Data Breach Notifications

Submission by the Australian Communications Consumer Action Network to the Attorney-General's Department

November 2012

About ACCAN

The Australian Communications Consumer Action Network (ACCAN) is the peak body that represents all consumers on communications issues including telecommunications, broadband and emerging new services. ACCAN provides a strong unified voice to industry and government as consumers work towards availability, accessibility and affordability of communications services for all Australians.

Consumers need ACCAN to promote better consumer protection outcomes ensuring speedy responses to complaints and issues. ACCAN aims to empower consumers so that they are well informed and can make good choices about products and services. As a peak body, ACCAN will activate its broad and diverse membership base to campaign to get a better deal for all communications consumers.

Contact

Steven Robertson

Suite 402, Level 4
55 Mountain Street
Ultimo NSW, 2007
Email: steven.robertson@accan.org.au
Phone: (02) 9288 4000
Fax: (02) 9288 4019
TTY: 9281 5322

Contents

Introduction 4

Consumer issues 5

Responses to the AGD Discussion Paper 6

(1) Should Australia introduce a mandatory data breach notification law? 6

(2) Which breaches should be reported? Triggers for notification 7

(3) Who should decide on whether to notify? 8

(4) What should be reported (content and method of notification), and in what time frame? 9

(5) What should be the penalty for failing to notify when required to do so? 10

(6) Who should be subject to a mandatory data breach notification law? 10

(7) Should there be an exception for law enforcement activities? 11

accan

Introduction

The Australian Communications Consumer Action Network (ACCAN) is the peak body that represents all consumers on communications issues including telecommunications, broadband and emerging new services. ACCAN provides a strong unified voice to industry and government as consumers work towards availability, accessibility and affordability of communications services for all Australians.

ACCAN welcomes the opportunity to respond to the Attorney-General's Department's (AGD's) discussion paper on introducing a mandatory data breach notification requirement. A number of significant breaches have occurred in recent years involving telecommunications providers or online services. In 2012, AAPT's servers were attacked by the group "Anonymous".[1] In late 2011, over 700,000 Telstra customer records were made publicly accessible over the internet.[2] In early 2011, the Sony Playstation Network was compromised, with approximately 77 million customers affected worldwide.[3] In late 2010, a mailing list error resulted in 220,000 letters with incorrect mailing addresses being mailed to Telstra customers.[4] In 2009, a design flaw resulted in the chat transcripts of a depression counselling service being made publicly accessible online.[5]

While these breaches were ultimately discovered (either by voluntary notification or through the media), there may be many more breaches that go undisclosed. A mandatory data breach notification requirement would provide greater information to consumers about the security of their personal information, and provide an incentive for organisations to improve their security practices. For these reasons, ACCAN supports the introduction of a mandatory data breach notification requirement – indeed, we think that such a requirement is long overdue.

---

[1] Office of the Australian Information Commissioner, *AAPT Anonymous hack*, 6 August 2012, <http://www.oaic.gov.au/news/statements/statement_120806_aapt_melb_it.html>.
[2] Office of the Australian Information Commissioner, *Telstra Corporation Limited*, June 2012, <http://www.oaic.gov.au/publications/reports/own_motion_telstra_bundles_June_2012.html>.
[3] Office of the Australian Information Commissioner, *Sony PlayStation Network/Qriocity*, 29 September 2011, <http://www.oaic.gov.au/publications/reports/own_motion_sony_sep_2011.html>.
[4] Office of the Australian Information Commissioner, *Telstra Corporation Limited (Telstra)*, 7 July 2011, <http://www.oaic.gov.au/publications/reports/own_motion_telstra_May_2011.html>.
[5] Sophie Scott, *Probe into depression chat leaks*, ABC News, 11 December 2009, <http://www.abc.net.au/news/2009-12-11/probe-into-depression-chat-leaks/2572248>.

accan

Consumer issues

The AGD's discussion paper asks a number of questions with relevance to consumer interests, and ACCAN has responded to these questions below. We also note several additional consumer issues that we recommend the AGD address in the future.

Further privacy reform required

While ACCAN supports a data breach notification law, we note that the passage of such a law should not be used to justify a weak approach to privacy and information security law reform. A notification requirement is an important component of consumer privacy and security, but it is not the only component.[6]

Cost to consumers

The costs associated with compliance with a mandatory data breach notification requirement should not be passed on to consumers.

