Online Privacy and Data Retention Controversy in Australia

A white paper by http://www.crucial.com.au/
April, 2015

Table of Contents

1. Introduction: privacy concerns in the internet age

"The cyber threat is not new. Cybercrime is just crime. Cyber espionage is just espionage. Cyber hacktivism is just activism and protest. So while the threat itself isn't new, cyberspace allows crime, espionage and protest to happen at a pace and scale that is unprecedented."

Telstra Cyber Security Report

Although primarily associated with increased information availability and facilitated global communications, the widespread use of the Internet also has given rise to new forms of privacy and security threats whose impact could be devastating for organizations and individuals alike. Even with the advancements in security systems, online privacy concerns have never faded in importance. On the contrary, they are only strengthened by the earlier revelations on governmental data monitoring practices in the USA, which gave a more serious tone to all the related discussions.

Thus, in the post-Snowden era, as some people refer to the level of internet privacy awareness the world seems to have reached, new privacy regulations are needed to enable everyone to use the web without fearing for their private data safety. At the same time, however, the increased volume of cyber-attacks requires new measures for handling increasingly sophisticated and aggressive forms of cyber-crime.

This is why national security and law enforcement agencies all over the world are taking drastic steps to improve their methods of fighting cyber-attacks. Such attempts, however, most frequently are regarded as an intrusion of individuals' privacy, as is the case with the new data retention legislation in Australia. Namely, Australian parliament recently passed a bill that inspired a great degree of controversy due to the fact it tackles the highly sensitive issue of online privacy. While on one hand intended to provide critical information for law enforcement agencies to fight cyber-crime, the bill imposes some questions regarding citizens' privacy, on the other. Therefore, it comes as no surprise that this legislation caused new concerns among Australian's, who partly see it as a way for government agencies to spy on citizens' online activities.

Considering the available data related to the legislation, this white paper aims to clarify its details and consider the possible effects it could have on the general security and privacy of the people in Australia.

2. Introducing data retention plan in Australia

Following many other countries that made an attempt at regulating the access to the information on people's online behaviour, Australian parliament recently passed a bill that obliges

telecommunications providers to keep customers' communication metadata for two years. The *Telecommunications (Interception and Access) Amendment (Data Retention) Bill* was first introduced late in 2014 with a goal of equipping law enforcement and security agencies with resources necessary for identifying and preventing criminal activities online. The Bill passed Parliament late in March 2015, while on April 13th 2015 it finally received Royal Assent.

2.1. Legislation and goals

According to the information published on the Australian Government's website, the primary reason for taking this step lies in the fact that "metadata plays a central role in almost all serious criminal and national security investigations," which is why law enforcement and security agencies need to be able to "lawfully access this kind of data in connection with their investigations." In an interview following the introduction of the Bill in October 2014, Communications Minister Turnbull, explained why this is central for government's attempts to fight cyber-terrorism and cyber-espionage. He noted that such practices historically have yielded positive results and gave an example of a current child exploitation investigation that was unable to identify a number of potential suspects only because the internet service providers did not retain the necessary metadata.

> *"Illegal downloads … cyber-crimes, cyber security, all these matters, our ability to investigate them is absolutely pinned to our ability to retrieve and use metadata."*

Considering the pace at which the number of criminal activities online increases, it is evident that certain regulations regarding this need to be introduced on the national level. However, the root controversy revolves around the fact that such a law at the same time implies a greater control over people's private online activities, which was a subject of criticism ever since the initial plan was crafted.

2.2. Facts and details

As of October 2015, licensed carriers, carriage services, ISPs and certain telecommunications service providers in Australia will be required to retain specific communications metadata for two years. Metadata is defined as "information about communication" that reveals *who*, *when*, *where* and *how* communicated. As specified by the bill, the types of data that will be collected are:

- identity of the subscriber to a communication service
- the source of the communication
- the destination of the communication
- the date, time and duration of communication
- the type of communication

- the location of the equipment used in communication (such as LTE, ADSL, Wi-Fi or VOIP)

