Hacking The Grapevine

Data Retention and protecting Australian consumer privacy

David Seidler

Google – ACCAN Internship Program

June 2014

Hacking The Grapevine: Data Retention and protecting Australian consumer privacy

Authored by David Seidler

Published in 2014

DISCLAIMER: The views and opinions expressed in this report are the author's own.

The operation of the Australian Communications Consumer Action Network is made possible by funding provided by the Commonwealth of Australia under section 593 of the *Telecommunications Act 1997*. This funding is recovered from charges on telecommunications carriers.

Australian Communications Consumer Action Network
Website: www.accan.org.au
Email: info@accan.org.au
Telephone: 02 9288 4000
TTY: 02 9281 5322

ISBN: 978-1-921974-22-9

This work is copyright, licensed under the Creative Commons Attribution 3.0 Australia Licence. You are free to cite, copy, communicate and adapt this work, so long as you attribute the author(s).

This work can be cited as: Seidler, D. *Hacking the Grapevine: Data Retention and protecting Australian consumer privacy*, Australian Communications Consumer Action Network, 2014

Table of Contents

Executive Summary

This research report is designed to inform the development of a consumer perspective on the issue of data retention in the telecommunications industry. In this context, data retention refers to the collection and storage of metadata over some time. Metadata for phone calls includes duration, location and numbers. For emails metadata includes sender and receiver addresses and the date and time of the communication.

The most recent Australian government proposal recommended a system of bulk collection of metadata for all Australian communications. Some metadata is already collected by telecommunications service providers (telcos) for business purposes. The proposal, however, would make such retention mandatory across all communications for a period of two years. A 2012 parliamentary inquiry established to determine whether Australia should introduce such a system failed to offer a solid conclusion. The topic is now being reconsidered with a Senate inquiry due to report on 27 August 2014.

This report seeks to examine the arguments for and against data retention in an effort to inform the consumer movement about an issue which has typically been debated by others but ultimately, significantly impacts them. For the most part, law enforcement and national security agencies are in favour of a data retention system. These agencies suggest that collecting metadata is essential to their operational effectiveness. In contrast, industry and civil liberties groups characterise data retention as unnecessary and expensive, as well as a threat to the privacy of telco consumers.

The consumer role in the data retention debate has been historically limited, perhaps because consumers have not always been particularly cognisant of or concerned by threats to their communications privacy. Revelations around the US National Security Agency (NSA) and its previously classified surveillance programs have changed that as privacy, and particularly government and corporate interactions with personal information, have become a major talking point. Recent survey data shows that Australian consumers are uncomfortable with the idea of their activities being monitored and concerned about how any information retained is handled. Especially in the wake of the European Union's rejection of data retention laws in April 2014 and the US attempt to scale back the NSA's surveillance after public outcry, advocates for data retention in Australia face a difficult task.

If law enforcement is to win the war over data retention, they will need to claim victory in the battle over the distinction between *metadata* and *content*. Law enforcement traditionally try to uphold the distinction, suggesting that metadata is inherently less private, less sensitive and therefore less vulnerable to abuse than the content of communications. Viewing metadata in this way, the other law enforcement arguments in favour of data retention become easier to accept. Chief among these arguments is the usefulness of metadata in the early stages of investigations. Even where metadata is less private, agencies argue that it can help to build a baseline profile of a criminal suspect and their network of associates. Given the long-term nature of many investigations, collecting this data over two years is said to be reasonable, particularly when combined with appropriate existing oversight of their access to it. Law enforcement contends that the introduction of a variety of new communications technologies means that this vital metadata is often not available to them. They argue mandatory data retention is the only way to ensure operational efficiency in the national interest.

Opponents of data retention paint a very different picture. They argue that there is no inherent difference between metadata and content, pointing to a range of research studies which indicate that big data analysis has provided the tools to effectively collapse the distinction between metadata and actual content. Metadata can be used to reveal sensitive personal information including medical conditions, financial connections and political affiliations. More importantly, mandatory data retention becomes a proposition inherently fraught with risk, particularly where network security cannot be promised by the telcos storing the metadata. Opponents argue that law enforcement agencies have not been able to establish evidence of their need for metadata. A range of practical issues also plague the proposal, including who will pay for a data retention system and whether the cost is passed on to consumers. There is the further issue of how a complaints system already under-resourced and offering inconsistent outcomes will cope with an influx of new consumer complaints around data retention.

Key findings and recommendations

Taking into account the arguments underscoring this highly contentious issue:

- A mandatory data retention proposal should not be supported. In the absence of statistical evidence of the need for such a system, security, cost and oversight issues make its introduction unwarranted.
- If law enforcement agencies cannot operate without metadata on criminal suspects, a data preservation system, targeting these suspects' metadata, is a workable alternative to fully-fledged data retention.
- Regardless of whether a data retention system is introduced, existing consumer privacy protections should be improved. This would involve the introduction of greater controls over current access to metadata (including the establishment of an independent, external oversight body), a system which would notify consumers when their personal information is compromised and ideally, a Consumer Privacy Bill of Rights.
- The existing complaints system also needs to be improved. However, the focus should not be purely on reactive measures but preventing privacy breaches in the first instance through expanding consumer education, building greater privacy protections into network and software architecture and allowing consumers to request that personal information they have provided be de-identified or destroyed.

Introduction

Just over a year ago, most people had never heard of the NSA, Edward Snowden or the term 'metadata'. The Attorney-General's Department under the then-Labor government had floated the idea of a data retention program which would see metadata including caller, receiver, call times and various Internet-usage information kept by telecommunications companies for up to two years. However, a parliamentary committee contemplated the issue and delivered no firm conclusions.[1]

What a difference a year makes. The June, 2013 Snowden leaks and attendant revelations about the United States' National Security Agency's (NSA) clandestine mass electronic surveillance program (known as PRISM) put telecommunications privacy back on the agenda of politicians, law enforcement agencies and concerned consumers. Federal Parliament's Legal and Constitutional Affairs References Committee is currently conducting a comprehensive revision of Telecommunications (Interception and Access) Act 1979[2] - the most concrete attempt to resolve the Australian position on the issue. [3]

The purpose of this research report is to thoroughly examine the current telecommunications privacy landscape with a particular focus on the status and viability of a data retention regime for metadata. Metadata is what can be described as data about data. For phone calls, metadata includes duration, location and parties' numbers. For emails, metadata includes sender and receiver addresses and the date and time of the communication. The first part of the report will serve as a brief overview of the current telecommunications privacy legislative environment, as well as utilising available survey data to offer an assessment of Australian public opinion. The second part of the report will explore the policy history, definitional quandaries and arguments for and against a mandatory data retention system. Finally, a number of focused recommendations regarding striking the appropriate balance between national security and consumer privacy will conclude the report.

By analysing support for a data retention regime and investigating the policy and practical motivations underpinning these positions, this report is designed to inform the development of a consumer perspective on data retention in the telecommunications industry. As the fallout from the Snowden leaks continues and governments around the world alternately shore up or scale back their retention programs, Australia now stands on the brink of a major policy shift on data privacy. Knowing the landscape, understanding the policy debates and critically evaluating the alternative positions will be essential for the consumer movement if it wishes to play an integral part in shaping the development of data retention policy in Australia.

Background to Privacy

What is privacy?

Before engaging with some of the finer elements of the data retention debate, it is worthwhile taking a step back to consider the core concept at the heart of much of the intellectual and political

[1] Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation,* (2013) (hereafter 'PJCIS Report').
[2] Hereafter 'TIA Act'
[3] Legal and Constitutional Affairs References Committee, Parliament of Australia, *Comprehensive Revisions of the Telecommunications (Interception and Access) Act 1979,* 2014 (hereafter 'LCA Inquiry').

hand-wringing on the subject. Although explicitly protected in a number of international legal documents,[4] the concept of privacy suffers from significant definitional problems. It can occur in different contexts and give rise to a range of different issues which do not readily conform to one single, stable definition. All legislatures confront an enduring challenge in fashioning legal protection that can comprehend social, technological and cultural variations of privacy.

While definitions are numerous, the broad explanation of privacy proposed by Warren and Brandeis in their seminal Harvard Law Review article on the subject continues to find favour, articulated as "the right to be left alone."[5] Trying to give shape to that expansive description, social psychologists have more recently described privacy as a "boundary regulation process whereby people optimise their accessibility along a spectrum of 'openness' and 'closedness'." [6] Similarly, Columbia Law Professor Alan Westin conceptualised a "personal adjustment process" which involves individuals balancing "the desire for privacy with the desire for disclosure and communication" in the context of social and environmental circumstances.[7]

Today, achieving a stable definition of privacy is increasingly difficult as our interactions with the Internet and other telecommunications technologies blur the boundaries between public and private spheres. For the purposes of this report, however, the concept we are concerned with – data privacy – has been given some structure by law professor Daniel Solove. Drawing a distinction between 'access control' and 'risk management', Solove identifies the key privacy concerns central to the data retention debate: consumers want both control over their personal information and some commitment from those companies with which they share this information to minimise future privacy risks once this data is no longer under their direct control.[8] The prospect of a data retention regime particularly threatens that second concern as ensuring the privacy of personal information becomes more difficult the longer the data is required to be stored.

Contemporary context

During both the research and writing stages, the author found that fast moving events could have turned this report into an exercise of chasing after headlines. To ensure this report does have lasting value, particular instances of data breaches, public indignation and government responses will not be examined at length here. Suffice to say that recent media coverage and concern over large-scale breaches of critical Internet cryptography protocols,[9] the potential exposure of Australian citizens' private government records,[10] the monitoring of public servants' social media usage,[11] and a

[4] See, eg, *International Covenant on Civil and Political Rights* (Article 17); *Universal Declaration of Human Rights* (Article 12); *European Convention on Human Rights* (Article 8).
[5] Samuel Warren and Louis Brandeis, 'The Right To Privacy', (1890) 4 Harvard Law Review 193.
[6] Irwin Altman, *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding* (Brooks/Cole Publishing Company, 1975), p.18.
[7] Alan F. Westin, *Privacy and Freedom* (Atheneum, 1967), p.7.
[8] Daniel Solove, 'A Taxonomy of Privacy', (2006) 154 University of Pennsylvania Law Review 477.
[9] Reuters, 'Heartbleed bug found in OpenSSL software prompts tech companies to urge passwords reset', *ABC News* (online), 10 April 2014, http://mobile.abc.net.au/news/2014-04-10/heartbleed-bug-password-reset-data-openssl/5379604.
[10] Ben Grubb and Noel Towell, 'Australians' private government details at mercy of hackers, say IT security experts', *Sydney Morning Herald* (online), 28 April 2014, <http://www.smh.com.au/it-pro/government-it/australians-private-government-details-at-mercy-of-hackers-say-it-security-experts-20140427-zqzkg.html>. Also, note the government's "appalling response" to the revelations: Ben Grubb, 'Revealed: serious flaws in myGov site exposed millions of Australians' private information', *Sydney Morning Herald* (online), 15 May,

significant leak of the personal information of asylum seekers[12] indicates that the topic is front of mind for many Australians.

Australian telco users, their privacy attitudes and behaviours

Users

The increasing number of users and the increasing frequency of use of telecommunications have meant that privacy issues now necessarily implicate more people than ever. Across both traditional telephony and Internet subscriptions, the latest ACMA Communications Report (2012-2013) has indicated that the uptake of telecommunications services continues apace in Australia. [13] While the number of fixed-line telephone services is down a quarter of a million to 10.32m over the two years to June 2013, the gap has been plugged by a growth of mobile services, increasing 1.8m in the same period to 31.09m.

The increase in mobile usage mirrors a 13% increase in Internet subscriptions from June 2012 to June 2013, much of which is being driven by mobile handset subscribers. Although no information on call or text message volumes is made publicly available, the Australian Bureau of Statistics does publish statistics on data downloaded. For the three-month period to December 2013, the total volume of data downloaded amounted to 888,547 terabytes with mobile handset downloads accounting for 27,627 terabytes of that (increases of 55% and 101% respectively over two years).[14] Taken together, these numbers reflect generally a growing number of Australians adopting telecommunications services and particularly, a surge in Internet use on mobile phones. This increase in telecommunications use across the board hints at the scope of a data retention regime and its implications for the Australian public.

Attitudes and behaviours

The development of attitudes towards privacy has been the subject of myriad research studies in fields as diverse as economics, computer science and social psychology. Just as a stable definition of privacy continues to elude legislative drafters, so too is conclusively explaining why consumers act in certain ways with regard to their privacy a difficult proposition.

An influential 1967 study by Columbia's Westin helped outline three privacy typologies for consumers.[15] A popular contemporary narrative is that of the apathetic consumer, either indifferent

---

2014, <http://www.smh.com.au/it-pro/security-it/revealed-serious-flaws-in-mygov-site-exposed-millions-of-australians-private-information-20140515-zrczw.html>.

[11] Nick Towell and Amy McNeilage, 'Facebook feud fires alarm over public service snoop plans', *Sydney Morning Herald* (online), 11 April 2014, <http://www.smh.com.au/federal-politics/political-news/facebook-feud-fires-alarm-over-public-service-snoop-plans-20140410-36g42.html>.