Effect on existing consumer protections

A mandatory data breach notification law should not have the effect of reducing existing consumer protections – for example, the limits on consumer liability under the *Electronic Funds Transfer Code of Conduct*[7] or the consumer protections of the *Telecommunications Consumer Protections Code*.[8] Similarly, notification should not relieve organisations of their existing obligations.

---

[6] The risks of a data breach notification law being used to avoid further privacy and security reforms are raised in Roger Clarke, *Why you should oppose a data breach notification law*, itnews, 19 October 2012, <http://www.itnews.com.au/News/319723%2cwhy-you-should-oppose-a-data-breach-notification-law.aspx>.

[7] *Electronic Funds Transfer Code of Conduct*, cl 5, <http://www.asic.gov.au/asic/asic.nsf/byheadline/EFT-code-amendments>.

[8] *Telecommunications Consumer Protections (TCP) Code*, C628:2012, <http://www.commsalliance.com.au/Documents/all/codes/c628>.

accan

Responses to the AGD Discussion Paper

(1) Should Australia introduce a mandatory data breach notification law?

1.1 Are the current voluntary data breach notification arrangements sufficient?

Current voluntary data breach notification arrangements are not sufficient. Although several breaches have been made public, various estimates[9,10] suggest that the vast majority of breaches go unreported. Going forward, various current proposals[11] and projects[12] suggest that the amount of personal information that will be at risk of data breach is likely to increase, and the need for a mandatory data breach notification requirement will also increase.

1.2 Should the Government introduce a mandatory data breach notification law?

ACCAN's view is that a mandatory data breach notification law should be introduced, and would offer three key benefits to consumers:

- The law would provide greater information to consumers about the security of their personal information, allowing consumers to respond to protect their information and identity when a breach occurs, and to avoid organisations with a record of lax security practices.
- As a corollary, the law would provide an incentive for organisations to improve their security practices. While the risk of information breaches cannot be removed entirely, it can be minimised. The law would, in particular, provide an incentive to avoid breaches arising from simple mistakes, such as the loss of a storage device containing unencrypted customer information.
- The law would bring Australia into line with global best practice on breach notifications. As noted in the AGD's discussion paper, data breach notification laws already exist in a number of key jurisdictions and are under consideration in others. It is important for Australia to meet this global standard, since consumer expectations about privacy and security will be in large part informed by what they see occurring in other jurisdictions.

We note that arguments have been made to the effect that mandatory breach notifications would lead to "unnecessary alarm"[13] or that "consumers will tune out if every minor incident

---

[9] Dan Harrison and Ben Grubb, *Roxon proposes compulsory reporting of online privacy breaches*, Sydney Morning Herald, 17 October 2012, <http://www.smh.com.au/it-pro/security-it/roxon-proposes-compulsory-reporting-of-online-privacy-breaches-20121017-27qf0.html>.

[10] Asher Moses, *Thousands of privacy breaches going unreported*, The Age, 27 July 2011, <http://www.theage.com.au/technology/technology-news/thousands-of-privacy-breaches-going-unreported-20110727-1hzes.html>.

[11] Notable proposals include the inquiry into reforming the national security legislation, and the proposed National Trusted Identifiers Framework.

[12] Notable projects include the "Digital Mailboxes" of Australia Post and Digital Post Australia, along with a general trend towards cloud-based services.

[13] This suggestion has been made by, for instance, the acting chief of the Australian Bankers' Association; see Andrew Colley, *Banks seek to hide privacy breaches from customers*, The Australian, 19 October 2012, <http://www.theaustralian.com.au/australian-it/government/banks-seek-to-hide-privacy-breaches-from-customers/story-fn4htb9o-1226498999294>.

is reported".[14] We suggest, however, that this concern has been overstated. It is at this stage clear to consumers that data breaches do occur, yet the consumer response has generally been one of concern rather than alarm. Moreover, the more complete and transparent information that would result from a breach notification law is likely to reduce consumer alarm, since the "unknown unknowns" will be reduced. As more breaches are reported, consumer expectations about privacy and security will come to reflect the fact that security cannot be guaranteed. However, if this change is to occur without a complete loss of confidence in organisations' security practices, it is essential that consumers are fully informed of the facts. In short, ACCAN's view is that, since the risks can never be completely removed, it is important that consumers are at least as informed about the risks as possible. Hiding relevant information from consumers is not an appropriate basis for managing consumer concern.

