Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014

Submission by the Australian Communications Consumer Action Network to the Parliamentary Joint Committee on Intelligence and Security

January 2015

Australian Communications Consumer Action Network (ACCAN)
Australia's peak telecommunications consumer organisation
Suite 4.02, 55 Mountain St, Ultimo NSW 2007
Tel: (02) 9288 4000 | TTY: (02) 9281 5322 | Fax: (02) 9288 4019
www.accan.org.au | info@accan.org.au | twitter: @ACCAN_AU

About ACCAN

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

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

Contact

Katerina Pavlidis
Grants and Research Officer

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

Contents

1. Introduction

1.1. Overview

ACCAN would like to thank the Parliamentary Joint Committee on Intelligence and Security for the opportunity to comment on the *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (the Bill).

ACCAN recognises that in many cases access to metadata by criminal law enforcement agencies is legitimate and necessary. However, we want to ensure that a data retention regime does not unduly increase the cost of phone and internet services for consumers, or act as a barrier to a competitive telecommunications market. We also believe that the need to establish robust and independent oversight mechanisms is crucial to ensuring that Australians' right to privacy is not compromised by this Bill. This includes transparent, frequent and consistent reporting to Parliament, and limiting the Attorney-General's discretion to add agencies or bodies to the list of "criminal law-enforcement agencies" that can access metadata without a warrant. This will ensure that bodies administering laws imposing pecuniary penalties or revenue laws, such as the ATO and ACCC, do not once again have warrantless access to Australians' data. Sufficient safeguards for the security of metadata are also necessary considering the sensitive nature of the data and the risk of unlawful access to the data. Such safeguards should consider how the misuse of information and the risk of data breaches, in particular, can have serious and detrimental impacts on the lives of individuals.

The Bill also raises questions on whether a universal data retention regime, which collects data on every Australian, is necessary and proportionate, when a more targeted approach (such as a preservation notice scheme) could achieve many of the same objectives.[1]

1.2. Recommendations

Recommendation 1: That the cost estimates, as outlined in the commissioned PwC report, are made publicly available and, if necessary, redacted but only to the minimum extent necessary to protect other interests.

Recommendation2: That the federal government covers the costs of a data retention scheme.

Recommendation 3: If the government does not cover the entire cost of a data retention regime (as per Recommendation 2), that the government subsidies are proportional to the subscriber base of the telecommunications provider, through a scaled subsidy arrangement.

Recommendation 4: That the Bill is amended to give the Attorney-General or Minister discretion to add an entity to the list of criminal law enforcement entities through an amendment to the TIA Act, rather than via a legislative instrument.

[1] The submission made to the Committee by the Australian Privacy Foundation (APF) contains a more detailed discussion on necessary and proportionate alternatives to a universal data retention scheme.

Recommendation 5: That the agencies added to the list of criminal law enforcement agencies meet the definition of a body investigating serious offences, as defined in the TIA Act.

Recommendation 6: That these additional agencies are included in the data retention scheme's annual report which is tabled in Parliament. A justification for the inclusion of these agencies is also necessary to increase the public confidence in the scheme.

Recommendation 7: That the Attorney-General clarifies whether information sharing between government agencies and related organisations will be approved under the legislation.

Recommendation 8: That the annual report on the operation of the Bill includes a disclosure of the number of criminal investigations which accessed customer metadata without a warrant, as well as the number of requests granted within each of these investigations.

Recommendation 9: That the annual report also includes details on the number of warrants, arrests, prosecutions, and convictions (reasonably attributed to the use of metadata) which occurred.

Recommendation 10: That the government accounts for the high cost associated with establishing robust and secure information storage systems in its subsidy arrangements with telecommunications providers.

Recommendation 11: That the types of data to be collected (the data set) are defined in the legislation.

Recommendation 12: That a definition of 'content' is included in the legislation.

Recommendation 13: That the Attorney-General clarifies the jurisdiction of redress mechanisms for individuals affected by data breaches or other inappropriate access of metadata by federal and state criminal law enforcement agencies.

Recommendation 14: That the statutory obligation to retain data is limited to 6 months, and that this timeframe is reviewed 3 years after the data retention scheme's implementation phase, in line with a wider review of the Bill.

