Submission to the Parliamentary Joint Commission on Intelligence and Security

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

Introduction

Thank you for the opportunity to make a submission to the inquiry on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (“the Bill” or “the Data Retention Bill”). We note the short time frame available for submissions over the New Year period and trust that submissions received will be given due consideration.

This submission is on behalf of and jointly authored by FutureWise. We are a group of Australian professionals of varied backgrounds who seek to promote ideas which improve the long-term direction of Australia, particularly in the areas of technology and health. More information about FutureWise is available on our website.[1] We are happy to provide further clarification of any of the points in the submission, or for one of the authors to attend the hearing in person if required.

[1] https://www.futurewise.org.au

Summary of Submission

We believe that the Bill in its present form is unworkable and should not proceed. In particular, the fact that key components of the data retention regime are not defined in the Bill but will be left to regulation means that it is impossible to have a meaningful consultation with stakeholders until the final data set is known.

Our concerns with the Bill in its current form in summary are:

Effectiveness of the proposed data retention regime

- Utility of data retention
- Futility of scheme given services not covered
- Technical feasibility

Secondary impacts of the bill

- Impact on personal privacy & presumption of innocence
- Warrantless access to personal data
- Cost implications (for ISPs and end users)
- Obligation includes creation of data
- Data creation includes a high resolution map of the location of every mobile user in Australia for a minimum of 2 years
- Length of retention period not necessary or proportionate

Legislative Issues

- Key dataset left to regulation
- Scope of agencies that can access the data left to be determined by the Minister
- Not limited to serious crime or national security
- Total lack of safeguards against unlawful or inadvertent disclosure or use of retained data
- Total lack of safeguards around the destruction of retained data.

The issues identified with this bill and its far-reaching impact on citizens, communications providers, and the relationships between the government and these groups mean that the Bill should undergo a far more extensive and rigorous discussion in the public domain. The remainder of the submission will discuss these areas in more detail.

The government has not yet made the case that mass data retention is necessary, reasonable, or proportionate. In any event, the scheme as it is articulated in this Bill is fundamentally flawed and should not be passed.

FutureWise believes that there are substantial issues with the telecommunications intercept and access bills. The original Bill was passed in 1979 and we feel that attempting to fix the identified issues by adding another layer of legislation, represents a “band-aid” rather than a long-term solution, a comprehensive and holistic review is required. Furthermore, the government has seemingly ignored the recent submissions from the public and from carriage service providers to the JCIS which overwhelmingly opposed mandatory data retention.

Telecommunications data is not "the envelope"

A major failing of the Bill is that it does not adequately detail what "telecommunications data" will be retained under the regime,[2] but instead leaves this to be done by regulation. The proposed dataset was further refined by a working group (consisting largely of bureaucrats and representatives of law-enforcement agencies, with only three members from the communications industry). Leaving the definition of the dataset out of the legislation and relegating it to regulatory control reduces parliamentary oversight and could too easily lead to scope creep.

The explanatory memorandum makes an unclear distinction between "content" and "telecommunications data" but does not provide evidence to support its assertion that "telecommunications data is less privacy intrusive than content".[3] In fact, the Government's own words in its 2010 consultation paper[4] contradict this assertion: "In some situations, telecommunications data can be of equal or even greater benefit than the content of communications."

FutureWise wishes to directly challenge the assertion that telecommunications data is "less privacy intrusive than content" as this is not true generally for any given set of telecommunications data, but in particular the dataset proposed by the Attorney-General's Department and further refined, we understand, by the working group.

Senior members of the United States National Security Agency (NSA) have revealed the intrusive nature of this telecommunications data on privacy - the former general counsel, Stewart Baker said that "metadata absolutely tells you everything about somebody's life".[5] General Michael Hayden (previously the director of both the NSA and the Central Intelligence Agency - CIA) said "we kill people based on metadata".[6]

---

[2] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, s 187A(2)(a). Available online:

http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fbills%2Fr5375_first-reps%2F0001%22;rec=0

[3] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, Explanatory Memorandum; General Outline, s10. Available online: http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fems%2Fr5375_ems_e6cf11b4-5a4e-41bc-ae27-031e2b90e001%22

[4] Carrier-Carriage Service Provider Data Set Consultation Paper Version 1.0. Available online at: http://media.cnetnetworks.com.au/audio/musiccentre/Technolatte/dataretention-20100309-withredactions-02.pdf

