CHAPTER 2

KEY ISSUES

2.1 Some submissions strongly supported the introduction of mandatory data breach notification provisions for Commonwealth government agencies and certain private sector organisations, including the Australian Law Reform Commission (ALRC) and the Office of the Australian Information Commissioner (OAIC).[1] Submissions also highlighted key concerns, including:

- meaning of the phrase 'real risk of serious harm' within the definition of 'serious data breach';
- application of the steps set out in the mandatory notification provisions; and
- inclusion and breadth of exceptions to the mandatory notification provisions.

'Real risk of serious harm'

2.2 Proposed new sections 26X-ZA of the *Privacy Act 1988* (Cth) (Privacy Act) establish the circumstances in which APP entities, credit reporting bodies, credit providers and file number recipients will have committed a 'serious data breach'. One of the conditions is that the breach will result in a real risk of serious harm to any of the individuals to whom the information relates.[2]

2.3 Some submissions questioned the meaning of the phrase 'real risk of serious harm' or its various elements (such as 'serious harm' and 'real risk'),[3] with submitters suggesting ways in which this ambiguity could be ameliorated or rectified.

2.4 The Australian Bankers' Association (ABA) submitted that the meaning of the criterion will be unclear in an entity's operational environment: 'the issue for entities is going to be determining what to report and what not to report'.[4] The ABA suggested

---

1 For example: Australian Law Reform Commission, *Submission 6*, p. 1; Australian Communications Consumer Action Network, *Submission 7*, p. 1; Consumer Credit Legal Centre, *Submission 8*, p. 1; Office of the Australian Information Commissioner, *Submission 12*, p. 1.

2 Proposed new paragraphs 26X(1)(d) and (2)(d), 26Y(1)(d) and (2)(d), 26Z(1)(d) and (2)(d), and 26ZA(1)(d) of the *Privacy Act 1988* (Cth) (Privacy Act) (item 4 of Schedule 1).

3 For example: Fundraising Institute Australia, *Submission 1*, p. 1; Communications Alliance, *Submission 2*, p. 2; Association for Data-driven Marketing and Advertising, *Submission 3*, p. 2; Australian Communications Consumer Action Network, *Submission 7*, p. 2; Australian Bankers' Association, *Submission 11*, p. 2: Office of the Victorian Privacy Commissioner, *Submission 14*, p. 5.

4 *Submission 11*, p. 2.

that, if the Bill is enacted 'it is critical for the [Australian Information Commissioner (Commissioner)] to be required to develop guidelines for industry on this matter'.[5]

2.5 The Office of the Victorian Privacy Commissioner (Victorian Privacy Commissioner) acknowledged that the Commissioner could be granted legal authority to provide guidance on issues of definition but 'any OAIC guidance will be merely persuasive'. The Victorian Privacy Commissioner suggested:

> Ultimately, the best way to determine the trigger for notification is not through abstract legislative definitions (irrespective of whether such definitions are exclusive or inclusive) but by the [Commissioner] developing binding guidelines to flesh out these terms and providing the Commissioner with an ability to amend those guidelines as circumstances, harms and risks evolve.[6]

2.6 The Communications Alliance submitted that there should be a 'threshold test that industry can use to determine whether 'serious harm' could or would be caused'. Its submission warned that, in the absence of a definition of 'serious harm', there is a possibility of entities inadvertently undermining the objectives of the Bill:

> [I]in the absence of a definition of 'serious harm', it is possible that the legislation will cause an organisation to take a risk-averse position in order to avoid breaching such an obligation. This could, potentially, result in over-reporting of relatively minor data-related errors.[7]

2.7 Alternatively, the Australian Privacy Foundation (APF) did not support the 'real risk of serious harm' threshold, whether or not it was clarified by the Commissioner or in the Bill. In the APF's view, the threshold should not be set at too high a risk of harm, and risk of harm should not be the only trigger for notification (at least to the Commissioner):

> Aggregation of terms limiting the nature of the harm that triggers notification increases the risk that organizations will argue that one or other aggregated term do not apply to them. For example, a phrase such as "real risk of serious harm" is a very high threshold, because of the combination of 'real' (i.e. 'not remote') risk, 'serious' harm' (with no clear notion of seriousness) and 'harm' which may be given a limited definition…
>
> In addition, a second trigger is necessary. Any significant breach should be subject to notification in any case. If that were not the case, then a

---

5 *Submission 11*, p. 3. Also see: Association for Data-driven Marketing and Advertising, *Submission 3*, p. 4, which argued that the failure to define key terms will endow the Australian Information Commissioner (Commissioner) with a free hand to interpret the legislation via regulation.