2. Cost

2.1. Cost estimates

ACCAN understands that the Attorney-General's Department (AGD) has twice engaged PricewaterhouseCoopers (PwC) in the last three months to calculate the costs associated with a data retention scheme and to develop a funding model for government to contribute to these costs. Furthermore, the Data Retention Implementation Working Group, a government and industry partnership, will continue to work on developing an accurate understanding of costs throughout December 2014 and January 2015. However, despite this, no information has been made publicly available on initial cost estimates or the factors the cost estimates are taking into consideration. As such, ACCAN has largely based its arguments on a number of cost estimates provided by telecommunications providers in the past.

In 2012, Telstra identified that data retention involves costs associated with several distinct activities:[2]

- Collating data
- Storing data
- Securing data to maintain data integrity for both consumers and for agency investigative purposes
- Making data available to agencies in a form that can be used for their investigations
- The destruction of that data after the life-cycle of retention has expired
- Agencies manipulating and investigating data

In summary, set up costs are fixed and incremental (depending on the size of the platform), and then ongoing operating costs are taken into account.

An internal Optus memo pointed out that, while it stores various types of data for various periods, much of it was not in a form that could be readily accessed by law enforcement agencies. The memo said that an "over-arching data-retention regime…with rapid or automated inquiry capability would be a non-trivial change and cost". It went on to explain that "[b]ased on work done in 2010 and refreshed in 2012, a data-retention regime could cost Optus in the order of $30-plus million to $200-plus million, depending on a range of assumptions about scope and definition."[3]

[2] 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)

3 http://www.afr.com/p/technology/optus_facing_bill_for_abbott_policy_ROfOdbG70YGjRhdoRuw0QK

With metadata volumes doubling every two years, iiNet estimated that the cost of complying with a data retention scheme could be $100 million over two years. The company estimated that this would see consumers affected by price rises of $5 to $10 a month.[4]

Similarly, the telecommunications industry peak body, Communications Alliance (CA), has estimated that the setup cost to industry may be around $100 million. With the inclusion of source and destination IP addresses, the setup costs would be likely to approach a figure in the region of $500 million to $700 million. CA has observed that the inclusion of a single additional data element has the potential to increase the capture and retention cost by tens of millions of dollars.[5]

These figures were calculated before the release in December 2014 of the draft data set, so of necessity they are estimates only.

At this stage, we are concerned that there is contradictory evidence of the cost of the scheme. The Attorney-General Department's websites states that, "international experience indicates that the cost of mandatory data retention schemes is small."[6] However, this claim unsubstantiated when viewed in the context of the UK experience.[7] The estimated cost of the UK 2014 revised data retention scheme was relatively small at £8.4 million, annually, because "the infrastructure to support the retention and storage of data by Communications Service Providers, and the secure and reliable transmission of data, already exists."[8] However, by contrast the scheme proposed under the UK's failed Communications Data Bill (2012) was priced at £1.8 billion over ten years.[9]

As the recent PwC report, has not been made publicly available or tabled in Parliament due to commercial confidentiality, more precise cost estimates are not available. ACCAN believes that a redacted version of the report – which removes the information concerned with commercial confidentiality and market sensitivity – should be made public in the interests of open and transparent evidence-based policy development. This will allow Australians, including policy-makers and telecommunications providers, to make an informed judgement about the Bill's validity and potential impact on business practices.[10]

> Recommendation 1: That the cost estimates, as outlined in the commissioned PwC report, are made publicly available and, if necessary, redacted but only to the minimum extent necessary to protect other interests.

---

[4] http://www.smh.com.au/it-pro/government-it/data-retention-scheme-would-lead-to-surveillance-tax-on-consumers-say-telcos-20140729-zy4ch.html

[5] AMTA and Communications Alliance, Submission No 114 to PJCIS Inquiry, 2012, p.14

[6] http://www.ag.gov.au/NationalSecurity/DataRetention/Pages/Mythsandfacts.aspx

[7] http://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/FlagPost/2014/December/Costing_data_retention

[8] http://www.google.com.au/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CB8QFjAA&url=http%3A%2F%2Fwww.legislation.gov.uk%2Fukia%2F2014%2F266%2Fpdfs%2Fukia_20140266_en.pdf&ei=Vh2JVI7CHITpmQX1hoLIBQ&usg=AFQjCNGihXRDC8hDXYG_hkHMqKopzE3glg&bvm=bv.81456516,d.dGY

[9] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97999/communications-data-ia.pdf

[10] It is common for telecommunications providers to release redacted versions of commercial-in-confidence information. For example, where the ACCC undertakes access price determinations for telecommunication providers' assets and infrastructure, providers commonly release information in order to allow the ACCC to judge the cost of regulated assets. A redacted version of this information is then typically publicly released.

