Submission to the Attorney-General's Department on the Australian Privacy Breach Notification Discussion Paper

Pirate Party Australia

Simon Frew (simon.frew@pirateparty.org.au)

November 2012

Introduction

Pirate Party Australia would like to thank the Attorney General's Department for the opportunity to make a submission on this important issue. The need for mandatory data breach reporting is growing every year, as an increasing proportion of Australian life is being conducted using online services.

The only significant issue regarding the approach of the discussion paper is the lack of acknowledgement of how much extra work a scheme such as this would entail. The Office of the Privacy Commissioner will be expected to take on significant new responsibilities and will need to be adequately staffed and funded. The significant cost that data breaches incur upon affected businesses and departments demonstrates the need for efficient investigation and reporting, and reducing this cost on society will make any extra expense incurred by the government wholly justified.

Note

This PDF has been compiled from the submission originally made in November 2012. Formatting (including the formatting of citations) has been modified but apart from this notice no body text has been changed.

1 Should Australia introduce a mandatory data breach notification law?

1.1 Are the current voluntary data breach notification arrangements sufficient?

The current arrangements provide no guarantees that Australians subject to privacy breaches will be notified. It is vital that when such breaches occur the victims are informed as soon as possible so that they can take measures to secure their personal information. Having knowledge of a data breach gives the victim opportunity to cancel

credit cards, change passwords, and so on, before serious financial or personal harm can occur.

A study released by the Centre for Internet Safety in April this year indicated that 85% of Australians believe that data breach notifications should be mandatory and 86% rated identity theft as their greatest concern online.[1]

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

Mandatory data breach notification laws are necessary to ensure that organisations holding Australians' private data are required to disclose data breaches in a timely manner so measures can be taken to re-secure the data.

There is an incentive for organisations to cover up data breaches as they risk reputational harm. This is demonstrated by the Australian Bankers Association's response to the announcement of this discussion paper where their spokesperson Tony Bourke claimed that 'attempting to notify individuals potentially affected could lead to significant levels of community concern, disproportionate to the actual level of risk, which could well be zero.'[2]

The idea that the risk from a data breach 'could well be zero' is simply preposterous. Banking information in particular is extremely sensitive and its misuse could be devastating to any individual, even if a bank's insurance compensated for any loss in the medium-term. A bank may consider personal information such as address, date of birth or transaction information to be no further customer risk, whereas in reality every piece of information can allow criminal organisations to build up profiles of the customers.

What this attitude demonstrates is the need for breach notifications to be mandatory. Banks fear 'significant levels of community concern' and logically may be reluctant to report any data breach unless they

[1] Centre for Internet Safety, *Privacy and the Internet: Australian Attitudes to Online Privacy* (April 2012) <http://www.canberra.edu.au/cis/storage/Australian%20Attitutdes%20Towards%20Privacy%20Online.pdf>.

[2] Andrew Colley, 'Banks seek to hide privacy breaches from customers', *The Australian* (online), 19 October 2012 <http://www.theaustralian.com.au/australian-it/government/banks-seek-to-hide-privacy-breaches-from-customers/story-fn4htb9o-1226498999294>.

face stiff penalties for failing to do so.

Many companies that deal with customer data do not currently take security seriously enough. This can be seen by recent hacks, such as of AAPT,[3]where customer data was stolen due to poor security practices. The risk of reputational damage for failing to adequately protect customer data will be a motivating factor in many companies going to greater lengths to ensure their electronic systems are adequately protected.

2 Which breaches should be reported? Triggers for notification

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

All breaches where sensitive personal information has been, or is likely to have been, exposed to unauthorised persons should be reported to the victim of a data breach. The Privacy Commissioner should be informed whenever breaches occur, so a catalogue can be built of the types of attacks deployed. This would give IT security experts the ability to see what measures are needed to defend against attacks. A catalogue of security breaches will provide information about the types of attacks that can be launched against particular systems.

Reporting thresholds based on quantities of records exposed, or a judgement call about 'serious harm,' creates the risk of under-reporting of breaches. Any individual who has sensitive personal information exposed is at risk to a range of further attacks and must be informed in order to be able to take remedial actions to protect their data.

Private data includes, but is not limited to:

- Full name and address,
- Password or encryption keys,
- Banking or credit card details,

[3]Ben Grubb, 'Hackers publish AAPT data in protest over web spy plan', *The Sydney Morning Herald* (online), 30 July 2012 <http://www.smh.com.au/it-pro/security-it/hackers-publish-aapt-data-in-protest-over-web-spy-plan-20120730-238lp.html#ixzz2CuAG6Ide>.