[12] Oliver Laughland, Paul Farrell and Asher Wolf, 'immigration Department data lapse reveals asylum seekers' personal details', *The Guardian* (online), 19 February 2014, <http://www.theguardian.com/world/2014/feb/19/asylum-seekers-identities-revealed-in-immigration-department-data-lapse>.

[13] Australian Communications and Media Authority (ACMA), *Communications Report 2012-13,* <http://www.acma.gov.au/~/media/Communications%20Analysis/Comms%20Report%202012%2013/PDF/ACMA%20Communications%20report%20201213_WEB%20pdf.pdf>.

[14] Australian Bureau of Statistics, *Internet Activity, Australia, December 2013* (2013) <http://www.abs.gov.au/ausstats/abs@.nsf/Lookup/8153.0Chapter8December%202013>.

[15] Alan F. Westin, *Privacy and Freedom* (Atheneum, 1967).

to protecting their privacy[16] or else unable to control an impulse to reveal.[17] Westin would categorise these consumers as 'unconcerned'. Assigning somewhat more agency to consumers, 'privacy economics' researchers suggest that at least in an online setting, individuals see the disclosure of private information in return for services as part of a transactional negotiation.[18] Westin would call these consumers 'pragmatists'. Finally, Westin points to a third group, the 'fundamentalists', who always favour privacy above all else.

While some have characterised Westin's taxonomy as too limited and sought to add new categories of user,[19] a recent Office of the Australian Information Commissioner (OAIC) report suggests that Australian attitudes to privacy are still more varied.[20] Ultimately, attempting to demarcate distinct attitudes towards privacy among Australian telecommunications consumers appears a futile enterprise, especially considering how rapidly social and technological factors are changing in the space.

All that said, there are certain statistics in the 2013 OAIC Community Attitudes to Privacy report that are particularly relevant to the data retention discussion and so are worth mentioning here briefly:

- *The monitoring of online activities remains a major concern for Australian Internet users.* The survey asked respondents whether they would consider an organisation monitoring their activities on the Internet without their knowledge a misuse of personal information. While the same precise question was not asked in 2007 but rather split between government (86%) and business (96%) organisations, the average result in 2013 (93%) was still higher than the 2007 average (91%). Notably, the study collected survey data in the immediate aftermath of the Snowden leaks which might have had some impact on these results. [21]
- *There is some disparity between users' expectations around the collection of information but many Australians are uncomfortable with the prospect of collection in the first instance*. While there is no clear conclusion among Australians regarding whether all (28%/29%), most (42%/32%) or only some (17%/16%) websites or smartphones collect information on users, a significant 78% of those surveyed indicated that they were either somewhat uncomfortable or very uncomfortable with the idea of databases of this information being created in the long-term.
- *More generally, anxiety regarding the handling of personal information increased markedly* (by 20%) between 2007 and 2013 with 63% of those surveyed saying they have refused to

[16] Bettina Berendt et al., "Privacy in E-Commerce: Stated Preferences versus Actual Behavior," (2005) 484 Communications of the ACM 101. See also Alan F. Westin, *Privacy and Freedom* (Atheneum, 1967); Kim Sheehan, 'Toward a Typology of Internet Users and Online Privacy Concerns', (2002) 18 The Information Society Journal 21.

[17] Katherine Strandburg, 'Privacy, Rationality, and Temptation: A Theory of Willpower Norms', (2005) 57 Rutgers Law Review 1237.

[18] Mark Ackerman, Lorrie Cranor, and Joseph Reagle, 'Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences' (Paper presented at the First ACM Conference on Electronic Commerce, Denver, November 3-5, 1999), <http://web.eecs.umich.edu/~ackerm/pub/99b28/ecommerce.final.pdf>, pp.1-8.

[19] See, eg, Kim Sheehan's suggestion of extending to four typologies: unconcerned, circumspect, wary and alarmed in Kim Sheehan, 'Toward a Typology of Internet Users and Online Privacy Concerns', (2002) 18 The Information Society Journal 21.

[20] See, eg, Office of the Australian Information Commissioner (OAIC), *Community Attitudes to Privacy 2013*, <http://www.oaic.gov.au/privacy/privacy-resources/privacy-reports/oaic-community-attitudes-to-privacy-survey-research-report-2013>, p.38 (hereafter, 'OAIC Attitudes Survey').

[21] The OAIC Attitude Survey began June 13, 2013. The Guardian announced Snowden's leaks June 5, 2013.

deal with organisations because of concerns over those organisations use of information provided.

In light of the findings of the OAIC report and the recognition that simple typologies might by now be an outdated way to categorise consumer approaches to privacy, United States President Barack Obama's words in 2012, introducing a study entitled 'Consumer Data Privacy in a Networked World' are probably best suited to conclude this section: "One thing should be clear, even though we live in a world in which we share personal information more freely than in the past, we must reject the conclusion that privacy is an outmoded value."[22]

Privacy and legislation

An awareness of the legislative environment is vital to properly comprehending the impact of a mandatory data retention regime. In this regard, consumers must contend with three distinct pieces of Commonwealth legislation: the Telecommunications Act 1997, the Telecommunications (Interception and Access) Act 1979 (TIA) and the Privacy Act 1988. Taken together, the three Acts determine both the privacy rights of Australian telecommunications consumers and exceptions to these rights. The interaction between the three, however, is not always straightforward.

The Privacy Act offers baseline protection to Australian consumers. Following the Privacy Amendment (Enhancing Privacy Protection) Act 2012 which took effect on 12 March 2014, the Australian Privacy Principles (APPs) provide 13 enforceable guidelines for both public and private sector organisations on the handling of personal information.[23]

Significantly for a data retention discussion, the Act defines 'personal information' as "information or an opinion about an identified individual, or an individual who is reasonably identifiable." Moreover, law enforcement and national security agencies (LENSAs) are often exempt from the application of the new APPs by virtue of exceptions for actions which are "authorised by or under an Australian law." Provisions of the Telecommunications Act and TIA Act authorising certain LENSA behaviour often trigger these exceptions.

As far as privacy is concerned, Part 13 of the Telecommunications Act is a legislative attempt to tailor certain aspects of the Privacy Act to the telco industry. Accordingly, the Telecommunications Act regulates the use and disclosure of information relating to the contents or substance of communications. There is significant overlap between the Privacy Act and the Telecommunication Act, although the latter protects a slightly broader range of information than 'personal information' as defined under the Privacy Act, extending to include metadata where a person's identity cannot be reasonably ascertained. It is the collection of this metadata which is at the centre of data retention proposals.

[22] White House, *Consumer data privacy in a networked world: A framework for protecting privacy and promoting innovation in the global digital economy,* February 2012, <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>.

[23] The APPs represent the harmonisation of the Information Privacy Principles (IPPs) and National Privacy Principles (NPPs) – two distinct sets of Privacy Principles that applied to public and private sector organisations respectively until March, 2014. See http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/privacy-fact-sheet-17-australian-privacy-principles

Given the many parallels between the Telecommunications and Privacy Acts, the former is the subject of current deregulation efforts.[24] The proposed repeal of Part 13 would effectively end the Telecommunications Act's role in telecommunications privacy. Although the proposed Bill recommends that prohibitions on the disclosure of metadata to LENSAs would be retained post-repeal,[25] these provisions are in practice insignificant, circumvented by agency warrants and authorisations which have, to this point, been largely forthcoming.[26]

The TIA Act will likely remain the last bastion of industry-specific privacy protection if the repeal of Part 13 goes ahead. The TIA Act effectively regulates three types of information: communications, stored communications and metadata. With respect to the first two types, the TIA Act criminalises the interception of communications and regulates access to stored[27] communications.[28] These communications are protected by a warrant scheme for enforcement agencies seeking to access them.

Elsewhere, Chapter 4 of the Act establishes the circumstances when providing access to metadata is permitted by setting out a two-tiered program of authorisation (in contrast to a warrant regime) for existing and prospective information. [29] In this way, all forms of access to consumer communications are ostensibly monitored, either through warrants or less strict authorisation procedures.

It is evident that consumer privacy in telecommunications is protected through a fairly complex web of statutory provisions (see Fig 1) and further complicated by a supplementary industry code, enforced by the ACMA. [30]

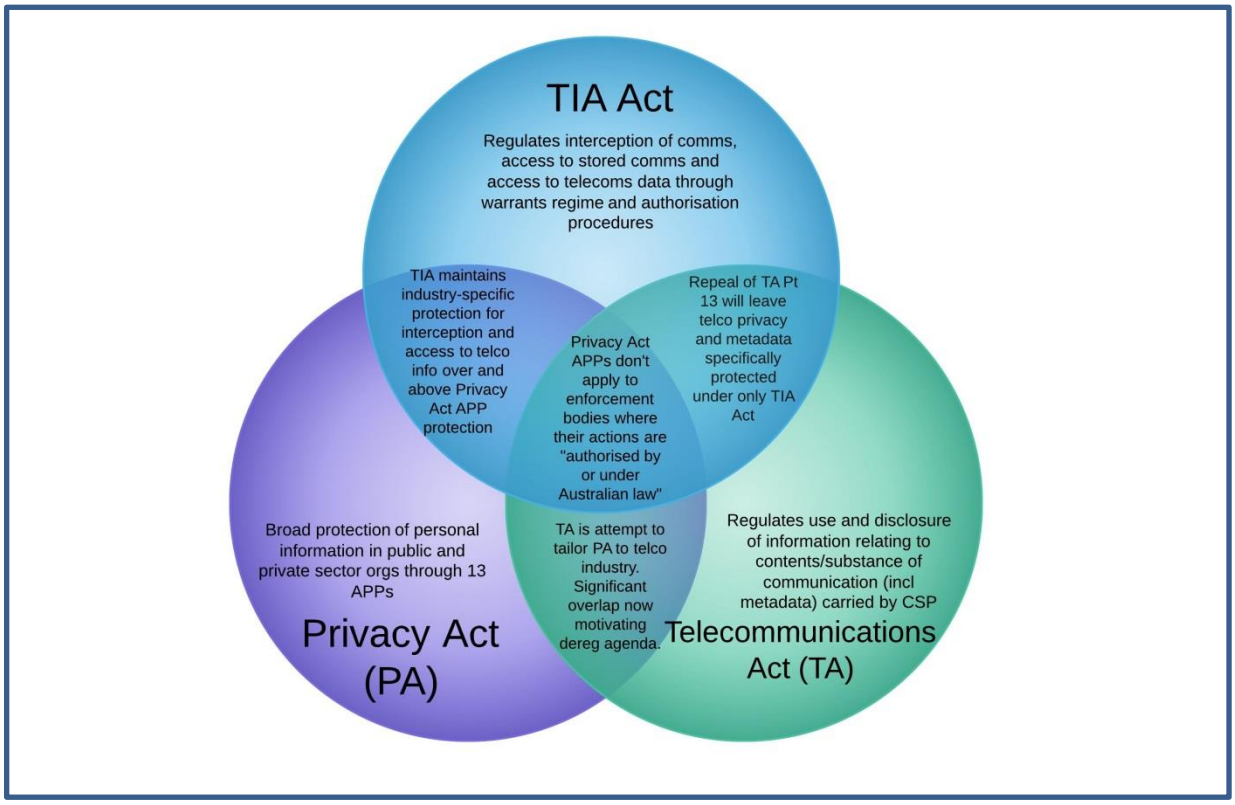
This statutory confusion was compounded by two events in 2011. The Office of the Privacy Commissioner (OPC) rebranded as the Office of the Australian Information Commissioner (OAIC) and the responsibility for privacy-related matters moved from the Department of Prime Minister and Cabinet to the Attorney General's Department. Nigel Waters, former Deputy Australian Federal Privacy Commissioner, has written that "privacy policy clearly remains an 'orphan' child with a series of temporary homes, lacking an effective champion at senior levels of government."[31]

ASIO's submission to the current Legal and Constitutional Affairs (LCA) inquiry notes a further difficulty that industry, LENSAs and consumers confront when interpreting privacy rights under the various Acts: the TIA Act and Telecommunications Act "are over 30 and 15 years old respectively and

[24] Telecommunications Deregulation Bill (No 1) 2014 (Cth).
[25] Telecommunications Deregulation Bill (No 1) 2014 (Cth) Consultation Paper, <http://www.communications.gov.au/__data/assets/pdf_file/0010/223021/Consultation_paper_-_Proposed_measures_for_the_Telecommunications_Deregulation_Bill_No._1_2014.pdf>, p.8.
[26] See 'Lack of checks and balances' section under 'Arguments opposed to a data retention proposal', below.
[27] Ie. Not passing over telecommunications systems at the time.
[28] See Chapter 2 and Chapter 3 of the TIA Act respectively.
[29] See *TIA Act* ss 175, 176 respectively.
[30] Communications Alliance, *Telecommunications Consumer Protections Code*, 2012, <http://www.acma.gov.au/webwr/telcomm/industry_codes/codes/c628-2012_tcp_code.pdf>
[31] Nigel Waters, 'Responding to new challenges to privacy through law reform: a privacy advocate's perspective' in Normann Witzleb, David Lindsay, Moira Paterson and Sharon Rodrick (eds), *Emerging Challenges in Privacy Law: Comparative Perspectives*. (Cambridge University Press, 2014), p.51.

are based on the technologies and business practices at that time."[32] The revision of the TIA Act is therefore a welcomed move.