2.2. Covering the costs

When the Minister for Communications, Malcolm Turnbull, introduced the Bill into Parliament at the end of October, he said that the government "expects to make a substantial contribution to both the cost of implementation and the operation of the scheme."[11] This echoes the recommendation of the 2013 PJCIS report on national security and data retention, which was that "the costs incurred by providers should be reimbursed by the Government."[12]

The information available suggests that the costs associated with the scheme are not marginal per user but are predominately fixed for each telecommunications provider. As such, it is likely that smaller providers – with fewer users – would have to pass on a disproportionately higher cost to their customers. ACCAN is concerned that these costs will detrimentally impact on low-income consumers. Research indicates that many low-income consumers struggle to pay for their telecommunications services. For example, research conducted by ACCAN and Anglicare in 2013 found that two-thirds of low-income mobile phone users had difficulty paying their account and 62 per cent of those with a pre-paid account ran out of credit sooner than expected.[13] This demonstrates that any increase in phone and internet prices, arising from costs imposed by a data retention scheme, could place a significant strain on this group of consumers. Therefore, to ensure that costs passed on to consumers are minimised, ACCAN supports the view that government should bear the cost of the mandatory data retention scheme. Furthermore, in line with the public policy theory of user-pays, the federal government should cover the costs because the scheme is being implemented as a policy objective of the government rather than of the telecommunications industry. Government funding, while falling on taxpayers, would be less regressive than necessitating recovery from consumers.

Government funding could be implemented in two ways, as suggested by ACCAN member the Internet Society of Australia (ISOC-AU):

- Relevant law enforcement and national security agencies could subsidise the telecommunications provider's capital implementation costs and pay the true cost of each access request they make; and
- A public subsidy could be made available to telecommunications providers and calculated and allocated in an effective manner.[14]

> Recommendation 2: That the federal government covers the costs of a data retention scheme.

[11] http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;db=CHAMBER;id=chamber%2Fhansardr%2F4a3ea2e7-05f5-4423-88aa-f33e93256485%2F0010;query=Id%3A%22chamber%2Fhansardr%2F4a3ea2e7-05f5-4423-88aa-f33e93256485%2F0009%22

[12] www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/report/front.pdf

[13] https://accan.org.au/our-work/research/711-affordability-for-low-income-consumers

[14] http://www.isoc-au.org.au/Media/ISOC-AU_Ten_questions_metadata_retention20140806.pdf

2.3. The barriers to competition

At June 2013 there were 419 Internet Service Providers (ISPs) operating in Australia. Of those, 215 had 1–100 subscribers, 127 had 101–1,000 subscribers, 51 had 1,001–10,000, and 17 had 10,001–100,000 subscribers.[15]

As indicated above, if the cost of implementing a data retention scheme is dominated by fixed costs, rather than being proportional to the size of the telecommunications carrier, smaller providers would be disproportionately affected by higher costs, because the cost would be spread across a smaller customer base. If these marginal costs force smaller operators out of the market, this could negatively affect competition in the Australian telecommunications market and reduce consumer choice. We are also concerned that adding a significant financial burden on telecommunications providers could result in smaller providers, in particular, cutting corners in other important areas, such as customer service.

In order to ensure that the introduction of a metadata retention scheme has a neutral impact on competition, government should introduce a scaled subsidy arrangement proportional to the subscriber base of the telecommunications provider.

> Recommendation 3: If the government does not cover the entire cost of a data retention regime (as per Recommendation 2), that the government subsidies are proportional to the subscriber base of the telecommunications provider, through a scaled subsidy arrangement.

[15] http://www.acma.gov.au/theACMA/Library/Corporate-library/Corporate-publications/communications-report-2012-13

3. Oversight and Accountability

Communications data can reveal personal information about an individual, even without the content of a communication being made available. For example, revealing who a person is in contact with, how often and where can help to paint a picture of that person's political opinions, sexual habits, religion or medical conditions. The European Court of Justice has explained that metadata, "taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons who data has been retained such as the habits of everyday life, permanent or temporary places of residence, daily or other movements…"[16] As such, metadata is not innocuous and can reveal highly sensitive and personal information about individuals. It is important, therefore, that a mandatory data retention regime is subject to rigorous oversight and accountability measures to ensure that Australians' right to privacy is not compromised.