Metadata of a phone call, for example, is the information on the phone numbers included in the communication and the length of the call, while contents of the message are excluded. The same goes for all the online messages, whose contents will never be kept in any form. Data safety is further ensured through a set of safeguards that aim to:

- limit the range of agencies permitted to access the data
- regulate oversight of the agencies by Commonwealth Ombudsman
- introduce new reporting requirements for the Attorney-General's Department
- introduce a new journalist information warrant regime
- establish Public Interest Advocates (PIAs), who are entitled to make submissions on journalist information warrants
- require mandatory review of the data retention scheme by Parliamentary Joint Committee on Intelligence and Security (PJCIS)

2.3. Privacy concerns

Although the Bill is essentially conceptualized as a way to improve national cyber-crime investigation strategies, it has had a variety of opponents ever since it was first proposed. Back in November 2014, when the move was officially announced, the Parliamentary Joint Committee on Human Rights raised concerns about possible limitations to people's right to privacy. Namely, despite the fact contents of the message would not be kept, the pieces of data that will be collected can reveal sensitive information about individual users.

> *"These categories of data may provide significant identifying details about an individual, and therefore may significantly limit an individual's right to privacy. For example, the time of a communication and the location of communications equipment alone would provide significant details about an individual's life."*

More specifically, even without the content, communications metadata can reveal information related to a person's political attitudes, sexual preferences and religious concerns, which is why the Committee has suggested multiple amends to the Bill. The Bill was finally adopted with the suggested amends, but it still seems to lack some specific safeguards and this is why different reactions to it could be heard.

3. Reactions and implications

After the bill was passed, the news did not resonate well with some of the major media in Australia and beyond. Most security and web analysts agreed with the view that the Bill essentially represents an intrusion of people's privacy, which is a fundamental right of everyone. Warrantless access to data that may reveal a set of sensitive information is certainly a major issue that inspired such emotional reactions in the first place.

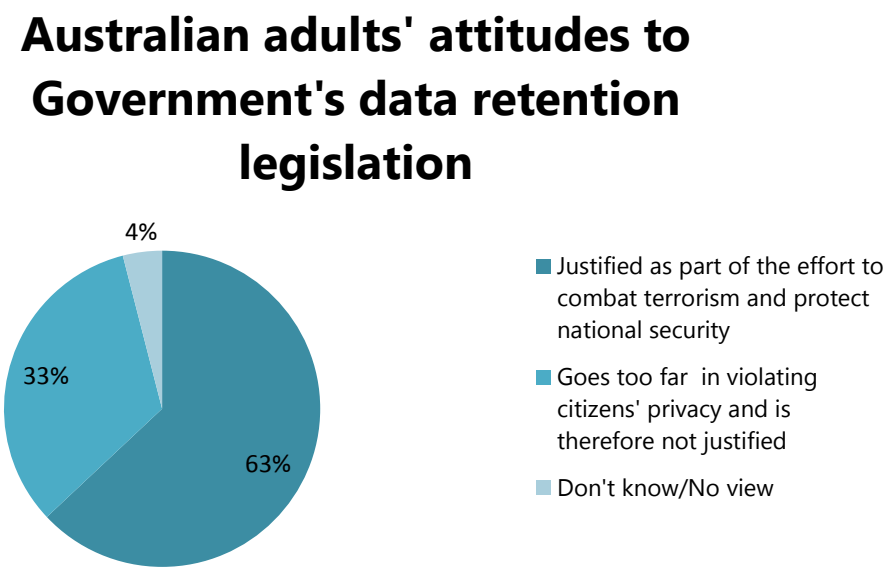
3.1. Media voices

Similar to the Parliamentary Joint Committee on Human Rights, most media representatives judged this decision as an intrusion of individual's privacy. Moreover, specific groups of professionals found that the plan would significantly affect their work. This is the case with Law Institute Victoria that expressed concerns about the safety of lawyers' communications with their clients and outlined a set of questions that the bill does not answer. These questions are mostly concerned with the control of data sets and agencies that have the access to them, legitimate purpose of the data retention scheme, as well as technical issues regarding precise way to filter metadata from whole messages.