Figure 1: The complex interaction of the three Federal privacy statutes



Mandatory data retention

What is data retention?

In the context of the telecommunications industry, data retention is the collection and storage of data for a specific period of time and for anticipated future business and legal purposes.

Data retention chiefly concerns the collection and storage of metadata. While the distinction between traditional telecommunications content and metadata is increasingly contentious, it is useful to think of metadata as the data which describes a communication. In a traditional telephony setting this might include data about the number that made a phone call, the number that received the call, the time and location where the call was made and its duration. In the context of email communications, metadata would include the sender's address, receiver's address and the date and time of the email.

It could also extend to the source and destination IP addresses of devices used in communications and the subject line of emails; however, one industry insider has suggested that Optus, Telstra and

[32] ASIO, Submission No 27 to LCA Inquiry, February 2014, p.21.

Vodafone have not historically been providing this information as part of metadata supplied to law enforcement bodies under the current legislative regime.[33]

Typically, the content of communications (eg. what is actually being typed in emails and spoken over telephones) is not collected and stored (unless there is a TIA Act warrant in force permitting that).

Current law reform situation

The 2005 Blunn Report which had as its terms of reference the review of "policy options for the regulation of access to telecommunications with particular emphasis on new and emerging telecommunications technologies"[34] is a good place to start a survey of the recent legislative reform attempts in this area. Whilst the data retention debate might be older than 2005, this date marks the first formally public effort of the Attorney-General's Department to grapple with the issue. Blunn's findings on the point were cautious and perhaps intentionally vague. He highlighted that metadata "is, and for the foreseeable future will remain, fundamental to effectively security and law enforcement" and so recommended legislatively introducing a system for the supply of this data, "subject to appropriate controls."[35]

The 2006 amendments to the TIA Act implemented many of Blunn's suggestions. The current two-tiered system for the production of historical and prospective metadata[36] outlined above is a legislative manifestation of Blunn's opinion on metadata. Under the Act, those "appropriate controls" Blunn advocated for amount to law enforcement agencies seeking authorisation for access to metadata.

Notably, these authorisations are made internally by agency Commissioners, Deputy Commissioners and other broadly defined 'authorised officers'.[37] Those agencies currently entitled to access metadata in this way include ASIO, the Australian Crime Commission (ACC) and the Independent Commission Against Corruption among others.[38] Organisations that have responsibilities for imposing pecuniary penalties or protecting public revenue can also make authorisations, greatly expanding the number of agencies with access to metadata. [39]

Reducing the number of agencies eligible to access metadata was one of the topics the Parliamentary Joint Committee on Intelligence and Security (PJCIS) canvassed in its 2012/13 inquiry into potential reforms of National Security Legislation. Its recommendation that the Attorney-General's Department review the threshold for access to metadata is illustrative of the general tenor of the Committee's report: circumspect and non-committal. Even after explicitly requesting submissions on the viability of a tailored data retention regime requiring the collection and storage

[33] Email from senior policy figure who asked not to be identified.
[34] Anthony Blunn, *Report of the review of the regulation of access to communications 2005,* <http://www.ag.gov.au/Publications/Documents/Blunn%20report%20of%20the%20review%20of%20the%20regulation%20of%20access%20to%20communications%20-%20August%202005/xBlunn%20Report%2013%20Sept.pdf>, p.3.
[35] Ibid, p.72.
[36] *TIA Act*, ch 4.
[37] *TIA Act*, s 5AB.
[38] See definition of 'enforcement agency': *TIA Act,* s 5.
[39] *TIA Act*, s 179.

of metadata for periods of up to two years,[40] the Committee concluded that the institution of a mandatory data retention regime was "ultimately a decision for Government."[41] The Australian Mobile Telecommunications Association (AMTA) CEO Chris Althaus lamented the Committee's failure to bring anything new to the table, suggesting at the time that many stakeholders' submissions had to "rely on assumptions and past debates on this subject in the absence of anything more concrete to go on."[42]

The Committee was ultimately unable to parse the arguments for and against such a system or appropriately consider many of the sensible data retention recommendations of a previous 2011 Senate Committee inquiry.[43] Senator Scott Ludlam, who initiated the 2011 inquiry and is currently sitting on the LCA inquiry, says the PJCIS report's muted response was "very unusual" given the Committee's legacy of handing down unanimous reports. This marked the issue of data retention as highly contested – a reform "hot potato."[44]

The current LCA inquiry (with the inadequate recommendations of the PJCIS included in its terms of reference)[45] should therefore strive to clarify the legislative reform agenda around data retention.

Domestic and international support

The first suggestion that a mandatory data retention scheme might be introduced in Australia came after documents obtained under Freedom of Information requests by the Pirate Party were published in the Fairfax press in 2009.[46] These documents - consultation papers seeking basic industry comment on the idea - did not necessarily signal that the government was in favour of establishing a scheme but merely sought to gauge industry sentiment. A political decision two years later would indicate that that non-partisan stance had shifted considerably. In July 2011, then Attorney General Robert McClelland met with his counterparts from the other Quintet nations – the US, UK, Canada and New Zealand – to agree to become a signatory to the Council of Europe Convention on Cybercrime. That Convention, ratified by Parliament in the Cybercrime Legislation Amendment Act 2012, calls on parties to "expedite the preservation and disclosure of traffic data [aka metadata]"[47] by adopting necessary legislative measures. Australia's assent to it suggested the government was not averse to collecting metadata for the purposes of fighting crime. The Coalition government has made no moves to alter or repeal the amendment.

---

[40] Attorney-General's Department, *Equipping Australia Against Emerging and Evolving Threats*, July 2012, <http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/additional/discussion%20paper.pdf>, p.13.

[41] PJCIS Report, above n1, p.190.

[42] AMTA, *Mobile telecommunications industry concerned about Inquiry's lack of detail on data retention,* 2012, <http://www.amta.org.au/articles/Mobile.telecommunications.industry.concerned.about.Inquirys.lack.of.detail.on.data.retention>.

[43] Senate Environment and Communications References Committee, Parliament of Australia, *Report on Inquiry into the adequacy of protections for the privacy of Australians online*, (2011), p.69.

[44] Interview with Senator Scott Ludlam (Phone interview, 23 May 2014).

[45] Originally reporting 10 June 2014. Now reporting 27 August 2014 after the Senate granted an extension of time for reporting on 14 May 2014.

[46] The documents can be viewed in their original form here: https://www.righttoknow.org.au/request/7/response/220/attach/4/R%20DR%20Industry%20Consultation%20Meetings%202009.pdf.

[47] *Convention on Cybercrime,* opened for signature 23 November 2001, CETS No. 185 (entered into force 1 July 2004), art 16.

More recently, the opinion of Attorney General George Brandis on mandatory data retention has become the subject of much speculation. It is not useful here to sift through Brandis' public statements on the issue given the ephemeral and constantly dynamic nature of the debate. That said, some particular points are worth mentioning. As shadow Attorney-General in 2012, Brandis, also a member of the indecisive PJCIS, suggested that before advancing an argument he would "examine all the issues [around data retention] carefully."[48] In late 2013, however, one of Brandis' first appointments was former ASIO chief Paul Sullivan as his chief of staff, perhaps hinting at a stronger national security focus for the Department than his previously balanced statements indicated.

The government's plan to abolish the National Security Legislation monitor[49] mirrors this promotion of the national security agenda on a whole-of-government level. Asked about data retention in recent months at a Washington D.C. policy institute, Brandis said, "The more intelligence I read, the more conservative I become."[50] Evoking the imagery acting chief executive of the Australian Crime Commission (ACC) Paul Jevtovic used giving evidence to the LCA inquiry[51], Brandis framed the discussion in the context of the fact that, "democracies fight terrorism with one arm tied behind their back."[52]

Even while Australia arguably adopts a war footing on the issue, international developments have recently undermined the legitimacy of this stance. Most significantly, the European Union introduced a Data Retention Directive in 2006 requiring member states to legislate that telcos retain metadata for between six and 24 months.[53] This very directive was used as a point of international comparison in the Attorney-General's Department submission to the PJCIS inquiry[54] and also used as evidence in the Department's submission to the current LCA inquiry.[55] After successful constitutional challenges in Germany[56], Romania[57] and the Czech Republic[58] the Court of Justice of the European Union declared the EU Data Retention Directive to be invalid on 8 April 2014. The Court reiterated

[48] David Wroe and Ben Grubb, 'Push for Australians' web browsing histories to be stored', *Sydney Morning Herald* (online), 17 march 2014, <http://www.smh.com.au/technology/technology-news/push-for-australians-web-browsing-histories-to-be-stored-20140317-34xtr.html>.
[49] Independent National Security Legislation Monitor Repeal Bill 2014 (Cth).
[50] The audio of that presentation is available here: http://csis.org/multimedia/audio-securing-our-freedoms-australian-attorney-general-george-brandis. An opinion piece for *The Guardian* ten days later saw Brandis using the same rhetoric: http://www.theguardian.com/commentisfree/2014/apr/09/the-more-intelligence-i-read-the-more-conservative-i-become.
[51] Katharine Murphy, 'Crime Commission pushes for communications data to be stored', *The Guardian* (online), 22 April 2014, <http://www.theguardian.com/world/2014/apr/22/commission-pushes-for-communications-data-to-be-stored>.
[52] George Brandis, 'Keynote Address' (Speech delivered at the Banyan Tree Leadership Forum, Centre for Strategic and International Studies, 8 April 2014).
[53] *Council Directive 2006/24/EC of 15 March 2006 on the retention of data generated in connection with the provision of publicly available electronic communications services or of public communications networks* [2006] OJ L 105/54, art 6.
[54] Attorney-General's Department, Submission No 218 to Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Inquiry into potential reforms of National Security Legislation*, 2012, p.9 (hereafter 'PJCIS Inquiry').
[55] Attorney-General's Department, Submission No 26 to LCA Inquiry, 2014, p.30.
[56] Data retention generated a perception of surveillance which could impair the free exercise of fundamental rights.
[57] Deemed incompatible with the rights to privacy and freedom of expression.
[58] Citizens had insufficient guarantees and safeguards against possible abuses of power by public authorities.

many of the same concerns as those other European courts including inadequate safeguards against abuse and a lack of criterion for access to data. It concluded that the Directive suffered from a proportionality problem: the interference with private communications was not sufficiently limited to where it was strictly necessary.[59] The decision renders the legal status of EU data retention regulations uncertain.[60] In the United Kingdom, for instance, the 2009 Data Retention (EC Directive) Regulations now effectively have no legal basis. Across the Atlantic, the full title of the United States' USA Freedom Act bill on the subject, introduced to Congress in late 2013, provides valuable insight into that country's retreat from data retention: 'Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-Collection and Online Monitoring Act'.

The Australian government, then, is left in a precarious position. Traditionally a follower, not a leader, on matters of security,[61] the government is seeing global support for data retention collapse around it just as its Parliament and law reform bodies attempt to fashion a similar program locally. Warning that "we don't necessarily borrow from the best of what is going on overseas," Senator Ludlam, a member of the current LCA inquiry, suggests that even five years after data retention first featured on the political agenda, it could still be implemented here: "It will ultimately come down to how strong the community feels and how much opposition and resistance they're able to generate."[62]

Metadata/content distinction

Just what metadata means in terms of consumer privacy is one of the key contested questions in the data retention debate. Determining an answer is essential to meeting the consumer right to be informed.[63] Part of the problem in this area is that Parliament has not been particularly helpful in proposing a workable definition of the term. Instead, the Explanatory Memorandum to the Telecommunications (Interception and Access) Amendment Bill 2007 appears to define metadata by reference to what it is not, stating that it is "information about a telecommunication, but does not include the content or substance of the communication."[64] It is this distinction – between metadata and content – that prevails in the PJCIS' recommendations[65] as well as in the submissions of the Attorney-General's Department and enforcement agencies on the matter.[66] It is this distinction which is becoming increasingly difficult to sustain.

Law enforcement worldwide has traditionally sought to distinguish metadata and content using similar language, describing content as the core communication information (the 'letter') and

[59] Court of Justice of the European Union, 'The Court of Justice declares the Data Retention Directive to be invalid' (Press Release No 54/14, 8 April 2014).
[60] Dave Neal, 'Open Rights Group presses UK ISPs on Data Retention Directive', *The Inquirer* (online), 11 April 2014, <http://www.theinquirer.net/inquirer/news/2339506/open-rights-group-presses-uk-isps-on-data-retention-directive>.
[61] Angela Daly and Sean Rintel, 'Europe says no to data retention, so why is it an option in Australia?', *The Conversation* (online), 14 April 2014, <http://www.smh.com.au/technology/technology-news/why-is-data-retention-an-option-in-australia-after-europe-says-no-20140414-zqup1.html#ixzz2yunmpPYA>.
[62] Interview with Senator Scott Ludlam (Phone interview, 23 May 2014).
[63] One of the provisions of the Consumer Bill of Rights. See http://www.presidency.ucsb.edu/ws/?pid=9108.
[64] Explanatory Memorandum, Telecommunications (Interception and Access) Amendment Bill 2007 (Cth), sch 1, Item 4, sub-s 5(1).
[65] PJCIS Report, above n1, p.226.
[66] See the submissions from ASIO, the AFP and the Attorney-General's Department to the LCA Inquiry at p.10, p.11 and p.22 respectively.

metadata as inherently less integral to the communication (the 'envelope'). Australian agencies and the Attorney-General's Department, too, have categorically diminished the privacy significance of this data by placing it in stark contrast to ostensibly far richer content, proposing that it is "less privacy intrusive"[67], "raises fewer privacy concerns"[68] and represents a "lesser level of intrusion" [69] than telecommunications content.