[5] Quote from: http://www.nybooks.com/articles/archives/2013/nov/21/snowden-leaks-and-public/

[6] Johns Hopkins Foreign Affairs Symposium: The Price of Privacy. Video available online at: https://www.youtube.com/watch?v=kV2HDM86XgI

Examples of how intrusive this telecommunications data are can be seen where individuals have volunteered to have their own data made available online. In 2009, a politician from the German Green Party requested his telecommunications data from Deutsche Telekom. This was then linked with information already available on the internet (for example, social media posts and news websites) to provide a very comprehensive map of his movements over six months.[7]

Even without such a long period of time or the use of other public information, telecommunications data is very revealing. Even a single week of this data allows a comprehensive profile of an individual to be compiled, as was shown in July last year by a lawyer working for the European digital rights group Bits of Freedom.[8]

Based on the broad definition of the telecommunications data in the Bill and the proposed dataset, the information collected could be interpreted such that the information from a mobile phone merely connecting to the network towers would be considered telecommunications data. 4G mobile phones include high resolution location data when they connect to mobile network towers, and these "pings" occur frequently. In fact, the background operations of almost all phone handsets (e.g. checking and sending email) meet the draft standard for telecommunications data and would provide location information. The result of this telecommunications data is that a mobile phone will act as a continuously active motion tracker, providing the full history of a person's movement at all times the mobile device is switched on. This represents an extremely concerning new police power, and is of such major privacy impact that we feel it is worth a full and frank public discussion on its own. This aspect of the Bill has not been discussed publicly, with statements from the Attorney-General (and others) focussing on the privacy of internet browsing history rather than the intrusiveness of panopticon-like continuous surveillance.

Despite the assurances of LEAs, the AGD, and the Attorney-General himself, telecommunications data is extremely privacy intrusive. It should be given the same legal protection as content with judicial oversight, such as a warrant, being required before access to this data is provided by a service provider.

---

[7] http://www.zeit.de/datenschutz/malte-spitz-data-retention/

[8] https://www.bof.nl/2014/07/30/how-your-innocent-smartphone-passes-on-almost-your-entire-life-to-the-secret-service/

Effectiveness of the data retention regime

Law enforcement and national security agencies are vocal advocates of the measures described in this bill, stating that they are “essential” for their law-enforcement activities.[9] However, no robust evidence to support such assertions has been supplied. Public comments by these agencies and the publicly available submissions to this committee confirm that access to this data is frequent but in no way confirms that it is either necessary or effective in preventing crime. Necessary is a different test than useful.

Given the wide-ranging impact of the Bill on personal privacy (see below), we believe that there must be demonstrated evidence that the loss of privacy and impact on freedom of expression, association and speech, associated with what effectively amounts to a mass-surveillance scheme is outweighed by the benefits in community safety due to effective policing and counter-terrorism. To date, this has not been proven. Furthermore, submissions by police to this inquiry seem to suggest that this would not be able to be proven given that law enforcement agencies are unable to even quantify how many times this data has been accessed.[10] This failure of record-keeping and accountability is not addressed in this Bill and should be fully considered in a broader review of the TIA Act. We believe that it is unacceptable that this data should be used without any record-keeping or accountability by the law enforcement agencies.

In 2013, the Privacy and Civil Liberties Oversight Board found that there is little evidence that the metadata program has made the US safer. In the Australian context, the former Victorian Privacy Commissioner has expressed scepticism as to whether data retention would aid law enforcement and national security agencies due to the incentive such a scheme would provide to anonymise communications.

Representatives appearing on behalf of the UK before the CJEU in July 2013 conceded there was no scientific data to underpin the claimed need for data retention. The UK’s Open Rights Group has reported that a 2012 case used to justify data retention in the UK was not a communication data problem as alleged but a failure to properly investigate the murder. In fact the case showed that diligent and proactive use of targeted data preservation could both prevent and detect crime.[11]

The proposed data retention regime does not cover all possible means of communicating using the internet, and also fails to take into account the widespread easy availability of

---

[9] http://www.abc.net.au/news/2014-02-27/federal-police-call-for-more-access-to-metadata/5286596

[10] http://www.theguardian.com/world/2014/dec/29/metadata-most-australian-police-forces-cant-say-how-many-times-it-has-been-used-to-prevent

[11] https://www.openrightsgroup.org/blog/2012/evidence-for-the-cdb

tools for anonymising internet access (many of which have come into existence as a direct result of measures like the ones suggested by this bill).[12]

Range of services and providers that won't be covered

Over-the-top services such as Skype, social media networks, and email services such as Gmail will not be covered by this Bill. Nor will overseas communications providers or peer-to-peer encrypted VOIP applications - given that many companies providing these internet services are based overseas, rather than in Australia, the bill is flawed in design even prior to its implementation. These are very commonly used methods of communication and if they offer a simple method to avoid a user's data being caught in warrantless surveillance, it would be reasonable to assume that they will only increase in popularity.

