Centre for Internet Safety

July 2012

Submission to the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 Enquiry

Foreword

The Centre for Internet Safety welcomes the opportunity to respond to the Senate Standing Committees on Legal and Constitutional Affairs enquiry into the Privacy Amendment (Enhancing Privacy Protection) Bill 2012.

The Centre for Internet Safety believes consumers, businesses and governments need to be aware of the critical nature of privacy in the online environment and therefore:

The Centre for Internet Safety supports the proposed amendments to the Privacy Act 1988, partially implementing the Australian Law Reform Commission's (ALRC) report, For Your Information: Australian Privacy Law and Practice. The Centre:

1. Recommends minor additions to the wording of Australian Privacy Principle 11 to bring into effect another ALRC proposal: data breach notification;

2. Recommends the powers of the Privacy Commissioner be expanded so that the office may appear before civil courts to have penalty units applied against privacy breaches; and

3. Calls for the Privacy Commissioner's office to be sufficiently staffed to reflect the volume and seriousness of investigations required to maintain public confidence.

We would be very happy to provide further information and details on the issues we raise.

Alastair MacGibbon
Director

Nigel Phair
Director

Background

The Internet traverses political, cultural and geographic boundaries within and between countries. It brings people and their views and behaviours closer together - and allows them to interact - in a speed and manner never seen before. The Internet exposes us to views and behaviours that reinforce and challenge our beliefs, threaten us, help us.

The Internet has opened international trade to consumers with person-to-person online financial transactions, eCommerce and classified ad platforms. It has reunited old friends - and helped us find new ones - via social networks, dating websites and computer-to-computer telephony and messaging. It has helped enable individuals to become publishers, commentators and journalists via blogs, video sites and social networks. And it has brought offenders closer to victims all around the world.[1]

About the Authors

Alastair MacGibbon is an internationally-respected authority on cybercrime, including Internet fraud, consumer victimisation and a range of Internet security and safety issues. For almost 5 years Alastair headed Trust & Safety at eBay Australia and later eBay Asia Pacific. He was a Federal Agent with the Australian Federal Police for 15 years, his final assignment as the founding Director of the Australian High Tech Crime Centre.

Nigel Phair is an influential analyst on the intersection of technology, crime and society. He has published two acclaimed books on the international impact of cybercrime, is a regular media commentator and provides executive advice on cyber security issues. In a 21 year career with the Australian Federal Police he achieved the rank of Detective Superintendent and headed up investigations at the Australian High Tech Crime Centre for four years.

About the Centre for Internet Safety

The Centre for Internet Safety at the University of Canberra was created to foster a safer, more trusted Internet by providing thought leadership and policy advice on the social, legal, political and economic impacts of cybercrime and threats to cyber security.

The Centre for Internet Safety is hosted within the Faculty of Law at the University of Canberra. The University of Canberra is Australia's capital university and focuses on preparing students for a successful and rewarding career.

www.canberra.edu.au/cis

[1] Centre for Internet Safety. Cyber White Paper Submission. http://www.canberra.edu.au/cis/storage/Centre%20for%20Internet%20Safety%20Cyber%20White%20Paper%20Submission.pdf [November 2011]

Data Breach and Loss of Personal Information

A privacy breach is the result of unauthorised access to, or collection, use or disclosure of, personal information. Proper data breach management (that results in a privacy breach), including notification where warranted, will assist government and private sector organisations in retaining the trust of the individuals whose information is improperly released and help them to protect themselves.[2]

It is increasingly common to hear news reports of data breaches of well known and trusted consumer brands resulting from information security failures. Notable examples include Sony with the loss of over 77 million personal records and Heartland Payment Systems with the loss of over 130 million credit and debit card numbers. But it is not just these large compromises that should be concerning: data breaches of varying sizes occur many times a day in Australia, directly affecting the welfare of Australians.

In fact, a privacy breach occurs when an individual's personal information is accessed, collected, used or disclosed in contravention of applicable privacy legislation or and organisation's privacy policy. The definition of such a breach should complement the proposed definition of personal information suggested in the proposed Bill at Schedule 1, subsection 6(1) where it says:

> [P]ersonal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable:
>
> (a) whether the information or opinion is true or not; and
>
> (b) whether the information or opinion is recorded in a material form or not.

A loss of personally identifying information arising from a privacy breach can expose individuals to risks such as embarrassment, loss of employment or business opportunities, personal safety and identity theft. These risks can have significant consequences for Australian consumers with the impact lasting many years.

Under existing Australian law, government agencies and organisations are not required to notify individuals when their personal information has been compromised. Too few organisations are prepared to respond to a privacy breach when it happens. Too many naively believe a privacy breach will not happen to them.

Australian Privacy Principle (APP) 11 deals with the security of personal information. The proposed Bill at Part 4 states:

> If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information:
>
> (a) from misuse, interference and loss; and
>
> (b) from unauthorised access, modification or disclosure.

The use of the word 'reasonable' is insufficient to ensure action. We therefore recommend APP 11 be bolstered with additional wording compelling APP entities to report a loss of personal information to the Privacy Commissioner and inform all data owners in a timely manner.

---

[2] Centre for Internet Safety. Privacy and the Internet: Australian Attitudes Towards Privacy in the Online Environment. http://www.canberra.edu.au/cis/storage/Australian%20Attitutdes%20Towards%20Privacy%20Online.pdf [May 2012]

There is significant community consensus for such reporting: In 2012 the Centre for Internet Safety partnered with eBay.com.au to survey eBay users about their attitudes towards privacy and how it affects their actions online. The survey was conducted in March 2012 and comprised of a representative sample of 700 Australians who visited eBay in the past 12 months. The survey revealed 85% of respondents wanted mandatory data breach for private businesses.[3]

Data breach legislation needs to create an actionable regime for organisations to inform their customers in the event of a breach of privacy with a notice which needs to be consistent how the organisation normally communicates with its customers and include the type of personal information exposed and a description of what happened. It must be actionable so that remedy steps can be taken.

The Australian economy would be healthier if consumer confidence was based on a more transparent knowledge of how their data is collected, stored, used and potentially lost or stolen.

Functions and Powers of the Information Commissioner

Presently, when the Office of the Australian Information Commissioner (AOIC) conducts an own motion investigation into an alleged privacy breach, there is no penalty or other sanction that can be imposed upon release of their finding/s.

We believe there is a continued threat to privacy while there are no sanctions arising from "own motion" actions of the Privacy Commissioner. This in turn will allow public trust to continue to erode. We therefore recommend a civil sanction process whereby the Privacy Commissioner is able to ask a civil court to impose 'penalty units' arising from privacy breaches proven on the balance of probabilities. The imposition of such penalty units could be categorised in a sliding scale from accidental breaches; a failure to implement and follow privacy policies and procedures; through to deliberate violation with harmful intent.

In addition, we believe the Privacy Commissioner's office is insufficiently staffed and we therefore call for adequate staffing of the Privacy Commissioner's office to reflect the volume and seriousness of investigations required to maintain public confidence in a modern information age.

[3] ibid.