notification*

16.68 For notifications to be meaningful, and provide individuals with the ability to reduce the adverse effects that can flow from data breaches, sufficient information for the individual to act upon must be included in the notification. The New Zealand guidelines suggest that the following be included:<sup>1528</sup>

- information about the incident and its timing in general terms;
- a description of the personal information involved in the breach;
- a general account of what the agency has done to control or reduce any harm;
- what the agency will do to assist individuals and what steps an individual can take to mitigate any harm, including directing individuals to further information;
- contact information of a person or department within the agency who can provide further information;
- sources of further information such as the Police, the Ministry of Consumer Affairs, or Netsafe;
- whether the organisation has notified the Office of the Privacy Commissioner; and
- the contact information of the Privacy Commissioner.

Q180 What information should have to be included in a breach notification?

### **Exceptions**

16.69 In some US States specific exceptions exist that remove the requirement to notify in a particular case, thereby recognising that in certain cases other rights trump the important right to know that information has been compromised. Some of these considerations could be dealt with as a factor to weigh up when considering the level of risk of harm to the individual (such as encryption). Alternatively, some interests (such as state security) may be absolute exceptions.

16.70 Specific exceptions are discussed below.

---

1526 Office of the Privacy Commissioner *Key Steps for Agencies in Responding to Privacy Breaches and Privacy Breach Checklist* (Wellington, February 2008) 7.

1527 California Civil Code § 1798. 29(g)(3).

1528 Office of the Privacy Commissioner *Key Steps for Agencies in Responding to Privacy Breaches and Privacy Breach Checklist* (Wellington, February 2008) 7.

### Encryption

- 16.71 Some US States treat the encryption of data as a specific exception from the obligation to notify on the basis that the likelihood of harm resulting from a breach involving encrypted data is small. Other models deal with encryption as part of the risk assessment exercise that is carried out when making a decision whether or not to notify. The ALRC took the latter approach.<sup>1529</sup>
- 16.72 The ALRC acknowledged that encryption should be a ground to excuse an organisation from the obligation to notify but noted that any encryption must be “adequate”. This recognises the different data encryption techniques that exist and the difficulty of comparing them. An assessment of whether or not encryption is “adequate” will depend on the particular facts of the case.<sup>1530</sup> The ALRC recommends that the Privacy Commissioner issue guidance as to what forms of encryption are “adequate” for the storage of personal information.

### Public interest exception

- 16.73 In response to the concerns of stakeholders to its review, the ALRC recommended that the Privacy Commissioner should have a broad discretion to waive the notification requirement when notification would not be in the public interest.<sup>1531</sup> This decision would lie with the Privacy Commissioner. This could apply in cases such as where the information involved concerns matters of national security.

### Other exceptions

- 16.74 Other express exceptions could be included in the breach notification regime to ensure that certain important interests are adequately protected.

Q181 What exceptions, if any, should be included in a data breach notification regime? In particular:

- Should encryption be an express exception or one of the matters to be included in the risk assessment exercise?
- Should public interest be included as a ground on which the Privacy Commissioner can waive an organisation’s obligation to notify, or are more narrowly-defined exceptions more appropriate?

### Failures to notify

- 16.75 Rules are generally meaningless without the availability of sanctions in cases where they are not followed. If a mandatory rule approach is adopted it is important to consider what sanctions are available in situations where an organisation fails to notify individuals affected by a data breach. An individual would have recourse through making a complaint to the Privacy Commissioner, either on the basis

<sup>1529</sup> Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) para 51.91.

<sup>1530</sup> Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) para 51.92.

<sup>1531</sup> Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) para 51.94.

of a new ground of complaint (a failure to notify) or under existing grounds such as a failure to take reasonable steps to protect personal information (under principle 5).

- 16.76 The complaint could be dealt with in accordance with the options we are proposing in chapter 8. If the Privacy Commissioner found that an agency was in breach of the terms of the Act, if the proposals are adopted, he or she would then have the ability to issue an enforcement notice. Essentially an enforcement notice is a notice to comply with the terms of the Privacy Act issued by the Privacy Commissioner that carries consequences for failing to comply.<sup>1532</sup>

Q182 Is the complaints process an adequate mechanism for dealing with an organisation's failure to notify in the case of a data breach, or are further sanctions necessary?

### Vehicle for a mandatory model

- 16.77 If a mandatory notification requirement is to be adopted, consideration needs to be given to how it would be introduced into the Privacy Act regime. Our tentative opinion is that if a notification requirement were to be mandated, it should be enacted as an aspect of one of the privacy principles, with corresponding detailed provisions inserted in a new part or sub-part later in the Act.
- 16.78 As noted above, in investigating a complaint concerning a breach of principle 5, the Privacy Commissioner currently takes into account the failure to notify individuals whose information has been compromised in appropriate cases. This must be because notification can be considered a security safeguard that agencies should use to protect the personal information that they hold. The Law Commission believes that it would be possible to add a new sub-paragraph (c) to principle 5 that contains the notification obligation. We also envisage that this could contain a cross-reference to sections or a part later in the Act, as is the case with Principle 6(3), and that those later sections or later part can include the more detailed requirements that collectively make up the notification scheme.
- 16.79 We also wish to point out that codes could be used to tailor aspects of technical reporting requirements or varying requirements to particular sectors or contexts. We have no view on the need for particular codes at this time but foresee codes as an appropriate means to tailor requirements where necessary.

Q183 Should it be decided that notification should be mandatory, do you agree that an amendment to principle 5, backed up by provisions later in the Act, is the best way to enact an obligation to notify? If not, how do you think the obligation should be enacted?

<sup>1532</sup> Enforcement notices are proposed and discussed in more detail in chapter 8.