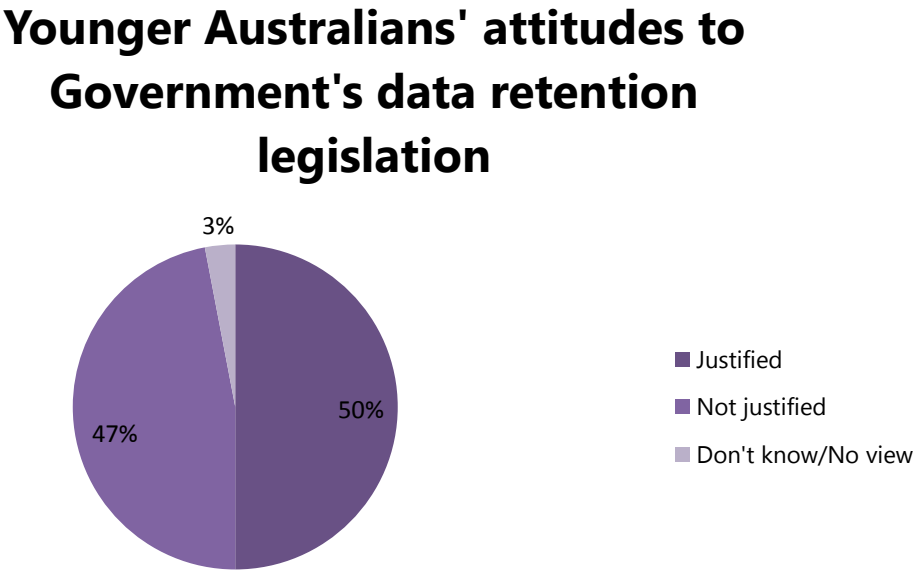
Additionally, journalists and news organizations criticized the move, especially before the specific amends that regulate access to journalists' data were added to the Bill. Although amends that require "journalist information warrant" were added, many people still question their efficiency. In a media release from March 20th, Angela Daly of Swinburne University of Technology and Adam Molnar of Deakin University explained that obtaining a warrant for accessing journalists' data will be relatively easy, which is why they argue this should not be taken as a proper safeguard. Moreover, they also point to possible circumventions of the requested procedures, meaning that the specified safeguards cannot do much to actually stop law enforcement agencies from accessing journalists' data.

3.2. Citizens' perspective

Despite the relevant arguments by media representatives and security specialists, citizens of Australia seem to have a different perspective on the issue. Namely, in a recent research by Lowy Institute, which is based on a nationally representative telephone survey of 1,200 Australian adults, majority of respondents (63%) believe data retention legislation is justified.



When it comes to younger populations (aged 18-29), there is a slightly greater tendency to see the legislation as not justified, which is the case with 47% of respondents.



Such a discrepancy may be attributed to the fact that younger generations previously showed greater awareness of the internet privacy regulations, as shown in different global reports. Namely, millennials and digital natives mostly believe that no one should be able to access their personal data.

Paradoxically, however, they are also more willing to "trade" their personal information if offered something in return. Namely, University of Southern California Annenberg Centre showed that 70% of millennials and 75% of people aged 35 and over say that no one should be able to access their personal data on web behaviour, while 51% of millennials and 40% of people aged 35 and over say they are fine with sharing information with companies if they get something in return. This clearly shows that online privacy may still be a vague concept for a great portion of internet users, who might be exposing their data to third-parties in variety of ways.

4. Understanding the online risks

As pointed out in the introduction, the main idea behind introducing such a drastic measure is an immense rise in the use of new technologies that encourage people to transfer large amounts of sensitive data via the web. Like in most countries, the use of web technologies in Australia keeps growing and so does the number of cyber-attacks.

4.1. Australian data demands

As the use of web resources becomes a more common activity among Australians, the amounts of digital data they transfer via the web grows at an astonishing rate. ACMA Communications Report for 2013-2015 suggests some impressive statistics in relation to the growth of digital data use.