6 *Submission 14*, p. 6.

7 *Submission 2*, p. 2. In relation to potential over-reporting and under-reporting, also see: Association for Data-driven Marketing and Advertising, *Submission 3*, p. 2; Australian Bankers' Association, *Submission 11*, p. 3; Office of the Victorian Privacy Commissioner, *Submission 14*, p. 5.

> significant insecurity would not become apparent, and would not be addressed, and it would be very likely that it would later give rise to a serious breach that was eminently avoidable. A single threshold test would result in a scheme which was a failure. [8]

Government response

2.8 The Explanatory Memorandum (EM) explicitly states that the definition of 'serious data breach', including the element of a 'real risk of serious harm', is intended to capture only those breaches which are significant enough to warrant notification:

> This will ensure the Government does not create or impose an unreasonable compliance burden on entities regulated by the scheme, and [will] avoid the risk of 'notification fatigue' among individuals receiving a large number of notifications in relation to non-serious breaches.[9]

2.9 In particular, the EM notes that a '*real risk of serious harm to the individual* to whom the information relates…is the standard recommended by the ALRC' (Recommendation 51-1(a)), and is incorporated into the Commissioner's voluntary data breach guidelines, *Data Breach Notification: A guide to handling personal information security breaches* (OAIC guide).[10] The Attorney-General's Department (Department) submitted:

> [The proposed standard] is therefore a commonly understood concept amongst agencies and organisations that have sought to comply with the OAIC guide.[11]

2.10 The Department explained further that the proposed concept of 'serious harm' is also based on the OAIC guide. In addition to that term being well understood, the Department emphasised the flexibility of the OAIC guide to adapt to specific contexts and to evolve over time:

> Accordingly, rather than seek to prescribe a definition in legislation, it is preferable that the OAIC develop guidance about the particular circumstances and factors that might be relevant to the question of harm. This is a common approach taken in privacy regulation, which is more

---

8 *Submission 4*, p. 2. The Australian Privacy Foundation suggested that the Privacy Amendment (Privacy Alerts) Bill 2013 (Bill) should require either a real risk of harm (without qualifications such as 'serious') or a significant breach (regardless whether a real risk of harm has arisen).

9 Explanatory Memorandum (EM), p. 40. Also see: the Hon. Mark Dreyfus QC MP, Attorney-General, 'Privacy Alerts to notify Australians of data breaches', Media Release, 28 May 2013.

10 EM, pp 1-2 (emphasis in original). Also see: Office of the Australian Information Commissioner, *Data Breach Notification: A guide to handling personal information security breaches* (OAIC guidelines), April 2012, p. 1, available at: http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches (accessed 19 June 2013); Australian Communications Consumer Action Network, *Submission 7*, p. 2.

11 *Submission 10*, p. 4.

> principles-based in nature. It is intended that a revised OAIC guide will continue to provide guidance on the factors that entities should consider when assessing whether the harm is 'serious'.[12]

2.11 In this context, the OAIC advised that, if the Bill proceeds, 'the OAIC will prioritise the amendment of the [OAIC guide] to address and provide clarity on the operation of the new mandatory notification requirements'.[13]

Mandatory notification provisions

2.12 Proposed new section 26ZB of the Privacy Act requires an entity to undertake three specific actions, as soon as practicable, after forming a reasonable belief that a 'serious data breach' has occurred:

- preparation of a detailed statement concerning the breach;[14]
- provision of a copy statement to the Commissioner;[15] and
- notification:
  - by taking such steps as are reasonable in the circumstances to notify the contents of the statement to each 'significantly affected' individual;[16] and
  - by publishing a copy of the statement on the entity's website (if any) and in at least one newspaper circulating generally in each state/territory, if prescribed 'general publication conditions' are satisfied (collectively, the notification requirement).[17]

2.13 Liberty Victoria welcomed the proposed mandatory notification provisions, submitting that the proposed process reflects similar processes in environmental protection legislation, as well as providing 'a beneficial remedy [and] deterrent to lax procedures for organisations and entities upon whom the requirement is imposed'.[18]

---

12 *Submission 10*, p. 4.

13 *Submission 12*, p. 5.

14 Proposed new paragraph 26ZB(1)(e) and proposed new subsection 26ZB(2) of the Privacy Act (item 4 of Schedule 1). Also see: EM, p. 50, which notes that the content of the statement is based on the matters set out in the OAIC guidelines.

15 Proposed new paragraph 26ZB(1)(f) of the Privacy Act (item 4 of Schedule 1).

16 Proposed new paragraph 26ZB(1)(g) of the Privacy Act (item 4 of Schedule 1). An individual will be 'significantly affected' by a serious data breach in one of two situations: if the individual is at real risk of serious harm from the breach; or if the information relates to the individual and the individual is deemed by the regulations to be significantly affected by the breach: see proposed new paragraph 26ZB(1)(h) of the Privacy Act (item 4 of Schedule 1).