3.1. Authorisation and access

ACCAN acknowledges that the Bill proposes to limit the number and types of entities that will be authorised to access metadata without a warrant. The Bill, however, also gives the Minister or the Attorney-General the discretion to add entities to this list, through a "legislative instrument". ACCAN recommends that the Attorney-General or Minister adds an agency to the list of criminal law enforcement agencies through an amendment to the Act, rather than via a legislative instrument. This will ensure that this process is subject to full parliamentary scrutiny. Furthermore, entities added to the list of criminal law enforcement agencies must meet the definition of an entity investigating serious offences, as defined in s 5D of the TIA Act.

Recommendation 4: That the Bill is amended to give the Attorney-General or Minister discretion to add an entity to the list of criminal law enforcement entities through an amendment to the TIA Act, rather than via a legislative instrument.
Recommendation 5: That the agencies added to the list of criminal law enforcement agencies meet the definition of a body investigating serious offences, as defined in the TIA Act.
Recommendation 6: That these additional agencies are included in the data retention scheme's annual report which is tabled in Parliament. A justification for the inclusion of these agencies is also necessary to increase the public confidence in the scheme.

A further risk exists that metadata could be shared between various agencies – those with warrantless access and those without. For example, the *Telecommunications (Interception and Access) Act 1979* (the TIA Act) and the *Australian Security Intelligence Organisation Act 1979* include information sharing provisions which allow the Australian Secret Intelligence Service to receive information gained by ASIO through the TIA Act.[17] Therefore, the data retention regime might allow data that is disclosed for an authorised purpose to be used for unrelated purposes through

[16] www.aph.gov.au/~/media/Committees/Senate/committee/humanrights_ctte/reports/2014/15_44/15th%20Report.pdf

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

information sharing between those defined as 'criminal law enforcement agencies' in the Bill and other agencies that cannot lawfully access data without a warrant.

> Recommendation 7: That the Attorney-General clarifies whether information sharing between government agencies and related organisations will be approved under the legislation.

3.2. Transparent reporting

ACCAN welcomes new accountability measures in the Bill including an increase in the oversight powers of the Commonwealth Ombudsman. Clear, consistent and transparent reporting is required for consumers to understand the extent and scope of the data retention scheme. These changes include the introduction of an obligation for law enforcement agencies to keep records in relation to their access of stored telecommunications data. The maintenance of these records, for a period of three years, will assist the Ombudsman to assess enforcement agencies' compliance against the exercise of their powers under Chapters 3 and 4 of the TIA Act[18] and is an important oversight function. The Bill contains a requirement for the Minister to report annually on its operation to Parliament. However, the Bill does not specify that criminal investigations without a warrant, arrests, prosecutions and convictions associated with metadata requests be reported separately. Separate reporting for metadata will allow an evaluation of the effectiveness of the scheme, and increase public accountability of requesting agencies.

> Recommendation 8: That the annual report on the operation of the Bill includes a disclosure of the number of criminal investigations which accessed customer metadata without a warrant, as well as the number of requests granted within each of these investigations.
> Recommendation 9: That the annual report also includes details on the number of warrants, arrests, prosecutions, and convictions (reasonably attributed to the use of metadata) which occurred.

3.3. Protecting consumers against data breaches

No information storage system is ever completely secure and the larger the data set, the more attractive it will potentially be to hackers. Unintentional data breaches can also occur as a result of inadequate security measures. In its recently published annual report for the 2013-14 financial year, the Office of the Australian Information Commissioner (OAIC) reported that it had received a record number of data breach complaints against government agencies and private companies. Overall, 4239 privacy complaints were received – an increase of 183.3% over the figures reported in 2012-13.[19]

The increase in complaints about data breaches is concerning because it demonstrates that data is not always securely stored and data breaches are increasingly affecting consumers. Maintaining

[18] http://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r5375_ems_e6cf11b4-5a4e-41bc-ae27-031e2b90e001/upload_pdf/14242b01EM.pdf;fileType=application%2Fpdf

[19] http://www.oaic.gov.au/images/documents/about-us/corporate-information/annual-reports/annual-report-2013-14/Office-of-the-Australian-Information-Commissioner-Annual-report-2013-14.pdf

metadata in a highly secure system and to a standard that meets evidentiary requirements is a significant safeguard against data breaches for consumers, but the required security could be both costly and difficult for many smaller telecommunications providers.

> Recommendation 10: That the government accounts for the high cost associated with establishing robust and secure information storage systems in its subsidy arrangements with telecommunications providers.