Further, the Australian Government's NetAlert national filter scheme was able to be bypassed by a teenage internet user in around half an hour.[13] The use of Virtual Private Networks (VPNs) and offshore hosting in countries will still allow people who wish to reduce their surveillance footprint to do so.

The Bill fails to address the potential for future developments in internet communication technology. Given the rapid pace of technological change over the last twenty years, any measure which does not attempt to solve a problem in a technology-neutral way can only be doomed to failure. There is no material difference between a person communicating via a fixed-line telephone, a mobile telephone, using some sort of voice-over-IP application. To attempt to treat these communications differently because of the involvement of the Internet represents a fundamental flaw in the development of law enforcement measures. Surveillance should not occur merely because it is possible, but have a demonstrated need.

False positive screening

The mass collection of this surveillance data also raises issues around signal-to-noise ratio. A significant volume of data will be retained (see below, under Impacts on ISPs). Collected data however, does not become intelligence until it is analysed. Clearly, it is not feasible to analyse this volume of data as it is collected without the use of automated systems - such as the Unified Targeting Tool[14] used by the United States National Security Agency, as revealed by Edward Snowden in his intelligence leaks.

---

[12] https://freedom.press/

[13] http://newsweekly.com.au/article.php?id=3229

[14] http://en.wikipedia.org/wiki/Unified_Targeting_Tool

Automatic analysis of data also runs the very significant risk of false positive flagging - that an Australian citizen's communications may be identified as being of interest to law enforcement agencies, despite there being no crime planned or having been committed. This "false-positive" alarm is for statistical reasons, much more likely than the correct identification of a random terrorist based on telecommunications data.[15] Assuming that the data is not being manually screened (due to volume) or automatically screened (due to low strike-rate or false-positives), then the purpose of the retained data must be to have a pool of data available for law enforcement agencies to access when they have suspicion that a persons' telecommunication data may be required.

This risk of false positives is not just a theory. As recently as 2007 the AFP and ASIO were responsible for falsely imprisoning and interrogating Dr Mohammed Haneef, an Indian-national medical doctor working at a Queensland Hospital.[16] These actions were based solely on the fact he gave a mobile phone Subscriber Identity Module (SIM) card to his cousin (one year prior to his cousin being involved in a terrorist event). Dr Haneef was detained without charge for twelve days. The Clarke review[17] found that there were:

> "mistakes of detail, but they were in the main the results of the need to rely on overseas information and what I think were the inadequate systems of evidence recording employed"

We have not yet been provided with evidence that demonstrates that our law enforcement agencies have the technical capability to analyse and use the more complicated internet-related data set out in the draft data set. Data only becomes intelligence when it is sorted and analysed in a meaningful way. As we will discuss later in the submission, law enforcement agencies in Australia are not currently even able to quantify their access to this telecommunications data. This suggests that the results of the Clarke report are yet to result in a change in the law enforcement agencies' handling of this data.

Overseas Experience of Mandatory Data Retention

The Attorney General's Department on its website has stated: "more than 25 countries around the world have implemented data retention laws similar to those proposed by the Australian government".

---

[15] http://www.r-bloggers.com/how-likely-is-the-nsa-prism-program-to-catch-a-terrorist/

[16] http://www.lawcouncil.asn.au/lawcouncil/index.php/10-divisions/145-mohamed-haneef-case

[17] http://pandora.nla.gov.au/pan/84427/20090121-0022/www.haneefcaseinquiry.gov.au/www/inquiry/rwpattach.nsf/VAP/(3A6790B96C927794AF1031D9395C5C20)_Volume+1+FINAL.pdf/$file/Volume+1+FINAL.pdf

In the proposed data set,[18] it is also noted that the categories of data in the Bill "are based closely on the European Union data retention directive".