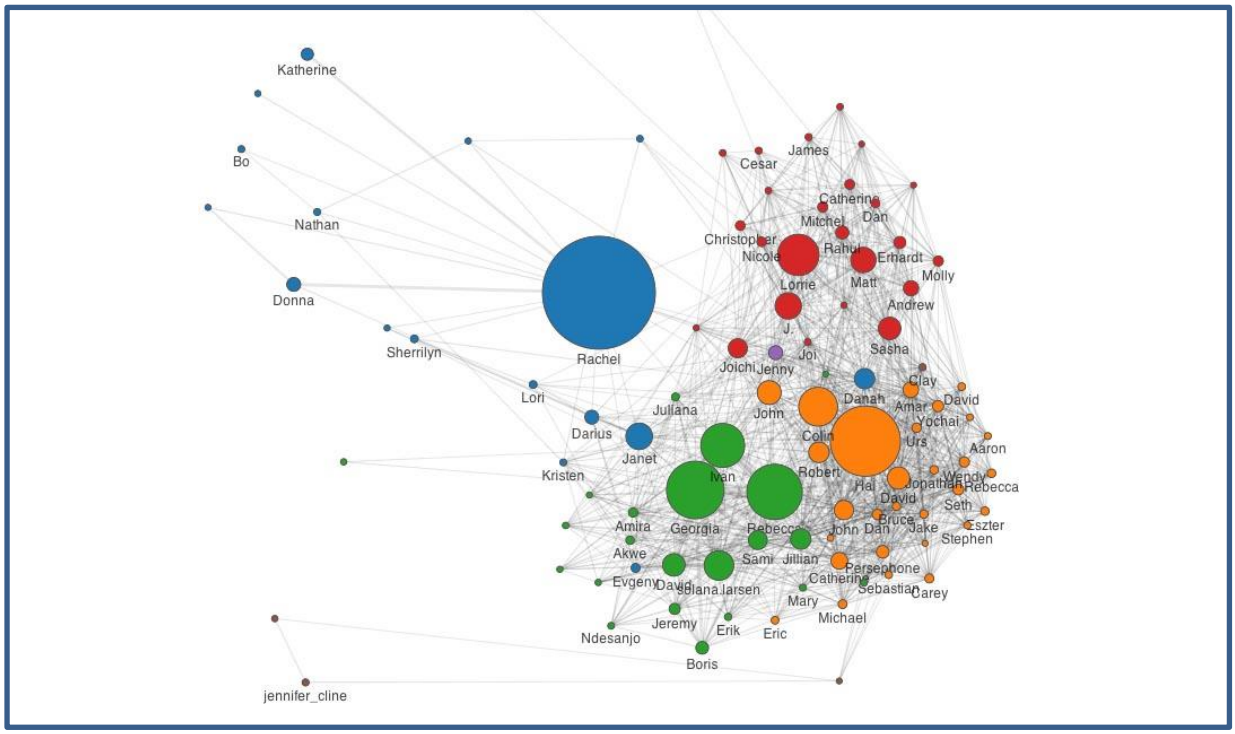
While the letter and envelope analogy might be an historically accurate one, the reality of modern technology and modern law enforcement, recognised by these agencies themselves, has undermined its contemporary application. "Anyone who thinks that metadata is harmless because it's 'just the envelope' either doesn't understand technology," says Senator Ludlam, "or is doing their best to impede other people's understanding."[70] Myriad statements from law enforcement and the Attorney-General's Department run contrary to the 'less intrusive' narrative outlined above, hinting at the breakdown of the distinction vital for proponents of data retention. That metadata is essential to successful investigations[71], "can contain particularly sensitive personal information"[72] and helps "build a picture of a target and their network of associates"[73] undermines the claim that its mass collection poses less of a threat to consumer privacy. As one senior telco industry figure suggested, "If it [metadata] were harmless, law enforcement would not be working so hard to get hold of it."[74]

A wealth of academic studies on the point has confirmed what LENSAs have long attempted to deny: "metadata is often a proxy for content."[75] The Privacy Act defines 'personal information' as "information or an opinion about an identified individual, or an individual who is *reasonably identifiable*" (emphasis added).[76] Although on its face, metadata might appear anonymised and trivial, the development of big data analysis techniques (for which metadata is "perfect fodder"[77]) means that the insights it provides after manipulation might well meet this definition.[78] The use of

[67] Attorney-General's Department, Submission No 26 to LCA Inquiry, 2014, p.22.
[68] Attorney-General's Department, Submission No 218 to PJCIS Inquiry, 2012, p.7.
[69] ASIO, Submission No 27 to LCA Inquiry, February 2014, p.10. See also AFP, Submission No 25 to LCA Inquiry, February 2014, p.11.
[70] Interview with Senator Scott Ludlam (Phone interview, 23 May 2014).
[71] Tim Morris, AFP national manager of high tech crime operations, quoted at CeBIT Cyber Security Conference 2014, Sydney in Hamish Barwick, 'Data sovereignty laws hamper international crime investigations: AFP', *Computerworld* (online), 8 May 2014, <http://www.computerworld.com.au/article/544591/data_sovereignty_laws_hamper_international_crime_investigations_afp/>.
[72] Attorney-General's Department, Submission No 26 to LCA Inquiry, 2014, p.12.
[73] Ibid, p.55.
[74] Email from senior industry policy figure who asked not to be identified.
[75] Expert declaration of Professor Edward W. Felten in *American Civil Liberties Union v James Clapper*, No. 13-3994 (S.D. New York December 28, 2013), <https://www.aclu.org/files/pdfs/natsec/clapper/2013.08.26%20ACLU%20PI%20Brief%20-%20Declaration%20-%20Felten.pdf>, p.14.
[76] *Privacy Act 1988* (Cth) s 6.
[77] Interview with David Vaile (Phone interview, 14 May 2014).
[78] This might even be the case with apparently de-identified data which, after being exposed to the so-called 'mosaic effect' of integrating diverse data to re-identify it, might become personally identifiable and sensitive. This potential was highlighted in White House, *Consumer data privacy in a networked world: A framework for protecting privacy and promoting innovation in the global digital economy,* February 2012, <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>, p.8.

telco metadata to accurately map a German Green politician's movements over six months,[79] visualisations of online networks rendered exclusively from email metadata (as below in Figure 2)[80] and the much-discussed case of Target mailing pregnancy coupons to a Minnesota girl whose family did not know she was pregnant yet[81] reveal the deeply personal nature of metadata.

Figure 2: 'Immersion' Gmail metadata visualisation, showing social networks



Most recently, a Stanford study which collected only the phone metadata of volunteers confirmed that metadata reveals a great deal about consumers' personal lives. The Stanford research indicated that metadata could be used to identify medical conditions[82], financial and legal connections and even whether phone users owned a gun.[83] While the dataset analysed in the Stanford example spanned hundreds of users over several months, the notion of warehousing this kind of

[79] 'Tell All Telephone', *Zeit Online,* <http://www.zeit.de/datenschutz/malte-spitz-data-retention>. This project was later mirrored by Swiss National Councillor Balthasar Glättli: http://apps.opendatacity.de/vds/index_en.html

[80] See https://immersion.media.mit.edu/

[81] Kashmir Hill, 'How Target figured out a teen girl was pregnant before her father did', *Forbes* (online), 16 February 2012, <http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/>. Also, interestingly, note the difficulty of trying to evade these systems, as humorously depicted in 'Dragnet Nation' (2014, Macmillan) in which author Julia Angwin tried to avoid sharing news of her pregnancy through any communications.

[82] Eg. Participant B spoke at length with cardiologists at a major medical center, talked briefly with a medical laboratory, received calls from a pharmacy, and placed short calls to a home reporting hotline for a medical device used to monitor cardiac arrhythmia. For more examples, see Jonathan Mayer and Patrick Mutchler, 'MetaPhone: The Sensitivity of Telephone Metadata', *Web Policy* (online), 12 March 2014, <http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/>.

[83] The study reinforced the findings of US Judge Richard Leon in *Klayman v Obama*, ruling in December 2013 that the NSA's bulk collection program likely violates the US Constitution, ruling: "Metadata reflects a wealth of detail about her familial, political, professional, religious and sexual associations." The case is currently on appeal.

"unambiguously sensitive"[84] data for all Australians over two years[85] presents a greater threat to consumer privacy still.[86] The United States government, grappling with a public relations disaster around their PRISM dragnet surveillance program, has, through a number of its advisory bodies, offered unqualified support for the notion that the distinction between content and metadata is now bankrupt.[87] Even those responsible for instituting surveillance programs in the US reject the divide. Former NSA General Counsel Stewart Baker has said "If you have enough metadata, you don't really need content"[88] and in a potential faux pas, the agency's former director General Michael Hayden recently asserted, "We kill people based on metadata." [89] A number of Australian LENSAs, including the Australian Security and Intelligence Organisation (ASIO), the Australian Federal Police (AFP) and the Australian Crime Commission (ACC), were approached to respond to the privacy-sensitive nature of metadata in the light of these revelations for this report. All agencies declined to comment.

Arguments in favour of a data retention proposal

Technical challenges

The primary argument proposed by law enforcement in favour of data retention is that briefly mentioned above in 'Privacy and Legislation': 35 years after its introduction the TIA no longer adequately takes into account the technical realities of communication. Across submissions from the AFP, ASIO and ACC the "diversity of the evolving telecommunications and digital landscape,"[90] the increasing use of VoIP[91] and other Internet communication services[92] and the changing criminal environment[93] are pointed to as reasons for introducing a data retention regime. More often than not, the degree of technological challenge is reinforced through the presentation of these changes in list form (or in diagrams, eg. Figure 3), presumably with the intention of showing that, in aggregate, the contemporary circumstances law enforcement confronts make it particularly difficult to properly

[84] Clifton Parker, 'Stanford students show that phone record surveillance can yield vast amounts of information', *Stanford News* (online), 12 March 2014, <http://news.stanford.edu/news/2014/march/nsa-phone-surveillance-031214.html>.

[85] Contrast the average duration of a telecommunications interception warrant under the TIA Act, which, in 2012/13, stood at only 75 days: Attorney-General's Department, Telecommunications (Interception and Access) Act 1979 *Annual Report 2012-13*, <http://www.ag.gov.au/NationalSecurity/TelecommunicationsSurveillance/Documents/TSLB-GAPSTIAActAnnualReport2012-13.pdf>, p.20.

[86] "The [big data] effect of collecting metadata about one individual is magnified when information is collected across the whole population." Felten, above n74, p.22.

[87] This includes the Privacy and Civil Liberties Oversight Board: "Telephone calling records, especially when assembled in bulk, clearly implicate privacy interests as a matter of public policy"; the President's Review Group on Intelligence and Communications Technologies: "In a world of ever more complex technology, it is increasingly unclear whether the distinction between 'meta-data' and other information carries much weight"; and even the parallel report by the President's Council of Advisors for Science & Technology (PCAST): "There is no reason to believe that metadata raise fewer privacy concerns than the data they describe."

[88] Alan Rusbridger, 'The Snowden Leaks and the Public', *The New York Review of Books* (online), 21 November 2013, <http://www.nybooks.com/articles/archives/2013/nov/21/snowden-leaks-and-public/>.

[89] David Cole, 'We kill people based on metadata', *New York Review of Books Blog* (online), 10 May 2014, <http://www.nybooks.com/blogs/nyrblog/2014/may/10/we-kill-people-based-metadata/>.

[90] AFP, Submission No 25 to LCA Inquiry, February 2014, p.8.

[91] Voice over Internet Protocol – a group of technologies for the delivery of voice communications and multimedia sessions over the Internet.