Other submissions made to the ALRC's review of the *Privacy Act* argued that existing laws make a mandatory breach notification requirement unnecessary. The ALRC noted that:

> "Some stakeholders stated that there was no need for a data breach notification requirement. The Australian Bankers' Association (ABA) noted that there is an express obligation under the *Privacy Act* to have in place adequate data security measures. It argued that this obligation, combined with the ALRC's proposed new enforcement powers for the Privacy Commissioner, will ensure that there are sufficient 'commercial incentives' for organisations to secure data, without a need for breach notification requirements."[15]

ACCAN disagrees with the ABA's suggestion as stated by the ALRC. Clearly, the express obligation to secure data under the *Privacy Act* has been inadequate in ensuring that organisations actually secure data. Moreover, the requirement to secure data under the *Privacy Act* – even in the event that the proposed amendments to the Commissioner's powers[16] do encourage organisations to meet the requirement – does not achieve the further goals of informing consumers about the security of their personal information.

(2) Which breaches should be reported? Triggers for notification

2.1 What should be the appropriate test to determine the trigger for notification?

ACCAN suggests that the trigger should be at a level similar to that in the *Privacy (Data Security Breach Notification) Amendment Bill 2007*, i.e. that notification should occur:

> "when there has been a confirmed or reasonably suspected breach of data security involving that person's personal information following the discovery of the breach."

---

[14] ADMA, *Constant stream of data breach notifications will cause unnecessary consumer angst*, 17 October 2012, <http://www.adma.com.au/connect/articles/adma-concerned-constant-stream-of-data-breach-notifications-will-cause-unnecessary-consumer-angst/>.
[15] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108, 51.53.
[16] *Privacy Amendment (Enhancing Privacy Protection) Bill 2012*.

More demanding triggers suggested in the AGD's discussion paper, such as

- A real risk of serious harm;
- A material breach of data security standards; and
- The disclosure is likely to adversely affect the personal data or privacy of an individual,

are, in ACCAN's view, open to interpretation in a manner than negatively impacts on consumers – it is not clear, for instance, whether the disclosure of credit card information carries "a real risk of serious harm". The broader definition from the 2007 Bill would limit the need for organisations to make judgments on the degree of risk introduced by a breach.

At the same time, we note that some of the possible triggers referred to in the AGD's discussion paper may be excessively broad. Any online transaction, for instance, carries to some degree "a risk of unauthorised disclosure". While certain types of data are particularly sensitive and should automatically trigger a breach notification (see question 2.3), we recognise the concerns of "notification fatigue" if notifications are made for too wide a range of events, and agree that an excessively broad definition might contribute to this fatigue.

2.2 Should it be based on a 'catch all' test, or based on more specific triggers, or another test?

The trigger should be based on a catch all test. However, some specific triggers could, and should, be included to ensure notification is required in particular cases.

2.3 What specific elements should be included in the notification trigger?

We suggest that the following elements, at a minimum, be included as specific triggers:

- Sensitive information, as defined in the *Privacy Act* (or the *Privacy Amendment (Enhancing Privacy Protection) Bill 2012*);
- Financial information;
- Addresses and other contact information;
- Unencrypted personal information; and
- Passwords and other security credentials.

(3) Who should decide on whether to notify?

3.1 Who should be notified about the breach?

Both the Privacy Commissioner and individuals who are likely to be affected should be notified of the breach. We suggest that notification should be made to all relevant parties where personal information is hosted by a third party. If a small business hosts its customer information on a cloud storage system, for example, the small business and its customers should be notified of a breach of that cloud storage system.

3.2 Which of the below should decide whether to notify?

(i) the organisation or agency;

(ii) the Commissioner; or

(iii) the organisation/agency in consultation with the Commissioner.

In the first instance, the organisation or agency should make the decision. We acknowledge that it would be impractical for the Commissioner to make determinations in every case of a possible breach. However, consultation with the Commissioner should be encouraged.