What is missing is any acknowledgment that:

- most if not all of these "25 countries" are EU Member States[19] and
- the Court of Justice of the European Union ruled in April last that the EU Data Retention Directive:[20]

> entails a wide-ranging and particularly serious interference with the fundamental rights to respect for private life and to the protection of personal data, without that interference being limited to what is strictly necessary.

The Bill fails to address the numerous flaws identified with the EU Data Retention Directive by the Court of Justice of the European Union (CJEU).

As the EU Parliament's legal opinion confirmed, in practice, the CJEU ruling means that any legislation requiring retention of communications data by a Member State of the EU should now comply within the framework set out in the judgment. This framework includes, but is not limited to, the following principles:

- restrict retention to data that is related to a threat to public security and in particular restrict retention to a particular time period, geographical area and /or suspects or persons whose data would contribute to the prevention, detection or prosecution of serious offences (paragraph 59);
- distinguish between the usefulness of different kinds of data and tailor retention periods to the objective pursued or the persons concerned (paragraph 63);
- ensure retention periods are limited to that which is 'strictly necessary' (paragraph 64);
- restrict access and use of the data to the prevention, detection or prosecution of defined, sufficiently serious crimes (paragraphs 60-61).

---

[18] http://www.scribd.com/doc/244951610/Data-Retention-Draft-Data-Set-301014

[19] Communications Alliance - Submission 6 to this inquiry, Attachment 1

[20] http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

Substantial volumes of complex and broad categories of data can now be accessed in Australia under the TIA Act without a warrant. The justification that a warrant is not needed is that access to telecommunications data is less intrusive than other powers. This claim is no longer valid.

We agree with the recommendation of the Parliamentary Joint Committee on Human Rights that access to retained data be granted only on the basis of a warrant approved by a court or independent administrative tribunal, taking into account the necessity of access for the purpose of preventing or detecting serious crime on defined objective grounds. Furthermore, the previous Independent National Security Legislation Monitor, Bret Walker SC has stated that he holds the same opinion.[21] We believe that these are reasonable standards to adhere to, and should form the benchmark for access to telecommunications data by law enforcement agencies.

European experience shows that judicial oversight of access to telecommunications data is possible, with a 2011 report identifying 11 countries with various warrant requirements.[17] We have not yet been given appropriate evidence about why such a system is not feasible in Australia.

As is shown by the release of the EU Parliament's legal opinion[22] on the consequences of this ruling, Australia's data retention plans are looking increasingly out of touch.

---

[21] http://www.abc.net.au/news/2014-08-07/ex-national-security-monitor-concerned-by-proposed-terrorism-law/5653916

[22] https://www.accessnow.org/blog/2015/01/07/leaked-european-parliament-long-awaited-legal-study-on-data-retention

Secondary Impacts of the Bill

Law enforcement arguments in favour of mandatory data retention seem to distill down to two major justifications: 1) all persons are potential persons of interest and therefore data should be retained; or 2) telecommunications data should be readily available when there is a legitimate need for access to it.

If the first of these is true, then this Bill represents a major shift in the position of the Government on the presumption of innocence of Australian citizens. This itself is worthy of greater consideration than the submission period for this Bill allows.

If the second is true and law enforcement agencies would only access data on persons in whom they have a legitimate law enforcement interest, then the onus in an open and free democratic society must be on the law enforcement agencies to prove that they have this legitimate interest. The law enforcement agencies have not provided sufficient justification that, if access is required, it should be done without a warrant. That the Victorian Police, to cite just one example, access telecommunications data some 1200 times a week is very concerning. Are there that many legitimate targets involved in serious crime? Does the ease in which such access can be obtained lead to more disclosures than is strictly necessary? What is the outcome from these 1200 requests? How long is the data left on file?

To the extent that legislation requires retention of data relating to persons who will never be implicated in a criminal investigation, it causes a massive inefficiency, in that significant resources are required to collect, store, back-up, secure, and control access to a vast quantity of data The Commonwealth's position seems to be that they'd prefer private communications providers to bear the brunt of that inefficiency, rather than paying for it themselves. Communications providers will also bear the risk of such storage in the event of a data breach.