17 Proposed new paragraph 26ZB(1)(h) of the Privacy Act (item 4 of Schedule 1).

18 S*ubmission 9*, pp 3-4.

2.14 The Communications Alliance argued however that the specific actions outlined in proposed new section 26ZB are contrary to good business practice, as reflected in the OAIC guide:

> [G]ood business practice would be to (a) contain the breach and do an assessment; (b) evaluate the risks; and then, if necessary, notify those affected by the breach. It is concerning that the Bill places more emphasis on notifying – and potentially confusing or alarming customers – than containing the breach, rectifying the issue and preventing its reoccurrence.[19]

2.15 The ABA referred to proposed new subsection 26ZB(12), which provides for regulations to declare that one or more specified conditions are 'general publication conditions' for the purposes of the section. The ABA expressed concern regarding the uncertain scope of the 'general publication conditions' notification model:

> There is a critical element of the notification model in the Bill that is missing because it is unclear what "general publication conditions" will mean if these conditions are satisfied. Without this definition, the real impact of the Bill cannot be assessed because the meaning of this expression will be covered by a regulation-making power in the Bill. Regulations dealing with this aspect have not been provided with the Bill.[20]

Government response

2.16 The Department submitted that there are a range of factors which might be relevant to 'general publication conditions', such as the type of entity involved or the location of the affected individuals:

> The making of regulations would enable more flexibility in allowing these matters of detail to be changed as notification processes develop into the future.
>
> For example, the regulations could provide that the 'general publication conditions' are met:
>
> - where particular individuals do not have readily available contact details, or
> - where online and newspaper publication methods may reach a larger number of affected individuals in a more timely manner. [21]

2.17 The Department assured the committee that the development of privacy regulations would be conducted in close consultation with relevant stakeholders, including interest groups. The Department noted also that any regulations made would be subject to disallowance by the parliament as disallowable instruments.[22]

---

19 *Submission 2*, p. 3.

20 *Submission 11*, p. 5.

21 *Submission 10*, pp 5-6. Also see: EM, p. 51.

22 *Submission 10*, p. 6.

2.18 In response to concerns regarding the order of the actions set out in proposed new section 26ZB, the Department contended that the Bill will not depart from the approach adopted in the OAIC guide:

> The OAIC guide contains numbered steps to take in response to a data breach, but notes that particular steps may be taken simultaneously or in quick succession. Further, the OAIC guide states that immediate notification should be the first step if appropriate.
>
> Therefore, the Bill does not have the effect of prioritising notification over other remedial action. The new notification requirement is completely consistent with the existing OAIC guide, and will complement existing legislative requirements that must be complied with in responding to a data breach.[23]

Exceptions to the mandatory notification provisions

2.19 Proposed new section 26ZB of the Privacy Act wholly or partially exempts some entities from the measures proposed in the Bill.[24] For example, the Commissioner will be empowered to issue a written notice of exemption on public interest grounds, on the application of an entity or on the Commissioner's own initiative. This exemption would apply to the totality of the notification requirements set out in proposed new section 26ZB.[25]

Opposition to the proposed measure

2.20 Some submissions expressed concern with the proposed exceptions to the mandatory notification provisions, arguing that the provisions should be narrower, if they are to be legislated at all, and be subject to a greater degree of accountability and transparency.

2.21 Liberty Victoria, for example, submitted that a 'large part of the Bill is dedicated to exceptions', the breadth of which Liberty Victoria opposed. In relation to the proposed public interest exemption, Liberty Victoria argued:

> [T]his exemption should be limited to subsections (1)(g) & (h) [the notification requirement] and not provision of the statement to the Commissioner…[I]t might be preferable to allow certain classes of matter to be referred to the Commissioner by enforcement bodies seeking a recommendation as to disclosure or non-disclosure or exemption under the new part, rather than the enforcement body clothing itself with total

23 *Submission 10*, p. 6.

24 Proposed new subsections 26ZB(4) -(11) of the Privacy Act (item 4 of Schedule 1).

25 Proposed new subsections 26ZB(5)-(7) of the Privacy Act (item 4 of Schedule 1). Note: the exemption applies to the three mandatory steps set out in proposed new subsection 26ZB(1) of the Privacy Act.