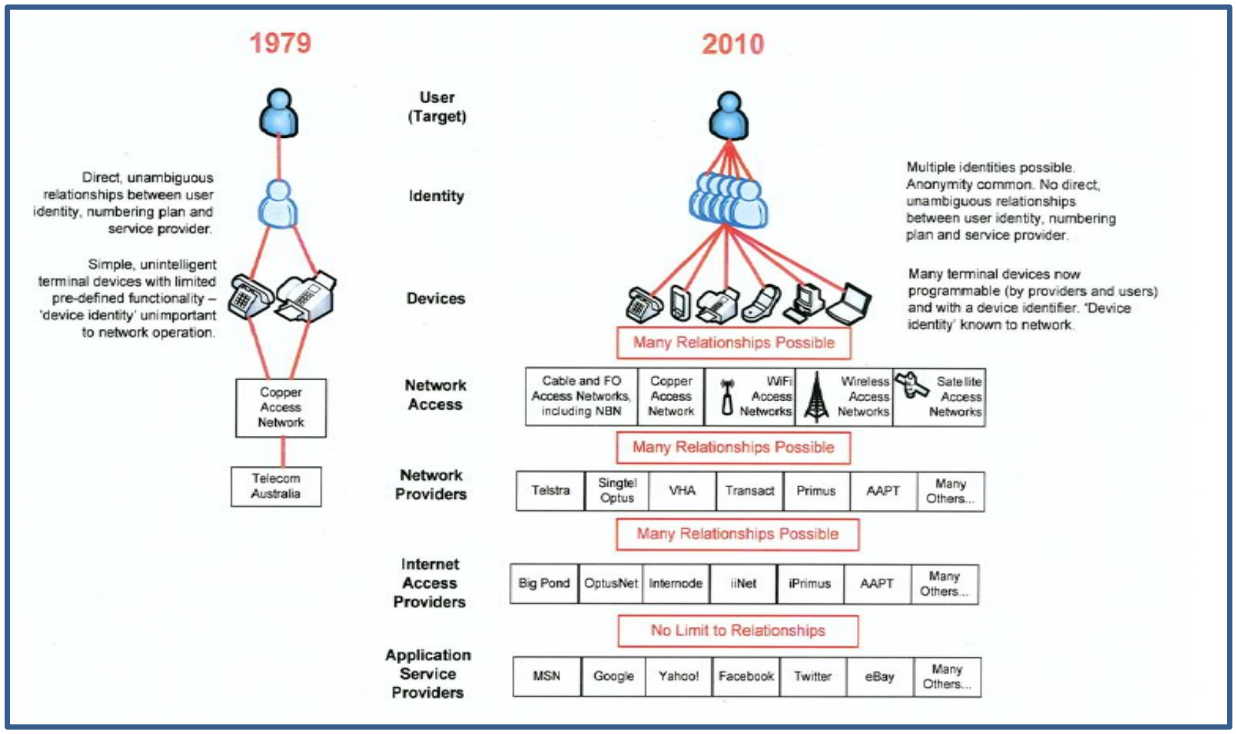
[92] ASIO, Submission No 27 to LCA Inquiry, February 2014, p.22.

[93] Australian Crime Commission, Submission No 23 to LCA Inquiry, February 2014, p.3.

investigate crimes with only an outdated TIA Act on hand. These sorts of general claims appear to be supported by empirical evidence but may falter when exposed to closer scrutiny. For instance, the statement from the Attorney-General's Department that "Anecdotal reporting from agencies is that increasingly, requests for telecommunications data are not being met"[94] does not present a particularly compelling argument for expanding access.

Many experts interviewed for this report suggested they have sympathy for law enforcement, particularly given that it is likely more difficult to surveil new technologies such as VoIP than traditional communications. However, there remained some scepticism as to how significantly investigations were compromised by an inability to keep pace with technology. Executive Director at the UNSW Cyberspace Law and Community Centre David Vaile suggested that "in many respects, there has been a massive increase in metadata available, presenting an Aladdin's cave of opportunity [for law enforcement]."[95] AMTA recognised that while "mobile technology continues to develop at a rapid pace… the underlying obligations to provide assistance to law enforcement have not changed."[96] Matthew Lobb, General Manager of Public Policy at Vodafone, indicated that as far as official, telco channels are concerned, LENSAs continue to have the same access to metadata they have had,[97] while another senior industry policy figure suggested, "The Attorney-General wants surveillance without checks, balances or transparency and is trying to dress it up as a technological issue, which it isn't."[98]

Figure 3: Diagrammatic example of the services and devices available in 1979 compared to 2010 (reproduced from the Attorney-General's Department submission to LCA inquiry)



[94] Attorney-General's Department, Submission No 218 to PJCIS Inquiry, 2012, p.8.
[95] Interview with David Vaile (Phone interview, 14 May 2014).
[96] Email from Lisa Brown to David Seidler, 5 June 2014.
[97] Email from Matthew Lobb to David Seidler, 23 May 2014.
[98] Email from senior industry policy figure who asked not to be identified.

Early-stage investigative assistance

From a procedural perspective, those in favour of a data retention system argue that metadata is essential in the early stages of investigations where it can be used to identify and obtain basic background information about persons of interest.[99] Further propagating the notion that, by nature, metadata interferes less with privacy than content, law enforcement suggest that early access to metadata "defers the need for other more intrusive and resource intensive investigation methods."[100]

The ACC's Paul Jevtovic has gone as far as proposing that the Telecommunications Act be amended to provide for penalties for service providers who do not cooperate with government requests for metadata.[101] As outlined by those studies and experiments examined above, there is obvious value in metadata for early-stage investigative purposes. Professor Michael Fraser of the Communications Law Centre agrees that "if law enforcement has a reasonable suspicion that you are planning a crime, they have both a right and a duty to collect this information."[102] Uncovering the networks of individuals associated with espionage cells, for instance, is possible relying only on metadata.[103] Just because metadata is helpful, however, does not necessarily affirm law enforcement's mass, largely unhindered access to it.

Appropriate oversight and accountability

The ACC, AFP and ASIO each separately stress the adequacy of existing oversight mechanisms as a reason that a mandatory regime would not adversely impact privacy. A common theme in these submissions is the emphasis placed on proportionality; that (less private) metadata already has relatively strict access thresholds and compliance procedures applied to it.[104] In a joint submission to the PJCIS inquiry, the three agencies pointed to the Commonwealth Ombudsman as providing accountability through its oversight of the TIA Act.[105] ASIO, particularly, is at pains to describe the scrutiny applied to its activities, involving answering to the Ombudsman, the Attorney-General[106] and the Inspector-General of Intelligence and Security.[107] The existing TIA legislation allows access to metadata with authorisations provided by 'authorised officers' of enforcement agencies. While the agencies concerned submit that these data authorisations "are already subject to various but equally rigorous and stringent accountability regimes"[108] that suggestion will be challenged below.

---

[99] ACC, Submission No 23 to LCA Inquiry, February 2014, p.15.
[100] AFP, Submission No 25 to LCA Inquiry, February 2014, p.11.
[101] Adding an offence in s 313 of the *Telecommunications Act 1997* (Cth): Juha Saarinen, 'Crime Commission wants to fine telcos who refuse to retain data', *IT News* (online), 23 April 2014, <http://www.itnews.com.au/News/383490,acc-wants-to-fine-telcos-who-refuse-to-hand-over-data.aspx>.
[102] Interview with Professor Michael Fraser (Phone interview, 22 May 2014).
[103] ASIO, Submission No 27 to LCA Inquiry, February 2014, p.27.
[104] See, eg, ACC, Submission No 23 to LCA Inquiry, February 2014, p.20; ASIO, Submission No 27 to LCA Inquiry, February 2014, p.18.
[105] ASIO, AFP, ACC (joint submission), Submission No 227 to PJCIS Inquiry, 2012, p.5.
[106] ASIO, *The Attorney-General's Guidelines*, <http://www.asio.gov.au/About-ASIO/Oversight-and-Accountability/Attorney-General-Guidelines.html>.
[107] ASIO, *Oversight and Accountability,* <http://www.asio.gov.au/About-ASIO/Oversight-and-Accountability.html>.
[108] ASIO, AFP, ACC (joint submission), Submission No 227 to PJCIS Inquiry, 2012, p.8.

Lengthy investigations

One position primarily promoted by ASIO (potentially because it is the agency most concerned with the conduct in question) is that data retention is necessary in light of both those technical constraints outlined above and temporal constraints. The need to "baseline the activities and threat posed by adversaries over an extended period"[109] appears perhaps the strongest reason for implementing a longer-term data retention policy. That said, there has been no evidence in the public domain beyond assertion provided by ASIO.

Public relations spin

Finally, one argument not specifically advanced by any of the LENSAs concerned but implicit in much of the rhetoric around the data retention issue globally is that bulk collection is not tantamount to mass surveillance. Defending the NSA's position at a symposium on the subject, the agency's former director General Michael Hayden highlighted the difference between the two, stressing a need to be "precise" in order not to be caught up in scare tactics borne out of nomenclature.[110] Drawing this distinction, between the potentiality and the reality of data retention programs, would be a good thing for Australian government agencies to be doing. Instead, they seem to be fighting a losing public relations battle.

Arguments opposed to a data retention proposal

No evidence of the need for telecommunications data

Perhaps the most compelling argument that can be made against data retention proposals is the simplest one: does law enforcement actually need two years of metadata on every person communicating over the Internet or by phone? If, as Professor Michael Fraser suggests, a data retention regime would "fundamentally alter the relationship between citizen and state and undermine the autonomy of the citizen as a self-determining agent,"[111] LENSAs would have to fairly strenuously outline the necessity of implementing such a system. Despite those arguments examined above, and perhaps not assisted by the confidential nature of many of their operations, law enforcement has been unable to mount a very convincing case to date, relying instead on anecdotal evidence, general social and technical shifts and "highlighting individual cases of repugnant crimes without any detail as to the significance of the role played by retained communications data [metadata]." [112]

In support of the claimed significance of metadata for crime-fighting efforts, LENSAs do not, and essentially cannot, offer statistical evidence. This failure comes down to a legislative anomaly which subverts those arguments of appropriate oversight and accountability outlined above. While the TIA Act makes it compulsory to report both interception and stored communication access warrant

[109] ASIO, Submission No 27 to LCA Inquiry, February 2014, p.27.
[110] David Cole and General Michael Hayden, 'The Price of Privacy: Re-Evaluating the NSA, A Debate' (Debate at the Johns Hopkins Foreign Affairs Symposium, Johns Hopkins University, 7 April 2014), <https://www.youtube.com/watch?v=kV2HDM86XgI>, from 1:10:00.
[111] Interview with Professor Michael Fraser (Phone interview, 22 May 2014).
[112] This aligns with international convention, as examined in Ian Brown, 'Communications Data Retention in an Evolving Internet' (2010), 19:2 *International Journal of Law and Information Technology* 95, p.106.

numbers, duration and effectiveness,[113] only the number of metadata authorisations is required to be reported under the Act.[114]

ASIO's use of metadata obtained under authorisations is still more opaque. Their figures are contained in a classified annual report to the Attorney-General and not made publicly available in the Attorney-General's annual report on the TIA Act.[115] In contrast, the United States' Freedom Act bill, which was recently passed by the US House of Representatives, reflects an obvious need for transparency in reporting procedures around metadata requests. It requires reports on both the numbers of metadata requests and the effectiveness of the program.[116] Without any statistical data on the efficacy of metadata in advancing the law enforcement agenda in Australia,[117] it is difficult to sustain an argument that it is essential to operations.[118]

Additionally, where information is available on the usefulness of metadata for LENSAs, the results are damning. In Germany, for instance, where requests for metadata were successful in 96% of all cases, it was found that a data retention program could raise the crime clearance rate by 0.002% at best.[119] Elsewhere, five years after the introduction of a one-year mandatory retention scheme there, Danish Police indicated in 2013 that the effort involved in sifting through masses of metadata had "caused serious practical problems" for their operations.[120] In Australia, the potential infeasibility of bulk metadata collection has also been raised by AMTA.[121] A 2011 European Commission review of the ill-fated EU Data Retention Directive outlined that almost 70% of all

---

[113] *TIA Act*: interception warrants (ss 100-102), stored communications access warrants (ss 162-163).
[114] *TIA Act* s 186.
[115] See, eg, ASIO's non-existence in Attorney-General's Department, Telecommunications (Interception and Access) Act 1979 *Annual Report 2012-13*, <http://www.ag.gov.au/NationalSecurity/TelecommunicationsSurveillance/Documents/TSLB-GAPSTIAActAnnualReport2012-13.pdf>.
[116] USA Freedom Act, HR 3361, 113th Congress (2013). Note, however, the "gradual loosening of its [the Bill's] privacy and disclosure measures" as this surveillance reform is challenged by the US intelligence community as it moves towards passage in the Senate. Spencer Ackerman, 'Surveillance reform slips away', *The Guardian Weekly* (Manchester), 13-19 June 2014, p.1.
[117] Note, too, that while asking for two years' worth of data retention, the AFP cannot say how long it requires data to be kept for operational purposes. Josh Taylor, 'AFP can't get data on how long it needs data', *ZDNet* (online), 8 January 2013, <http://www.zdnet.com/au/afp-cant-get-data-on-how-long-it-needs-data-7000009507/>.
[118] The author notes that the ability of LENSAs to provide particulars might be hindered by a need to keep their work secret, however, the release of statistics would not seem to compromise these operations. The need for statistical evidence of need is supported by a Parliamentary Library note on data retention: "Such information [on operational use of metadata] would go a long way to demonstrating the true nature and extent of the problem, and significantly bolster the Government's case that data retention is necessary and appropriate." Parliamentary Library, *Telecommunications data retention – an overview,* 24 October 2012, <http://parlinfo.aph.gov.au/parlInfo/download/library/prspub/1998792/upload_binary/1998792.pdf;fileType=application%2Fpdf>.
[119] Working group on Data Retention: Schriftsatz der Kläger des Ausgangsverfahrens in den Vorabentscheidungsverfahren mit den Aktenzeichen C-92/09 (Volker und Markus Schecke) und C-93/09 (Eifert), 11 October 2009, cited in Ian Brown, 'Communications Data Retention in an Evolving Internet' (2010), 19:2 *International Journal of Law and Information Technology* 95, p.107.
[120] See: http://www.ft.dk/samling/20121/almdel/reu/bilag/125/1200765.pdf, cited in Torben Olander, 'In Denmark, Online Tracking of Citizens is an Unwieldy Failure', *TechPresident* (online), 22 May 2013, <http://techpresident.com/news/wegov/23918/denmark-government-will-not-allow-ordinary-citizens-have-digital-privacy>.
[121] AMTA, Submission No 16 to LCA Inquiry, February 2014, p.12.

metadata is used within 3 months of its storage.[122] The prospect of LENSAs wading through scores of irrelevant, old metadata to find the information they require looms large.