Writing about the UK's new data retention laws, academic Paul Bernal highlighted that the legislation:[23]

[23] http://paulbernal.wordpress.com/2014/07/12/drip-a-shabby-process-for-a-shady-law/

> still works on the assumption that there is no problem with collecting data, and that the only place for controls or targeting is at the accessing stage. This is a fundamentally flawed assumption – morally, legally and practically. At the moral level, it treats us all as suspects. Legally it has been challenged and beaten many times – consistently in the European Court of Human Rights, in cases from as far back as Leander in 1987, and now in the ECJ in the declaration of invalidity of the Data Retention Directive. Practically, it means that data gathered is vulnerable in many ways – from the all too evident risks of function creep that RIPA has demonstrated over the years (dog-fouling, fly-tippers etc) to vulnerability to leaking, hacking, human error, human malice and so forth. Moreover, it is the gathering of data that creates the chilling effect – impacting upon our freedom of speech, of assembly and association and so forth. This isn't just about privacy.

Impact on Privacy

The Bill contains no meaningful protections for privacy and data protection.

The retention obligations will displace Australian Privacy Principle 3.2 which provides that the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of the entity's functions or activities. Further, APP 11.2 which establishes requirements for entities to destroy or de-identify personal information where it is no longer needed is also trumped by this scheme. There are no requirements in this Bill governing when law enforcement agencies should destroy data they have accessed under the scheme. If this data deletion does not occur in a secure manner, then it creates a second cache of data that may potentially attract the interest of criminals.

The primary data storage by the communication carriage providers, and then secondary storage by law enforcement agencies will create concentrated collections of personally identifying data (see above) to facilitate identity theft. These datacentres through their stated goal of preventing crime, will in effect be honeypots for technologically savvy criminals. There no way an ISP can offer a complete guarantee of data security, as the numerous large-scale data breaches of 2014 clearly showed.[24] Even the law enforcement

[24] http://www.zdnet.com/pictures/2014-in-security-the-biggest-hacks-leaks-and-data-breaches/

agencies themselves are not immune to the risks of inadvertent data breaches - there were multiple breaches of the Australian Federal Police's data storage in 2014.[25,26]

The Bill appears to fail to consider this issue, as it does not impose any requirements for data security or privacy on the carriage service providers, but seems to rely on the provisions of the Privacy act. However, not all services providers will fall within the scope of the Privacy Act in which case there is little privacy protection at all.

The Government's view, consistent with Bernal's description above, is indicative of a form of exceptionalism: Privacy legislation affecting private companies heavily regulates the collection of private data, as well as its use, disclosure, and eventual destruction. But in relation to data retention, the Government's position is that there is no problem with unspecified collection of arbitrary data without the informed consent of the data's subject, and the only questions worth discussing concern how much should be stored and who can access it.

Consideration should also be given to the harm of providing new invasive privacy-related powers to police forces who have established a demonstrated track record of abusing the powers they already have. One recent example involves a NSW Ombudsman investigation into the unlawful bugging of approximately 120 NSW Police officers by their own Special Crime and Internal Affairs (SCIA) unit, which allegedly lied to a magistrate[27] to obtain warrants for the installation of listening devices.

When formulating a law, it is important to consider how it will be misused, as well as how it will be used. What new powers is mandatory data retention giving to corrupt police officers? In the UK, we have seen similar powers being used regularly to access data relating to journalist's communications, with journalists here echoing similar concerns.[28]

Cost & Regulatory Implications

The Australian communications industry is much more diverse than the government has recognised in its consultation to date. In the most recent Communications Report, the ACMA stated that as at June 204 there were 1,384 carriage services providers (CSPs) and

---

[25] http://www.theguardian.com/world/2014/aug/28/federal-police-mistakenly-publish-metadata-from-criminal-investigations

[26] http://www.theguardian.com/australia-news/2014/dec/08/afp-mistakenly-names-two-people-involved-in-criminal-investigation

[27] http://www.smh.com.au/nsw/bent-police-officers-preemptive-strike-20130505-2j130.html

[28] http://www.theaustralian.com.au/media/government-surveillance-makes-shield-laws-futile/story-e6frg996-1227188939153

208 telecommunications carriers supplying network infrastructure. How will local and smaller service providers be able to compete with international service providers that won't need to comply with the retention obligations? What will be the regulatory and cost burden on these smaller providers?