> immunity and exercising their own broad exemption for all classes of data breach for all time.[26]

2.22 The APF argued that the mandatory notification provisions should apply to all organisations and all personal information that are 'reasonably within reach of Commonwealth jurisdiction'.[27] Its views in regard to exemptions were consistent with those of the Cyberspace Law and Policy Centre, which submitted:

> Exceptions, if they are permitted, should be limited to named entities not classes, require full justification and verification, be limited in duration to the minimum time necessary, not allow failure to inform the regulator, and otherwise be as limited as possible…Similarly, the OAIC's operation of the scheme should not be subject to discretionary variation or exceptions; where discretions exist they should be defined, and transparently reported. This Bill should not set up a scheme where there is an endless queue to the Commissioner's door for secret exemptions, which would undermine the purpose of the Bill, and the basis of public trust and confidence that they will be able to find out if there is a breach; this would be both a waste of the Commissioner's time, which is better spent pursuing breaches and complaints, and undermines the expectation of compliance.[28]

2.23 Mr Bruce Arnold, a lecturer in privacy, secrecy and data protection law at the University of Canberra, also did not support endowing the Commissioner with discretionary power to grant exemptions to the mandatory notification requirement:

> Supervision by the [Commissioner] of mandatory breach reporting should not be fundamentally weakened through scope for discretionary exceptions. For the purposes of public administration we should reduce the subjectivity that results in 'closed door' deal-making – and requests for deals. Consistency and transparency will reinforce the credibility of the [OAIC], which has been eroded by perceptions that the organisation is either very permissive or naïve[.][29]

Government response

2.24 In determining whether an exemption notice will be issued on the grounds of public interest, the EM indicates that guidance on the relevant factors will be developed by the Commissioner and be made available to stakeholders:

> In that respect, the ALRC commented that [provisions such as those establishing the discretionary exemption power on public interest grounds] could cover situations, for example, where there is a law enforcement investigation being undertaken into a data breach…and notification would

---

26 *Submission 9*, pp 4-5.

27 *Submission 4*, Attachment 2, p. 2. Also see: Mr Bruce Arnold, *Submission 5*, p. 4; Cyberspace Law and Policy Centre, *Submission 13*, p. 2.

28 *Submission 13*, p. 3. Also see: Australian Privacy Foundation, *Submission 4*, p. 4.

29 *Submission 5*, p. 4.

> impede that investigation, or where the information concerned matters of national security. This provision is intended to cover cases of that nature (where these activities, or the information concerned, are not already exempt from the scheme), particularly where a private sector organisation suffers the data breach and is responsible for reporting. In those situations, a Commonwealth agency or private sector organisation would have grounds to seek this exemption on advice from an enforcement body or intelligence agency.[30]

Committee view

2.25 The committee supports enhanced privacy protection for individuals whose personal information has been accessed by, or disclosed to, a third party as the result of a 'serious data breach'. The committee notes the Commissioner's evidence that data breaches are under-reported and on the increase within Australia.[31]

2.26 The measures proposed in the Bill are supported by the ALRC, which specifically recommended such a reform to help resolve the situation of individuals being adversely affected by the compromise of their personal information. The Commissioner has also expressed unconditional support for the Bill, as did consumer advocates who participated in the inquiry. The committee agrees that the proposed reform is 'long overdue' and would benefit Australian consumers, as well as industry stakeholders, who would be simultaneously encouraged to effect and maintain high-quality data security practices.

2.27 A public consultation paper was released by the Department in October 2012, seeking the community's view on whether a mandatory data breach notification law should be introduced in Australia and, if so, how the law should be framed.[32] This was followed by a confidential targeted consultation in respect of a more detailed legislative model in April 2013.[33] The committee considers that stakeholders have been afforded ample opportunity to comment on the proposals in the Bill, noting that the matters under consideration were first raised in 2008 by the ALRC.

2.28 The trigger for mandatory notification concerned several submitters. While the committee acknowledges these concerns, the Department pointed out that this threshold has been implemented in the voluntary data breach guidelines since 2008, when the ALRC recommended the standard. The committee therefore accepts the Department's view that the threshold is familiar to stakeholders, and agrees that it is preferable for the Commissioner to continue to issue guidance on the meaning of a 'real risk of serious harm', as circumstances require. In this context, the committee

---

30 EM, p. 52.

31 *Submission 12*, pp 2-4.

32 Attorney-General's Department, *Australian Privacy Breach Notification*, Discussion Paper, October 2012, p. 11.

33 EM, Regulation Impact Statement, p. 7.

notes that the Commissioner is already considering amendments to the OAIC guide, to account for the changes to be introduced by the Bill.

2.29 Accordingly, the committee concludes that the Bill should be passed.

Recommendation 1

2.30 The committee recommends that the Senate pass the Bill.

Senator Trish Crossin

Chair