- 68% of Australians accessed the Internet via three or more devices in six months
- 77% of active internet users in Australia used e-banking or paid a bill online
- 69% of Australians used social media

Translated into data volume, such a behaviour brings the following digits:

- 1,034,959 terabytes of data downloaded in the June quarter 2014 (53% up compared to the year before)
- 93% of data downloaded via fixed-line broadband.
- 1.9 GB of data downloaded per mobile user in the quarter ending June 2014

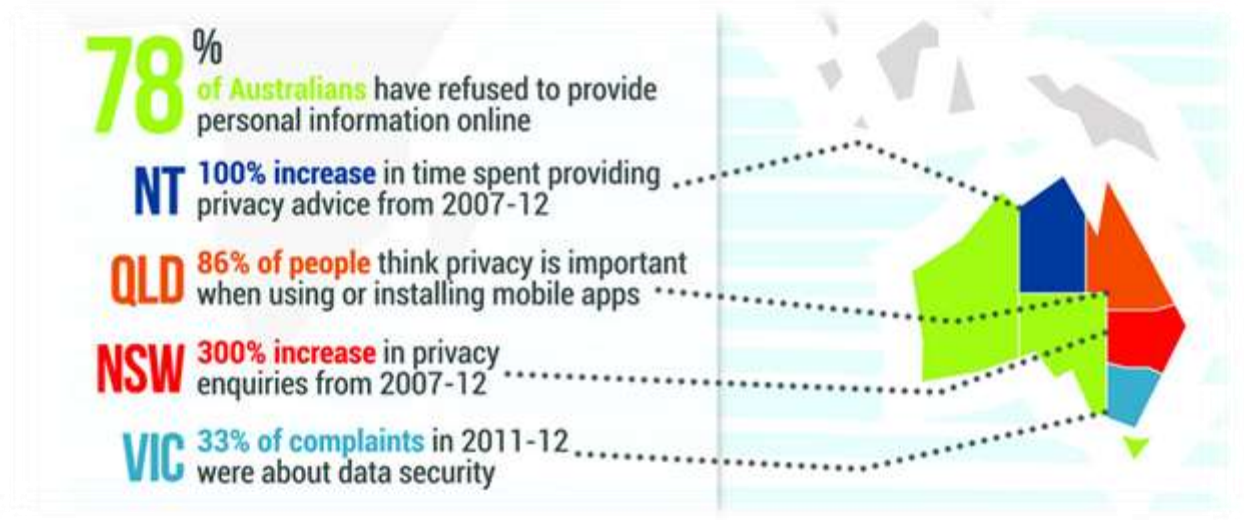
Parallel to such a great demand for web resources, the risk of data breaches grows both in individual and organizational settings. This is primarily due to the fact that hacking technologies are becoming more sophisticated, which leads to breaches even among users or organizations who actively seek to improve their protection strategies.

4.2. The state of cyber-crime in Australia

When it comes to the average degree of online risk web users are exposed to, multiple global and regional surveys suggest that industries are seeing a rapid growth in the number of data breaches. As the web technologies become more mature, hackers seem to use increasingly sophisticated methods to obtain both personal and corporate data. Perhaps more strikingly, cyber-crime in forms of hacktivism, cyber-terrorism and organized crime further question the state of cyber security and imply new standards for maintaining the internet privacy.

4.2.1. Individual web users

When it comes to individuals' online privacy, global reports reveal growing concerns. In a report by TRUSTe, for example, 86% of US web users said they have taken active steps to protect their privacy, which demonstrates that they are not only concerned about the issue, but also ready to adopt some practices for safer browsing. In Australia, online privacy awareness seems to have reached a peak in the last few years. Recent surveys suggest that 78% of Australians have refused to provide personal information online, which only points to the fact they no longer trust online portals as much.



Source: http://www.privacyawarenessweek.org/

Despite the great awareness of online security risks, individual web users in Australia often fall victims of cyber-attacks. As reported in a 2013 survey on identity crime and misuse in Australia, one in five people have been victims of computer hacking or fraudulent online banking and shopping activities. By comparison, Experian research of UK adults' computer security practices reveals that 86% of respondents in this country have fallen victim of cyber-crime, which is also partly related to the increased use of insufficiently protected mobile devices. Therefore, it is evident that some greater

efforts need to be made in terms of educating individuals on the best online security practices and this also poses questions on their ability to properly judge privacy risks and protect themselves.