- Personal records (such as medical records),
- Locational information (such as GPS movements).

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

There should be two standards of test. Any security breach occurring online should be reported to the Privacy Commissioner for the catalogue of online attacks. Any time sensitive personal information, such as encryption keys or credit card numbers are exposed, affected individuals must be informed as soon as possible.

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

The affected body will need to report to the Privacy Commissioner any time their security systems are breached and it has been possible for private data (be that customer data, business information or business documents) to be exposed. If, after investigation, the Privacy Commissioner believes on a balance of probability that private data has been exposed, then customers must be informed immediately.

If private personal data such as address details, passwords or credit card numbers are exposed then anyone whose data has been breached must be informed immediately.

3 Who should decide on whether to notify?

3.1 Who should be notified about the breach?

The Office of the Privacy Commissioner is the most appropriate authority to be informed when data breaches occur. Affected customers also must be informed as soon as practicably possible. In cases where security has been breached, but private data remains secure, informing the Privacy Commissioner would be a reasonable measure to ensure authorities are aware of any security issues.

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

The organisation should have primary responsibility for reporting data breaches to affected customers. In situations where data breaches occur and sensitive private information has not been exposed, a report should only required to be sent to the Privacy Commissioner, who should review the decision and catalogue the breach in order to ensure information about the types of attacks occurring can be countered by Australian IT security workers.

Pirate Party Australia believes that the Office of the Privacy Commissioner must receive extra funding proportionate to any new responsibilities received under this legislation. The cost of data breaches in Australia reached $2.18 million per incident in 2011.[4] Consequently we believe that any expansion of the Privacy Commissioner's Office would be justified to save Australian companies from serious financial harm. This would occur through the extra motivation to avoid data breaches by mandatory reporting and providing improved information about the types of attacks that occur by cataloguing data breaches as they occur around the country.

Additionally, allowing an organisation or agency to decide whether to notify or not would leave the intention of mandatory data breach reporting legislation — to protect customers' data — potentially nulled. Organisations should be required to report *all* data breaches, to the Commissioner and/or customers as described above.

[4] Ponemon Institute LLC, *2011 Cost of Data Breach Study: Australia* (March 2012) <https://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-australia-us.pdf>.

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?

Any data breach notification should be forwarded through the primary means of communication between the company or agency and the customer. If snail mail is the preferred method of communication, an email should also be sent where possible in order to limit the damage the breach may incur by informing the customer immediately.

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

Notification should be required as soon as reasonably possible so that the victim can take measures to protect their personal data from misuse.

4.3 What should be the content of the notification?

A data breach notification should include information about the breach, including: when it occurred, a description of data was exposed, what measures could be taken to re-secure the data ,and how to contact the Privacy Commissioner if there is a complaint.

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?

There needs to be serious financial sanctions for failing to report data breaches where the organisation or government department is aware that they have occurred.

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

Penalties should be greater than the financial harm that could be incurred by the loss of the data and become exponentially harsher for repeat offenders. Wilfully hiding the loss of private data should incur criminal sanctions. This will provide adequate motivation to ensure data breaches are reported in an accurate and timely manner.

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?

Any organisation that manages private data should be subject to mandatory breach notification laws. Penalties imposed for failure to disclose breaches should be proportional to the size of the organisation and the amount of data lost.

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

Mandatory data breach notification laws should also include government departments and agencies.

7 Should there be an exception for law enforcement activities?

7.1 Should there be an exception for law enforcement activities?

While reporting a breach of privacy by Police during a lawful investigation would be counterproductive, should the Police lose a suspect's, victim's or anyone else's information to another entity, it needs to be reported. Suspects and victims should not be subject to punishment through having their identity inadvertently stolen without being able to take measures to defend themselves against the breach. It is imperative that any person who has private data breached can take measures to limit or negate any harm that the loss of their personal information may incur. This may require special provisions for what action law enforcement agencies should take.

Suspect and victim data must be protected with the same care as the data of any other member of society and therefore they need to have the same right to take measures to protect breached private data. Government agencies must have the strictest data protection provisions so this is not an issue for investigations or the private data of suspects.

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

Pirate Party Australia believes that a public interest exception could be dangerous to the safety of online data due to the possibility of covering

up vast data leaks under the guise of protecting the public interest. Public servants could decide that keeping the public's confidence in the Medicare system (for example) required the loss of private medical records be kept secret.