Jurisdictional issues

The existence of markedly different standards on data retention globally (in flux again recently following the rejection of the EU Data Retention Directive) also fundamentally undermines the need for implementing a retention system in Australia. Access to the metadata of Australian communications, as well as those of the "clandestine foreign actors"[123] ASIO seeks to target, is invariably impacted by both the legislative situation overseas and the technological situation in Australia. As such, if Australian communications are made using networks or servers based elsewhere and these other jurisdictions do not enforce data retention laws, the ability of LENSAs to access their metadata is subverted. Telstra's James Shaw has pointed to the real manifestation of this techno-legal loophole, suggesting Telstra could not capture Gmail metadata because Google is based offshore and it is "over the top" of the telco's network.[124] The potential for a "chaotic situation"[125] of conflicting legal requirements and overlapping jurisdictions must inform any assessment of both the viability and value of a data retention regime.

Lack of checks and balances

Contrary to the suggestion of LENSAs outlined above, there is a fundamental lack of oversight of the current metadata access regime. While the warrant system in place for intercepting telecommunications and gaining access to stored communications necessitates the involvement of an independent third party (eligible judges or Administrative Appeals Tribunal members for the warrant applications of most enforcement agencies[126], the Attorney-General in ASIO's case[127]), the existing authorisation scheme for access to metadata requires no such oversight.

Instead, authorisations for access to metadata are made by "authorised officers" of enforcement agencies with no real accountability. We are left with only a report of the total number of authorisations granted on an annual basis.[128] The ease with which authorisations are granted is reflected in this number. A staggering 319,874 authorisations were made during the 2012/13 financial year.[129] The view of the Attorney-General's Department that "each authorisation… was justified on a case-by-case basis as being 'reasonably necessary'"[130] is unconvincing given that these determinations are made by the very agencies that grant the authorisations. Moreover, the sheer

---

[122] European Commission, *Evaluation report on the Data Retention Directive from the Commission to the Council and the European Parliament 2011,* <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:en:PDF>.
[123] ASIO, Submission No 27 to LCA Inquiry, February 2014, p.27.
[124] Evidence to Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, Canberra, 27 September 2012, p.12 (James Shaw, Director of Government Relations, Telstra).
[125] Australian Media Industry Association Digital Policy Group (AMIA), Submission No 198 to PJCIS Inquiry, 2012, p.3.
[126] *TIA Act* s 39.
[127] *TIA Act* s9.
[128] *TIA Act* ss 178-180.
[129] Attorney-General's Department, Telecommunications (Interception and Access) Act 1979 *Annual Report 2012-13*, <http://www.ag.gov.au/NationalSecurity/TelecommunicationsSurveillance/Documents/TSLB-GAPSTIAActAnnualReport2012-13.pdf>, p.49.
[130] Attorney-General's Department, Submission No 26 to LCA Inquiry, 2014, p.23.

quantity of authorisations signals that these merit assessments must take place rapidly, inevitably impacting their quality.[131]

The practical reality is more concerning still if, as these large numbers suggest, agencies' power to make authorisations has now become equivalent to blanket authority. Despite the collective claim of the AFP, ACC and ASIO that the Commonwealth Ombudsman provides oversight of law enforcement compliance with the TIA Act[132], this supervision does not extend to Chapter 3 of the TIA Act, which regulates agencies' access to metadata. ASIO is further made responsible to the Inspector-General of Intelligence and Security. Charged with assessing whether tens of thousands of authorisations were 'reasonably necessary', it is unlikely this agency is able to offer effective oversight. Noting the range of oversight issues, extending access to two years of metadata would seem to exacerbate the oversight deficit.

Costs

The costs of a mandatory data retention system are a sticking point for most of industry. The question of who will fund the costs of a mandatory data retention regime is not addressed by the AFP, ACC or ASIO in their submissions to the current LCA inquiry. To be sure, some metadata is already collected and retained by telcos for business (mainly billing) purposes but it is not harvested in any particularly structured or long-term way. By contrast, a two year mandatory data retention system necessarily involves far larger swathes of data. Accordingly, the following costs are anticipated:

- Cost of collating data
- Cost of storing data
- Cost of securing data to maintain data integrity for both consumers and for agency investigative purposes
- Cost of making data available to agencies in a form that can be used for their investigations
- Cost of destruction of that data after the life-cycle of retention has expired
- Cost associated with agencies manipulating and investigating data[133]

While the specific dollar figure for a data retention regime is unknowable given that the debate shaping its form continues, industry has provided tentative estimates. iiNet has been the telco most willing to put a number on what it believes data retention will cost individual companies. Its chief regulatory officer Steve Dalby has quoted the LCA inquiry at about $60 million to build and secure a 20 petabyte metadata centre.[134] More broadly, in a joint submission to the PJCIS inquiry, AMTA and Communications Alliance suggested that if source and destination IP addresses for devices used in communications were retained, the figure industry-wide for implementing a retention program could be as high as $700 million.[135] While much depends on exactly which data sets are required to

[131] As an example, NSW Police must be particularly busy weighing up whether their metadata authorisations are 'reasonably necessary' or not 327 times a day in order to meet the number of authorisations granted by the organisation in 2012/13: 119,705.
[132] ASIO, AFP, ACC (joint submission), Submission No 227 to PJCIS Inquiry, 2012, p.5.
[133] Evidence to Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, Canberra, 27 September 2012, p.4 (James Shaw, Director of Government Relations, Telstra).
[134] iiNet, Submission No 38 to LCA Inquiry, 2014, p.2.
[135] AMTA and Communications Alliance, Submission No 114 to PJCIS Inquiry, 2012, p.14.

be retained by telcos, given the mass scale of the system under consideration, the addition of a single data element has the potential to increase costs by tens of millions of dollars.[136]

Recognising the prohibitive nature of these costs, the next question is inevitably who will foot the bill for a data retention system? The three parties which would potentially be involved in funding are industry, government and consumers. The legislative situation across the European Union demonstrates a variety of approaches to funding. Examining the EU experience, it is useful to divide costs between 'capital expenditure' (infrastructure, rent, staff, utilities) and 'operational expenditure' (operating metadata databases). Industry was not reimbursed for capital expenditure in 19 of 21 EU member states that implemented data retention programs, nor was it reimbursed for operational expenditures in over half of member states.[137] In Australia, the PJCIS inquiry recommended that the costs incurred by telcos should be reimbursed by the government[138] but the scope of this reimbursement, as with the rest of the program, remains up for debate.

From a consumer perspective, the adoption of this PJCIS recommendation is critical. In arguing against a data retention program, iiNet's Dalby has suggested that if forced to take part, the company would pass any costs directly on to consumers, adding an additional $5 per month to all consumer products. [139] Further, the imposition of these costs on industry would create significant barriers to entry.[140] As an illustration, as of June 2013 there were 419 Internet Service Providers (ISPs) operating in Australia.[141] For the 393 of these with fewer than 10,000 subscribers, as well as any new entrants seeking to get a foothold in the Australian Internet market, adding the not insignificant cost of data retention infrastructure and security to the cost of doing business could prove prohibitive.

Security

Inspector-General of Intelligence and Security Vivienne Thom recently indicated that the Australian proposal is different from the United States situation in that, in Australia, telcos rather than law enforcement would be responsible for storing metadata.[142] Some experts contend that this distinction is a false one, suggesting "IT security is over"[143] and thus it does not matter "where the bucket is held."[144] A series of serious security breaches in Australia – involving telco servers[145] and

---

[136] Ibid.

[137] European Commission, *Evaluation report on the Data Retention Directive from the Commission to the Council and the European Parliament 2011,* <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:en:PDF>, p.27.

[138] PJCIS report, above n1, p.192 (Recommendation 42).

[139] Evidence to Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, Canberra, 27 September 2012, p.49 (Stephen Dalby, Chief Regulatory Officer, iiNet). See also PJCIS Report, above n1, p.177.

[140] An interesting issue to further consider is the likelihood that over-the-top providers (eg. Skype) will avoid paying for a data retention system, leading to a potential distortion of the market.

[141] ACMA, *Communications Report 2012-13*, <http://www.acma.gov.au/~/media/Communications%20Analysis/Comms%20Report%202012%2013/PDF/ACMA%20Communications%20report%20201213_WEB%20pdf.pdf>, p.25.

[142] Ben Grubb, 'It's wrong to assume we're all being spied on, spy watchdog says', *Sydney Morning Herald* (online), 7 May 2014, <http://www.smh.com.au/it-pro/security-it/its-wrong-to-assume-were-all-being-spied-on-spy-watchdog-says-20140507-zr6az.html>.

[143] Interview with David Vaile (Phone interview, 14 May 2014).

[144] Interview with Professor Michael Fraser (Phone interview, 22 May 2014).

customer lists,[146] social networks[147] and parliamentary email servers[148] – suggests that the distinction may indeed be obsolete. Security concerns extend beyond unauthorised access and dissemination to the prospect of tampering, which could damage the veracity (and potential, later evidential admissibility) of entire metadata databases. The collection of two years of sensitive metadata on every Australian communication is problematic where no entity - LENSA, telco or third party - can promise protection of information from diligent attackers.[149]

If, as Thom suggested, the responsibility for storing and securing data is left solely to telcos, the very nature of this obligation would tend to undermine data security. While law enforcement stand to gain from access to metadata, its security would represent a 'cost centre' for telcos – a part of the business that does not produce direct profit for telcos but adds to their cost of business. Where telcos derive no profit from securing metadata but rather do it begrudgingly for regulatory purposes, there is an obvious lack of incentives for investing in this security. Even if legislative penalties were to be introduced as a way to motivate telcos' security compliance,[150] Senator Ludlam suggested this would not alleviate a fundamental attitude problem in still requiring industry to "take care of information that they're desperate to not have to keep in the first place."[151] Additionally, those same market factors outlined in the costs discussion above would threaten the consistency of security across industry. Where major telcos like Telstra, Optus and Vodafone might have the knowledge, resources and critical mass of consumers to be able to properly protect vast troves of metadata, it is unlikely smaller players would.[152] Not only does industry in general have no incentive to provide adequate metadata security, but smaller entities have even less reason to do so.

These security concerns take on greater urgency when recognising that there is currently no legislation requiring telcos (or government, or other business) to proactively notify consumers when the security of their personal information has been compromised. Such a scheme, known as a data breach notification system, was proposed in the Privacy Amendment (Privacy Alerts) Bill of 2013 and, although Senator Ludlam suggested it had cross-Parliamentary support at the time, the Bill lapsed when Parliament was prorogued. It has since been reintroduced to Parliament in 2014[153] but one industry insider suggested the Bill has "zero chance of getting through" given the Coalition's

---

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

[146] Ben Grubb, 'Oops: Google search reveals private Telstra customer data', *Sydney Morning Herald* (online), 16 May 2013, <http://www.smh.com.au/technology/technology-news/oops-google-search-reveals-private-telstra-customer-data-20130516-2jnmw.html>.

[147] See examples of serious data breaches at Yahoo, LinkedIn and Twitter highlighted in NSW Young Lawyers, Submission No 133 to PJCIS Inquiry, 13 August 2012, p.11.

[148] Christopher Joye and Aaron Patrick, 'Chinese spies may have read all MPs' emails for a year', *Australian Financial Review* (online), 26 April 2014, <http://www.afr.com/p/technology/chinese_spies_may_have_read_all_sBngugTM3JvSXFkcjgo4cN>.

[149] Or internal threats for that matter - eg. Edward Snowden was a contractor at the NSA.

[150] As indicated in Recommendation 19 of the PJCIS Report, above n1, p.84.

[151] Interview with Senator Scott Ludlam (Phone interview, 23 May 2014).

[152] Reflected in AMTA CEO Chris Althaus' suggestion evidence to the PJCIS Inquiry: "There are large entities within the industry that are very skilled and expert and experienced but…under a data retention regime there would be a wide range of people who would not have those skills and there would be attendant risks to privacy." See PJCIS Report, above n1, p.177.