The Attorney-General's Department has said the cost of data retention is "small". On what basis? In the UK an impact assessment estimated that the cost of retaining information relating to IP address resolution alone at nearly $50 million (AUD).29 The draft dataset proposed by this Bill would result in far greater costs than this - the 2014 response to the industry discussion paper from iiNet noted that it would incur "significant cost, including audit costs".[30]

In 2010, Digital Rights Ireland reported:[31]

> Several network operators said the need to invest in retention infrastructure had caused them to delay or abandon improvements to national networks.
>
> Deutsche Telekom claimed it had spent €5.2 million on implementation of retention infrastructure and €3.7 million a year to facilitate about 13,000 call data requests and 6,500 internet data requests. Other operators said they had spent in excess of €4 million setting up systems for providing access to stored data.

Has the government prepared a Regulatory Impact Statement in line with its Guide to Regulation?[32] Is the scheme the least privacy intrusive option? There has been no public information released about the work done by PricewaterhouseCoopers to estimate the costs of the government's data retention proposal.

Despite statements from the Attorney-General and the Minister for Communications that no additional data will need to be created, internet service providers (ISPs) do not at present collect and retain several of the data items included in the draft data set.[33]

---

[29] https://www.gov.uk/government/publications/impact-assessment-ip-resolution

[30] http://www.iinet.net.au/about/mediacentre/papers-and-presentations/industry-consultation-paper-data-retention.pdf

[31] http://www.digitalrights.ie/leaked-assessment-of-data-retention-directive-shows-flaws/

[32] http://www.cuttingredtape.gov.au/handbook/ten-principles-australian-government-policy-makers

[33] http://www.iinet.net.au/about/mediacentre/papers-and-presentations/20142807-tia-act-1979.pdf

This Bill is not about preserving the status quo. It expressly requires service providers to create information where it is subject to retention obligations in s187A(1), where they do not already create the information as a normal part of doing business. This obligation highlights the hollowness of the claims that the data set is limited or this is what telcos are doing already.

Regardless of whether the points in the dataset are currently collected, the submission to the Attorney-General's Department in October last year by iiNet further makes the point that collection of this data makes no commercial sense for ISPs as it is not aligned with their core business, so collecting it represents an unnecessary expense and risk. Retaining all the internet data from all users will further increase costs by requiring the ISPs to commission new datacentres to store this telecommunications data.

Not necessary or proportionate

The government has not established that mandatory data retention is necessary or proportionate.

In October last year, United Nations human rights expert, Ben Emmerson concluded that mandatory data retention:[17]

> "amounts to a systematic interference with the right to respect for the privacy of communications", and therefore "it is incompatible with existing concepts of privacy for states to collect all communications or metadata all the time indiscriminately"

The Office of the Victorian Privacy Commissioner has previously submitted to the JCIS that mandatory data retention:[34]

> "…is characteristic of a police state. It is premised on the assumption that all citizens should be monitored. Not only does this completely remove the presumption of innocence which all persons are afforded, it goes against one of the essential dimensions of human rights and privacy law: freedom from surveillance and arbitrary intrusions into a person's life."

In 2012 the data preservation notice scheme was introduced into the Act. There has been no argument put forth for why this is not sufficient to meet the needs of LEAs in carrying out their duties.

---

[34] Submission 109 to Inquiry into Potential Reforms of Australia's National Security Legislation, available at: http://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=pjcis/nsl2012/subs.htm

Mandatory data retention is mass surveillance. This Bill fails to address the serious privacy and civil liberties concerns that have been raised in relation to mandatory data retention both in Australia and overseas.

Legislative Issues

As well as the Bill representing what we believe to be bad policy, it also poses a significant number of important legal questions.

Existing problems with the TIA Act

The data retention scheme compounds the existing significant problems with the current Telecommunications (Interception and Access) Act 1979 (TIA Act)[35] in relation to access and disclosure of telecommunications data.

A mandatory data retention Bill is a significant change that needs to be fully considered rather than being simply slotted into the existing framework of the TIA Act. The JCIS needs to meaningfully engage with the critical questions of:

- what data is to be retained
- what agencies can access telecommunications data
- what offences or contraventions should agencies be able to access telecommunications data
- whether a warrant should be required to access telecommunications data
- whether the data thus retained is available to anyone else under any other circumstances (e.g., to what extent will it be available for discovery or subpoenas in civil proceedings?)

Currently, the Bill is both a far-reaching and ill-defined shell for a scheme with substantive and critical obligations and provisions inappropriately left to regulations or declarations by the Minister.