4.2.2. Businesses

In the business realm, the issues of data security and privacy have always been much more sensitive given that the number of attacks has grown substantially over the last few years. In support of this view, CERT Australia Cyber Crime and Security Survey, which examined how companies and organizations across the country handle security internally, found out that out of 135 partner businesses surveyed, the number of cyber security incidents reported climbed from 56 organizations in 2012 to 76 organisations in 2013. Interestingly enough, the number of those that chose not to report cyber security incidents to an outside agency also grew - from 44% in 2012 to 57% in 2013. Nevertheless, agencies across Australia are clearly facing attacks more frequently, which justifies their concerns related to cyber-crime.

4.2.3. Hacktivism and cyber-espionage

Over the last few years, Australian organizations have been a target of hacktivist attacks multiple times, which only emphasizes the need to introduce some harsher measures for handling such threats. Some of the most important events related to this are the attack on the website of Federal Government back in 2010, which was a form of protest against internet filtering legislation. Somewhat more aggressively in 2012, hacktivists stole and published data held by Australian telecommunications providers to protest against new national security laws. As pointed out in Telstra Cyber Security report, such events make it evident that "modern cyber attackers are frequently well resourced, highly organized and determined," which is what makes cyber-crime more commonplace.

5. Conclusions

The extent to which an average person today uses web resources creates an ecosystem in which extensive amounts of intimate data are stored or transmitted online. Introducing any form of control over such data is justifiably a great concern for the nation and this is why such attempts could potentially have large-scale effects on how we see the freedoms of the online space. In relation to the data retention legislation in Australia, this means that despite its "noble" goal, the question of the exact way an average internet user might be affected by it remains.

Resources:

2015 TRUSTe US Consumer Confidence Index. TRUSTe.
https://www.truste.com/resources/privacy-research/us-consumer-confidence-index-2015/

ACMA Communications Report 2013-2014.
http://www.acma.gov.au/theACMA/engage-blogs/engage-blogs/researchacma/Australians-appetite-for-data-and-content-continues-to-grow

Australia a growing source of DDoS attacks as well as a target, Arbor warns. CSO.
http://www.cso.com.au/article/565022/australia-growing-source-ddos-attacks-well-target-arbor-warns/

Cyber Crime and Security Survey Report 2013. CERT Australia.
http://apo.org.au/research/cyber-crime-and-security-survey-report-2013

Data Retention. Australian Government Attorney General's Department.
http://www.ag.gov.au/dataretention

Data retention: Journalists decry 'Stasi-like surveillance state.' Computerworld.
http://www.computerworld.com.au/article/564804/data-retention-journalists-decry-stasi-like-surveillance-state/

Examination of Legislation in accordance with the Human Rights (Parliamentary Scrutiny) Act 2011. Parliamentary Joint Committee on Human Rights.
http://www.aph.gov.au/~/media/Committees/Senate/committee/humanrights_ctte/reports/2014/15_44/15th%20Report.pdf

Government's Data Retention Scheme has Clear Majority Support from Australians. Lowy Institute.
http://www.lowyinstitute.org/news-and-media/press-releases/governments-data-retention-scheme-has-majority-support-australians

Identity Crime and Misuse in Australia. Australian Institute of Criminology, May 2014.
http://aic.gov.au/publications/current%20series/rpp/121-140/rpp128.html

Infographic: Technology is changing. Privacy Awareness Week.
http://www.privacyawarenessweek.org/resources/infographic-tech-is-changing/tech-is-changing-en.jpg

Millennials Graphic. University of Southern California Annenberg Center.
http://annenberg.usc.edu/News%20and%20Events/News/~/media/news/big/Millennials_Graphic.ashx

One in Six Adults has Fallen Victim to Cyber-Crime. Experian.
http://www.experian.co.uk/blogs/latest-thinking/one-six-adults-fallen-victim-cyber-crime/

Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014. Law Institute Victoria. http://www.liv.asn.au/data-retention

Telstra Cyber Security Report 2014. Telstra. http://www.telstra.com.au/business-enterprise/download/document/telstra-cyber-security-report-2014.pdf