[153] Privacy Amendment (Privacy Alerts) Bill 2014.

deregulation agenda.[154] There is certainly strong opposition to the notion from industry, which sees the significant costs associated with data breach notification as an unfair burden given the resources it already invests to ensure privacy.[155] To be sure, the OAIC encourages telcos and others to refer to its 'Guide to handling personal information security breaches'[156] and the organisation handled 61 self-reported breach notifications in 2012-13.[157] In the data retention context, however, where industry would be made to collect vast quantities of metadata, be faced with a number of security threats and armed with little incentive to protect against them, the absence of a formalised data breach notification system is deeply concerning.

Criminals will evade detection

While the security of average telco users' metadata is threatened, it is possible that the criminals a data retention regime is designed to apprehend will recognise the status quo and adapt accordingly, effectively evading LENSAs in their analysis of metadata. Commissioner of the NSW Police Force Andrew Scipione has suggested that "Frankly, organised criminals are now able to operate outside the reach of ordinary telecommunications interception."[158] The introduction of a data retention regime would only further incentivise the circumvention of LENSA monitoring of telecommunications. Just as the avenues for communication have increased, so have potential evasion tactics proliferated. As such, LENSAs would confront criminals resorting to steganography[159], encryption, TOR anonymisers[160], wardriving[161], alternative internet service providers[162] as well as more traditional strategies like identity theft, identity fraud and secondary trading in prepaid mobile services.[163] Fundamentally, as Senator Ludlam notes, a mandatory data regime would be "driving an arms race whereby the only people who will take protective measures will be the very people they [LENSAs] are trying to catch."[164]

---

[154] Phone interview with industry figure who asked not to be identified.
[155] Hamish Barwick, 'Comms Alliance expresses concerns with mandatory data breach notification', *TechWorld* (online), 20 June 2013, <http://www.techworld.com.au/article/465419/comms_alliance_expresses_concerns_mandatory_data_breach_notification/>.
[156] OAIC, *Data breach notification – A guide to handling personal information security breaches,* <http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches>.
[157] OAIC, *Annual Report 2012-13*, <http://www.oaic.gov.au/images/documents/about-us/corporate-information/annual-reports/Annual-report-2012-13/Complete_pdf_AR_2012-13.pdf>, p.4.
[158] Quoted in Attorney-General's Department, Submission No 26 to LCA Inquiry, 2014, p.14.
[159] The practice of concealing a message within another message.
[160] TOR, short for 'The Onion Router', is free software enabling anonymous communication on the Internet. For a good explanation see Angela Daly, *Ubiquitous online surveillance and the right to anonymity*, Swinburne University of Technology, <https://www.academia.edu/5936311/Ubiquitous_Online_Surveillance_and_the_right_to_anonymity>. Catherine Smith, Assistant Secretary at the Attorney-General's Department has acknowledged that data retention is useless in the face of TOR anonymisers. See http://scott-ludlam.greensmps.org.au/content/estimates/attorney-generals-department-data-retention
[161] The practice of searching for Wi-Fi wireless networks in a moving vehicle with a laptop or smartphone. This is a modern update on the old practice of going to Internet cafes to avoid detection of online communications.
[162] Eg. riseup.net
[163] AMTA, Submission No 16 to LCA Inquiry, February 2014, p.13.
[164] Interview with Senator Scott Ludlam (Phone interview, 23 May 2014).

Straining an already deficient complaints system

The current LCA inquiry has, among its terms of reference, one of the chief concerns of the Australian Law Reform Commission's (ALRC) 2008 For Your Information privacy inquiry: "the roles and functions of the various bodies currently involved in the regulation of the telecommunications industry."[165] The focus here from a consumer perspective is on the right to redress and how well the complaints system works. A 2010 report on privacy complaints handling found that the system did not work very well at all. Instead, the system was found to be plagued by a disparity in complaint numbers across complaint bodies (ACMA, TIO, OAIC), consumers faced inconsistent resolution times and process issues and ultimately, uncertain and inconsistent outcomes.[166] When one of the authors of the 2010 report was asked if he had seen an improvement in the four years since its publication, he suggested that while no other detailed study had occurred in the interim, the responsible organisations had continually been given extra responsibilities and fewer resources.[167] The recent demise of the OAIC in the aftermath of the 2014 Federal Budget will undoubtedly impact privacy complaints resolution, dissolving an organisation that was responsible for responding to 127 telco privacy complaints in 2012/13.[168]

While the complaints system delivers uncertain results, many consumers do not even reach the stage of lodging a complaint given a lack of public awareness of redress options. The 2013 OAIC Community Attitudes to Privacy survey indicated that between 2007 and 2013, the number of those surveyed who "can't say" which organisations they would report a misuse of personal information to climbed 7% to 27%.[169] Reductions in complaint numbers year-on-year at the TIO[170] and stable numbers at the OAIC[171] might therefore reflect a generally unaware public rather than a decline in telcos' complaint-worthy behaviour. Part of the problem could be branding-related – many point to the distraction and brand awareness decline brought about by the Office of the Privacy Commissioner's name change to the OAIC in 2011[172] – but there must be a more fundamental awareness problem at play. The TIO deflected concern over this rise, highlighting a positive change in that over twice as many people would contact the organisation involved.[173] However, the

---

[165] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008), p.2395, Recommendation 71-2.

[166] Chris Connolly and David Vaile, Cyberspace Law and Policy Centre for Australian Communications Consumer Action Network, *Communications privacy complaints: in search of the right path,* 2010.

[167] Interview with David Vaile (Phone interview, 14 May 2014). See Information Commissioner Professor John McMillan's comments on resourcing here: http://www.oaic.gov.au/news-and-events/speeches/information-policy-speeches/iq-interview-with-professor-john-mcmillan

[168] OAIC, *Annual Report 2012-13*, <http://www.oaic.gov.au/images/documents/about-us/corporate-information/annual-reports/Annual-report-2012-13/Complete_pdf_AR_2012-13.pdf>, p.67.

[169] OAIC Attitudes Survey, above n20, p.22.

[170] TIO, *2012-13 Annual Report Statistics: Issues for new complaints*, <http://annualreport.tio.com.au/downloads/statistics>.

[171] Comparing OAIC annual reports for 2010-11, 2011-12 and 2012-13, the number of privacy complaints in the telecommunications space has remained at exactly 127 for the last three years.

[172] An opinion shared by David Vaile (Interview with David Vaile (Phone interview, 14 May 2014)) and Nigel Waters (Nigel Waters, 'Responding to new challenges to privacy through law reform: a privacy advocate's perspective' in Normann Witzleb, David Lindsay, Moira Paterson and Sharon Rodrick (eds), *Emerging Challenges in Privacy Law: Comparative Perspectives*. (Cambridge University Press, 2014), p.51.)

[173] Email from the TIO to David Seidler, 28 May 2014.

inconsistency that consumers face from disparate codes and privacy policies[174] subverts the value of this alternative dispute resolution option. Bogged down in internal complaints systems, consumers may experience a sense of despair so that they do not ultimately follow up with official complaint bodies which can actually make binding determinations. Recognising these inherent problems, introducing the bulk storage of metadata by telcos with no motivation to protect it and attendant security threats will only serve to further strain a complaints system already under-resourced and underperforming.

Conclusions and recommendations

1. The Government should abandon current data retention proposals

Reflecting on those arguments outlined above both in favour of and against data retention in Australia, on balance the prudent stance would be to delay the introduction of any such regime. Despite claims from LENSAs that changes to the technological environment have seriously impacted their crime-fighting abilities, none have provided sufficient empirical evidence to support their statements of need.[175] There remains a lack of public support for such a scheme with survey data suggesting Australians are comfortable with their government spying on other countries,[176] but not with the same techniques being applied to surveillance of their own activities.[177] Confronting a number of high profile about-faces across Europe and the United States in recent months and significant security risks, it is difficult to expect industry and the general public to willingly subscribe to a program of bulk collection which effectively puts all telco users into the 'guilty until proven innocent' basket.

2. A data preservation system is a suitable alternative to data retention

If the purpose of introducing a data retention regime is to better combat high tech and organised crime, a data preservation system is worth exploring as a more nuanced alternative to bulk data retention. Data preservation differs from data retention in that it requires telcos to collect metadata only for a specified period on targeted users, usually suspected of criminal activity.[178]

---

[174] See, eg, the findings of Chris Connolly and David Vaile, Cyberspace Law and Policy Centre, *Drowning in Codes of Conduct: an analysis of codes of conduct applying to online activity in Australia*, March 2012, <http://cyberlawcentre.org/onlinecodes/report.pdf>

[175] LENSAs have thus failed to meet a request that has been made in official recommendations since 2011. See, eg, "Recommendation 9: Justify the collection and retention of personal data by demonstrating the necessity of that data to law enforcement agencies." Senate Environment and Communications References Committee, Parliament of Australia, *Report on Inquiry into the adequacy of protections for the privacy of Australians online*, (2011), p.69.

[176] Alex Oliver, 'Lowy Institute Poll 2014', *Lowy Institute* (online), 2 June 2014, <http://www.lowyinstitute.org/publications/lowy-institute-poll-2014>.

[177] 78% of Australians are uncomfortable with having their activities monitored covertly on the Internet while 93% of those surveyed think that an organisation monitoring their activities on the Internet without their knowledge is a misuse of information. OAIC Attitudes Survey, above n20, p.7, 23.

[178] A number of industry figures mistakenly suggested that a data preservation system already exists in the Cybercrime Legislation Amendment Act 2012 (Cth) sch 1. Those provisions, however, apply to 'stored communications' rather than metadata.

LENSAs may argue that data preservation works well for investigating known criminals but fails where individuals are not known to authorities and accordingly, that important (historical) metadata might be lost before they were able to identify a criminal and request a data preservation order. Evidence from the European Union outlined above negates this concern. Metadata is most useful within a three-month window of its creation and as such, this data would be readily available to LENSAs if they require some retrospective investigation, given existing telco collection patterns.

A preservation system, coupled with improvements to existing Mutual Legal Assistance Treaties (for cross-border investigations), would seem to meet the objectives of LENSAs while proportionately reducing privacy intrusion. Restricting data collection to criminal suspects in this way would also serve to drastically lower the costs and security risks that accompany bulk collection.

Some proposals exist for a data preservation alternative involving closer scrutiny, requiring judicial authorisation for preservation orders.[179] While greater oversight is laudable and reduces the potential for abuse,[180] the sheer number of metadata authorisations under the current TIA Act system suggests that requiring judicial oversight would only swamp the courts and further frustrate LENSA's operational efforts.

3. We need more transparency and accountability

Regardless of whether or not a data retention system is implemented in Australia (but especially if it is), the existing oversight mechanisms that apply to LENSA access to metadata must be improved. Appropriate monitoring and public reporting is essential to improving public confidence and ensuring proportionate use of powers exercised under the TIA Act. The AFP specifically recognises this[181] while ASIO acknowledges the value of accountability and oversight as long as it does not impede "agile operational decision-making in the prevention of harm."[182] A disproportionate focus on operational matters at the expense of appropriate oversight has left the current accountability situation markedly inadequate. The Attorney-General's Department has proved the voice of reason in this debate, admitting in its LCA inquiry submission that the TIA Act's oversight arrangements "are, in part, fragmented and incomplete."[183]

A minimum first step is a more detailed and transparent reporting system for metadata access and use. If the public is ever going to feel comfortable with the collection of their metadata by LENSAs, these agencies will have to be more open. The existing reporting requirements for interception and access to stored communication should be extended to apply to metadata, specifically so that agencies must detail the operational effectiveness of their access to metadata.

---

[179] Ian Brown, 'Communications Data Retention in an Evolving Internet' (2010), 19:2 *International Journal of Law and Information Technology* 95, p.107.
[180] Thus ASIO is to be applauded for requiring their prospective metadata requests to be authorised by a "Senior Executive Service Band 2 officer or higher." ASIO, Submission No 27 to LCA Inquiry, February 2014, p.16.
[181] AFP, Submission No 25 to LCA Inquiry, February 2014, p.6.
[182] ASIO, Submission No 27 to LCA Inquiry, February 2014, p.25.
[183] Attorney-General's Department, Submission No 26 to LCA Inquiry, 2014, p.3.