3.4. Draft data set

The draft data set outlines the kinds of information (metadata) to be retained by telecommunications providers. The data set has not been specified in the Bill as the government wants to ensure "necessary technical detail to provide clarity to telecommunications service providers about their data retention obligations while remaining sufficiently flexible to adapt to rapid and significant future changes in communications technology." [20] For this reason, the Bill includes an in principle definition only, and the data set is to be included in regulation. ACCAN acknowledges that any data retention scheme and accompanying draft set need to respond sufficiently and in a timely manner to technological change in the telecommunications industry.

However, the Parliamentary Joint Committee on Human Rights has, recommended the data set be included in the Bill "to avoid the arbitrary interference with the right to privacy that would result from reliance on regulations…"[21] ACCAN agrees that the data set should be included in legislation rather than regulation, not only to ensure that the arbitrary interference with privacy is negated, but also to subject the data set to greater scrutiny by both Houses of Parliament. It is important that the categories of information to be collected on Australians cannot be changed arbitrarily and are instead subject to rigorous Parliamentary scrutiny. We are further concerned that in the absence of an explicit definition of content in the Bill that there is a possibility of scope creep which could result in retained data including aspects of content.

Finalising and including the data set in legislation will also ensure that the mandatory data retention regime is transparent. Individuals, including policy-makers and telecommunications providers, will be aware of the exact nature of data set from the outset of the Bill. The Communications Alliance notes in its submission on the Bill that capturing the data set in legislation will also better safeguard it against 'scope-creep'[22]. We share this concern. If the data set is defined in legislation, rather than regulation, it is less likely that it will broaden over time without adequate scrutiny.

> Recommendation 11: That the types of data to be collected (the data set) are defined in the legislation.
> Recommendation 12: That a definition of 'content' is included in the legislation.

---

[20] parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r5375_ems_e6cf11b4-5a4e-41bc-ae27-031e2b90e001/upload_pdf/14242b01EM.pdf;fileType=application%2Fpdf, p. 7

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

[22] www.aph.gov.au/DocumentStore.ashx?id=ed7a9668-6613-4f69-8fae-e2bf741eb9d2&subId=302386

3.5. Federal and state privacy legislation

While obligations to prevent the disclosure of information under the TIA Act do exist, the *Privacy Act 1988* has a much more comprehensive framework of privacy principles that agencies must comply with. This framework has been strengthened recently by the introduction of the Australian Privacy Principles (APPs) in March 2014. The *Privacy Act* also allows individuals to seek redress that can involve fines or sanctions imposed by the Privacy Commissioner. However, the jurisdiction of the Privacy Act is Commonwealth, and does not apply to state government agencies. Consequently, none of its protections will apply if state government agencies misuse personal information.[23] Instead, individuals whose metadata has been inappropriately accessed or leaked will have to seek recourse within state or territory regimes, which differ in their effectiveness, adding to an already complex interaction of state and federal powers.

> Recommendation 13: That the Attorney-General clarifies the jurisdiction of redress mechanisms for individuals affected by data breaches or other inappropriate access of metadata by federal and state criminal law enforcement agencies.

[23] http://www.oaic.gov.au/privacy/privacy-topics/government/do-the-australian-privacy-principles-apply-to-local-councils-or-state-or-territory-governments

4. Retention Period

4.1. Two year retention period

The Bill includes a statement of compatibility with human rights in the Explanatory Memorandum. This refers to evidence from European data retention regimes and states that, "frequently data accessed by agencies was less than six months old." The Parliamentary Joint Committee on Human Rights has also questioned whether a data retention period of two years is a proportionate period as it may go beyond the period necessary to achieve the scheme's legitimate objective. The joint Communications Alliance and AMTA submission to this inquiry provides a snapshot of the data retention periods of European Union countries, which are typically between 6 months and 12 months. Furthermore, in the UK, for example, 74 per cent of disclosures related to data that was less than 3 months old.[24] Considering the arguments that metadata accessed by law enforcement and security agencies is generally less than 6 months old, the University of New South Wales's Gilbert and Tobin Centre of Public Law has argued that a stronger justification for the two-year timeframe, "could help to reduce public perceptions that the Bill is designed to allow mass surveillance of the population."

> Recommendation 14: That the statutory obligation to retain data is limited to 6 months, and that this timeframe is reviewed 3 years after the data retention scheme's implementation phase, in line with a wider review of the Bill.

[24] http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Data_Retention/Submissions