A mechanism should also exist for an individual to complain to the Commissioner if the individual believes a breach should have been, but was not, notified.

The Commissioner should have the power to compel notification.

(4) What should be reported (content and method of notification), and in what time frame?

4.1 What should be the form or medium in which the data breach notification is provided?

To gain the greatest benefit from a data breach notification law (in terms of consumer awareness and incentives on organisations to implement suitable security practices) ACCAN submits that a public register of breaches should be maintained by the Commissioner.

In general, ACCAN supports the suggestion in the AGD's discussion paper that individuals are notified using whatever medium is appropriate and normally used by the organisation to communicate with the individual.

We note, however, that there is the potential for data breach notifications to be used as a vector for phishing attacks, and suggest that the use of hyperlinks and similar devices in email notifications be discouraged or prohibited.[17]

4.2 Should there be a set time limit for notification or a test based on notifying as soon as is practicable or reasonable?

Organisations should be responsible for notifying as soon as is practicable or reasonable after a breach is known (or reasonably suspected) to have occurred. To support organisations, guidance as to what constitutes "practicable or reasonable" timing should be issued by the Commissioner.

A set time limit would serve only to signal to organisations that notification could be delayed until that limit had been reached.

We note that delayed notification may be needed in particular cases, e.g. where notification would negatively impact on law enforcement activities.

---

[17] A note in ASIC's *ePaymanet Code*, art 21.2, similarly discourages the use of hyperlinks to give disclosures or information. The Australian Federal Police website also notes the risk of phishing attacks based on the use of hyperlinks in emails; see <http://www.afp.gov.au/policing/cybercrime/internet-fraud-and-scams.aspx>.

4.3 What should be the content of the notification?

ACCAN's view is that the notification should contain sufficient information to:

- Alert the individual to the occurrence of the breach, the date when it is believed to have occurred, and the nature of the breach (unauthorised remote access, unauthorised access by an employee, loss of a storage device containing data, etc.);
- Inform the individual of the types of data that are known, or are significantly likely, to have been accessed;
- Inform the individual whether any means (e.g. encryption) were in place to keep the information secure in the event of a breach;
- Suggest steps that the individual should take to minimise any harm resulting from the breach; and
- Suggest steps that the individual should take to minimise the risk and harm of any future breaches, e.g. by limiting the information they provide to organisations.

(5) What should be the penalty for failing to notify when required to do so?

5.1 Should there be a penalty or sanction for failing to comply with a legislative requirement to notify?

ACCAN supports the inclusion of a penalty or sanction for failure to comply with a legislative requirement to notify.

5.2 If so, what should be the penalty or sanction, and the appropriate level of that penalty or sanction?

The specific penalty or sanction should depend on the nature of the breach (including the types and volume of information disclosed) and the nature and history of the organisation with respect to privacy and security. We urge, however, that the penalty or sanction be severe enough to act as a deterrent to further failure to notify, to act as an incentive to organisations to notify in borderline cases and to encourage organisations to invest in privacy and security practices.

(6) Who should be subject to a mandatory data breach notification law?

6.1 Who should be subject to a mandatory data breach notification law?

ACCAN agrees with the ALRC's view that consistent privacy regulation is desirable. We therefore support the ALRC's recommendation that the data breach notification law should apply to entities regulated by the *Privacy Act*, i.e.:

- Public sector organisations; and
- Large private sector organisations.

6.2 Should the scope of a mandatory data breach notification law be the same as the existing scope of the Privacy Act?

ACCAN supports the ALRC's recommendation that the data breach notification law should apply to entities regulated by the *Privacy Act*.

(7) Should there be an exception for law enforcement activities?

7.1 Should there be an exception for law enforcement activities?

ACCAN's view is that an exception for law enforcement activities is appropriate in cases where the public benefit in notification would be outweighed by the public benefit in delaying notification. Any such exception should be restricted to cases where the notification would be detrimental to a specific law enforcement activity. A breach of a database should not be exempted, for instance, simply because the database was in use by a police force.

Notification should still occur once the relevant activities are completed.

7.2 Would such an exception add anything to the ALRC's proposed public interest exception?

Including specific exceptions may assist in avoiding the misuse of the public interest exception, for example by a company arguing that maintaining their reputation is in the public interest.