4. Introduce external accountability for metadata authorisations

Most oversight now occurs after the fact of authorisation. Real accountability mechanisms around authorisations would need to provide for checks on the exercise of the authorisation before it occurs. [184] Current internal agency authorisations are opaque and need to be the subject of external, independent monitoring in order to build greater integrity into the metadata access process. This additional layer of accountability could take a number of different forms. In its simplest form, it might involve an extension of the Commonwealth Ombudsman's oversight functions to metadata access. Alternatively, a newly formed body such as a Public Interest Monitor (PIM) – representing the public interest where LENSAs seek access to metadata – might play a similar role in balancing law enforcement and privacy intrusions. The ALRC previously rejected the need for a PIM on the grounds that many of its functions are already provided by other bodies.[185] A PIM could, however, provide a key link in a currently deficient chain of accountability by examining authorisations before they are approved.[186]

5. Introducing a data breach notification system

Letting consumers know when their personal information has been compromised is fundamental to corporate social responsibility. The amount of personal data that telcos and other corporations now store as well as the security risks inherent in this storage make the need for such alerts more pressing still. Surveys of the Australian public have demonstrated, however, that this sentiment is not shared by consumers, with between 85% and 96% of respondents in two different surveys suggesting that they expect organisations to tell them if their personal information is accessed without authorisation.[187]

Alerting consumers every time their data is accessed or disclosed without authorisation could lead to notification fatigue or compromise consumer confidence. To avoid both of these outcomes, any data breach notification system should be graded and transparent, "risk-driven" [188] such that consumers are not overwhelmed with notifications or discouraged from engaging with companies at all out of

---

[184] Note, for instance, that the Inspector-General of Intelligence and Security, responsible for overseeing ASIO among other national defence organisations, has herself recognised this scheduling problem by claiming, "If something does happen, I'll get a phone call and I'll be one of the first persons to be alerted that something's gone wrong." Ben Grubb, 'It's wrong to assume we're all being spied on, spy watchdog says', *Sydney Morning Herald* (online), 7 May 2014, <http://www.smh.com.au/it-pro/security-it/its-wrong-to-assume-were-all-being-spied-on-spy-watchdog-says-20140507-zr6az.html>.

[185] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008), p.2394.

[186] As opposed to judicial authorisations, a more specialised PIM dealing exclusively with metadata access could more efficiently deal with determining the validity of authorisation requests.

[187] 96% of Australians expect organisations to tell them if their personal information is lost: OAIC Attitudes Survey, above n20, p.5; 85% of Australians believe data breach notification should be mandatory for business: Centre for Internet Safety, *Privacy and the Internet: Australian attitudes towards privacy in the online environment April 2012,* <http://www.canberra.edu.au/cis/storage/Australian%20Attitutdes%20Towards%20Privacy%20Online.pdf>, p.5.

[188] Interview with David Vaile (Phone interview, 14 May 2014).

fear of data breaches. Consumers should not be directly contacted or breaches publicly advertised unless they are particularly egregious.

By ensuring that the reputational damage wreaked by notifications is proportional to breach severity, consumer and industry will be best protected. If appropriately designed and managed, a data breach notification system can mitigate the consequences of breaches, create incentives for improving security and maintain community confidence in legislative privacy protection.[189]

6. Streamline complaints bodies and boost their powers

OAIC survey statistics show that increasing numbers of consumers do not know where to lodge a complaint.[190] Currently, complaints that are lodged with complaints bodies often result in privately negotiated resolutions with little lasting behavioural impact for the offending telco. The existing privacy complaints system plainly does not meet consumer expectations.

The issues with the existing system are twofold: messaging and remedies.

In terms of messaging, most major telcos (except Vodafone which does not mention any third party[191]) point only to the TIO for last-resort complaints resolution, neglecting to mention additional avenues of redress offered by the OAIC and ACMA.[192] Advice provided by these complaints bodies is inconsistent and characterised by bureaucratic buck-passing. For example, the OAIC's 'Complaints Checklist' asks first whether consumers have lodged a complaint with the Commonwealth Ombudsman.[193] The Commonwealth Ombudsman's website in turn tells consumers with telecommunications privacy issues to lodge a complaint with the TIO.[194]

When it comes to remedies, similar discrepancies pervade the system. For instance, the OAIC (to be disbanded at the end of 2014) can accept enforceable undertakings (or promises of behaviour change) from telcos.[195] Taking the same complaint to the TIO could result in legally binding directions for telcos to pay compensation of up to $50,000 and recommendations for up to $100,000.[196]

An inter-organisational annual report focusing specifically on privacy complaints and their resolution would be a good first step towards achieving the consistency and coordination required. [197] Moreover, in the absence of a data breach notification system, the Privacy Commissioner needs more legal powers to penalise telcos and other businesses for substandard practices.

---

[189] As outlined by the Attorney-General's Department in the PJCIS Report, above nXX, p.175.
[190] OAIC Attitudes Survey, above n20, p.22.
[191] See vodafone.com.au/aboutvodafone/legal/complaintshandlingpolicy
[192] Note: ACMA's responsibilities around the resolution of privacy complaints (outside of Do Not Call Register and Spam Act issues) are comparatively negligible.
[193] See http://www.oaic.gov.au/privacy/privacy-complaints/privacy-complaint-checker/question-4
[194] See http://www.ombudsman.gov.au/pages/making-a-complaint/
[195] See http://www.oaic.gov.au/privacy/privacy-act/privacy-law-reform#powers
[196] See http://www.tio.com.au/publications/media/increased-powers-for-telecommunications-industry-ombudsman
[197] Not unlike a parallel to the Annual Report into the organisational use of the TIA Act, compiled by the Attorney-General's Department, referenced above in nXX.

7. Prevent privacy breaches in the first instance: improve education, privacy engineering and a new Australian Privacy Principle

Perhaps even more important than fixing those systems that are engaged when something goes wrong in privacy is pre-empting breaches and other substandard behaviours before they occur. One senior agency figure suggested, "Preventative medicine is better than reactive medicine."[198] This 'preventative medicine' might take the form of increased educational efforts, privacy engineering to further improve security or a new APP providing consumers with the ability to request the destruction or de-identification of their personal data.

Improving education

The OECD Council recently recommended that member countries consider the local implementation of measures "including education and awareness raising, skills development, and the promotion of technical measures which help to protect privacy."[199]

In an Australian law reform context, this need for educating telco users around privacy has been repeated by almost every major inquiry into the subject in recent years.[200] The results of a 2009 ACMA survey into online trust and confidence highlights the importance of educating users, with 68% of respondents indicating that in terms of their Internet training, they are 'self-taught'.[201]

Moreover, the privacy policy requirements under APP 1 are an inadequate method of user education given that the Privacy Commissioner himself has identified that they are often "extraordinarily complex and can become virtually worthless,"[202] reflected in the fact that 51% of Australian consumers do not read privacy policies.[203]

Although there are examples of good practice in government, telcos and the online industry, a more consistent and thorough approach to educating telco users about privacy is essential to curbing future breaches and enhancing the overall consumer privacy experience.

Privacy engineering

While education is certainly important, it is described as a "cop out"[204] or "smoke screen"[205] by some wary of its use to cover up poor privacy engineering – as Mark Rotenberg, President of the Electronic

---

[198] Phone interview with senior agency figure who asked not to be identified.
[199] OECD Council, *Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data 2013*, <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/DataProt/Legislation/2013-09-09_oecd-privacy-guidelines_EN.pdf>.
[200] See, eg, Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008), p.2250; Senate Environment and Communications References Committee, Parliament of Australia, *Report on Inquiry into the adequacy of protections for the privacy of Australians online*, (2011), p.16-19; Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Area*, Discussion Paper No 80 (2014), p.36.
[201] ACMA, *Australia in the Digital Economy: Trust and Confidence, March 2009*, <http://www.acma.gov.au/webwr/aba/about/recruitment/trust_and_confidence_aust_in_digital_economy.pdf>, p.35.
[202] Evidence to Environment and Communications References Committee, Parliament of Australia, Canberra, 29 October 2010, p.22 (Mr Timothy Pilgrim, Australian Privacy Commissioner).
[203] OAIC Attitudes Survey, above n20, p.4.
[204] Interview with Professor Michael Fraser (Phone interview, 22 May 2014).

Privacy Information Centre puts it, "the devil is always in the defaults."[206] Building privacy protection into systems is a fundamental prerequisite for best practice consumer privacy. The very size and characteristics of the databases that telcos develop mean that there are "no guarantees that they will not leak, or be subject to function creep, or be simply abused by those who have authority and access to the data."[207] Accordingly, technical mechanisms restricting both access and disclosure may not ultimately be successful in preventing breaches but are nonetheless baseline measures that should be implemented.[208]

A good example is Google encrypting Gmail by default and providing for second-factor authentication across its array of services. Facebook similarly implements 80 trillion daily backend privacy checks and 4000 daily privacy surveys.[209] The OAIC's publication of a best practice guide for building privacy into mobile apps[210] is also a step in the right direction. Telcos and online industry alike should be asking themselves "What do our customers expect from us in the context of their data transactions?" the answers to which will lead to privacy security engineered into hardware, software and services.[211]

Introducing a new APP

The recently released ALRC discussion paper for its Serious Invasions of Privacy inquiry recommended inserting a new Australian Privacy Principle (APP) into the Privacy Act, requiring APP entities to provide a simple mechanism for individuals to request the destruction or de-identification of personal information provided to the entity by the individual.[212]

Although incorrectly labelled as a 'Right to be forgotten' by Facebook Australia, the proposed APP differs from that right in that it would not allow consumers to request that information *others* had

---

[205] Jeffrey Chester, executive director of the Center for Digital Democracy, quoted in Grant Gross, 'Facebook rolls out privacy education for new users', *CIO* (online), 2 November 2012, <http://www.cio.com.au/article/440896/facebook_rolls_privacy_education_new_users/>.
[206] Ibid.
[207] Seda Gurses, Camela Troncoso and Claudia Diaz, 'Engineering Privacy by Design', (Paper presented at Computers, Privacy and Data Protection, CPDP 2011 Conference) <http://www.cosic.esat.kuleuven.be/publications/article-1542.pdf>, p.6.
[208] The themes underpinning privacy engineering have been most succinctly articulated by Canada's Information and privacy Commissioner, Ann Cavoukian in her 7 foundational principles of 'Privacy by Design':

1. *Proactive not reactive, Preventative, not Remedial*
2. *Privacy as the default*
3. *Privacy Embedded into Design*
4. *Full functionality - Positive Sum not Zero Sum*
5. *End-to-end security - Lifecyle Protection*
6. *Visibility and Transparency*
7. *Respect for User Privacy*

For further detail, see http://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/
[209] Josh Constine, 'Facebook admits users are confused about privacy, will show more on-screen explanations', *TechCrunch* (online), 8 April 2014, <http://techcrunch.com/2014/04/08/facebook-privacy-settings/>.
[210] OAIC, *Mobile Privacy: A better practice guide for mobile app developers,* September 2013, <http://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-guides/better-practice-guide-for-mobile-developers.pdf>.
[211] Sarah Spiekermann and Lorrie Faith Cranor, 'Engineering Privacy' (2009), 35:1 *IEEE Transactions on Software Engineering* 67, p.72.
[212] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Area*, Discussion Paper No 80 (2014), p.223.

provided on them be destroyed or de-identified. The recent approval of the more stringent 'Right to be forgotten' in the European Union[213] and the attendant angry ripostes from American lawmakers[214] will likely infect Australian discussions on the ALRC proposal. They shouldn't.

The ALRC proposal would provide consumers with the fundamental control over their personal data which they should be afforded, particularly in light of the increasing amounts of this data that is collected today and the myriad security threats to it. While there is room for sympathy for industry, which might be forced to fund this mechanism and ensure its smooth running,[215] the fundamental need for such a provision trumps these considerations.

The suggestion from AMTA and Communications Alliance that APP 11.2, referencing the destruction or de-identification of information when an entity no longer has a business need for it, somehow negates the need for this new APP 13 is flawed. In order to properly empower consumers in their interactions with their own personal data, the de-identify/destroy initiative must be theirs to employ. Perhaps there is no guarantee of complete erasure "in today's interconnected world"[216] but the prospect of ultimately elusive data should not compromise the prospect of consumer control over its originating source.

8. Looking forward: A Consumer Privacy Bill of Rights?

Finally, US President Barack Obama presented a blueprint for a Consumer Privacy Bill of Rights in a 2012 data privacy report,[217] support for which was recently reiterated in a 'Big Data' report.[218] A recommendation to adopt such a Bill of Rights in Australia is here presented in qualified terms, acknowledging the significant public consultation and legislative processes necessary before it might become a reality. Regardless of whether a data retention regime is introduced in Australia, many of the principles central to the proposed American Consumer Privacy Bill of Rights would represent valuable additions to the Australian consumer landscape.

---

[213] Note that the EU-approved 'right to be forgotten' is not actually a right to be forgotten, either. Instead, it is a right to have search engines forget particular information. Consumers have no right to have offending material taken down at the original source of the material. For more detail, see http://blogs.wsj.com/riskandcompliance/2014/06/04/right-to-be-forgotten-could-apply-beyond-search-engines/

[214] "Americans will find their searches bowdlerized by prissy European sensibilities," said Stewart Baker, former assistant secretary for policy at the U.S. Department of Homeland Security. Quoted in Martha Mendoza and Toby Sterling, 'Europe's new Google rule has many Americans angry and confused', *Huffington Post* (online), 25 May 2014, <http://www.huffingtonpost.com/2014/05/25/europes-google-search_n_5389148.html>.

[215] "This assessment is not always straightforward, particularly where there could be information connected with the personal information to be removed that is not covered by the removal obligation." AMTA and Communications Alliance, Submission No 101 to Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era Discussion Paper 80*, May 2014, p.7.

[216] Facebook, Submission No 65 to Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era Issues Paper 43*, 23 December 2013, p.7.

[217] White House, *Consumer data privacy in a networked world: A framework for protecting privacy and promoting innovation in the global digital economy,* February 2012, <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>.

[218] White House, *Big Data: Seizing opportunities, preserving values,* May 2014, <http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf>.