Data set should be exhaustively defined in legislation

The government has published a draft data set that would be set out in these regulations but this has not yet been finalised. It is extraordinary that the JCIS is again being asked to consider this issue without the data set being defined. Moreover, the government has refused to say if the data set will be finalised by the time this Committee is required to table its report.[36]

---

[35] http://www.austlii.edu.au/au/legis/cth/consol_act/taaa1979410/

[36] http://www.smartcompany.com.au/legal/politics/45109-data-retention-hearings-off-to-nonsensical-start.html

That such a critical component of the data retention scheme to be prescribed by regulations is an inappropriate delegation of power to the Executive, as recognised by the Senate Standing Committee for the Scrutiny of Bills.

We also remind the committee that the Attorney-General's Department has been working on this proposal since at least 2007, and that last time JCIS addressed data retention in 2012 it declined to make any substantive recommendations on it because it was so poorly defined (at the time, AGD withheld from JCIS the fact that they had defined it well enough to consult with ISPs[37] on it two years earlier).

The fact that it is still poorly defined three years later, despite ostensibly enjoying status as a major priority of our law enforcement community, is out-and-out astonishing.

Flaws with the draft data set

The unclear and open-ended language used in the proposed data set means that the obligations which service providers are required to comply with are far too vaguely defined and leave open the room for scope creep. For example: the use of the phrase "any information..." and the undefined term "identifier".

We are very concerned about the scope of the data set. Why is it necessary for law enforcement purposes for service providers to retain the features and service descriptions of their account holders products and services, how is it intended that this data will be used (category 5(c))? On a practical level, this data would include information like a customer changing their monthly broadband quota, whether they have call forwarding activated, whether their call plan allows free international calls to certain countries or how many text messages are included.

There are many aspects of the subscriber information set out in the draft data set (category 1) that seems to have marginal relevance to law enforcement, such as billing information, status of the service and metrics of the service.

If the data set is broader than what is strictly necessary this also has consequences about the regime of the TIA Act. It means that:

- this extra data will be available for purposes beyond serious crime including to prospective or current litigants by way of subpoena or discovery[38]
- there is more data that needs to be kept secure

---

[37] http://www.zdnet.com/article/leaked-paper-reveals-australias-obsessive-metadata-secrecy/

[38] http://www.digitalrights.ie/leaked-assessment-of-data-retention-directive-shows-flaws/

- there is more data that could be misused such as we've seen in the UK with police seeking access to journalist's data[39]
- there is greater expense and complexity in storing and retrieving the data
- more difficult to preserve the confidentiality of communications such as between lawyers and clients, doctors and patients, journalists and sources.

Who can access the data

The Bill creates a new definition of 'criminal law enforcement agencies', which is defined with a list of agencies. However, the Bill allows the Attorney General to declare by legislative instrument that an agency is a criminal law enforcement agency for the purposes of the TIA Act. This is yet another example of an inappropriate delegation of power in this Bill.

The Bill also leaves open for further scope creep what entities will be listed as an "enforcement agency". This aspect of the Bill has been downplayed in discussions of the scheme, with the government asserting that the Bill significantly limits the agencies that can access telecommunications data. The reality is that the Bill gives the Attorney General the power to list by legislative instrument any authority or body with functions to enforce criminal law or administer a law imposing a pecuniary penalty or relating to the protection of the public revenue. These are incredibly broad functions that extends well beyond the oft-cited purposes of national security and serious crime. There is nothing in the Bill preventing the Minister from allowing agencies such as local councils, a Taxi Directorate, Centrelink, or even the RSPCA from being listed as an "enforcement agency".

It is highly likely that entities such as ASIC,[40] ATO, Centrelink, and certain government departments who are accustomed to having access to telecommunications data upon request will seek to be listed as an "enforcement agency" under the new regime.

Retention period

The Bill establishes a blanket two year retention period for all components of the data set, which is intended to be ultimately set out in regulations. The government has not demonstrated why a blanket two year period is necessary or proportionate or why this particular retention period of two years should apply uniformly across all the categories of data set out in the proposal.

---

[39] http://www.theguardian.com/media/2014/nov/04/police-ripa-powers-spy-journalists-sourc

[40] http://www.itnews.com.au/News/398334,asic-to-lobby-govt-for-metadata-access.aspx

In the UK, a 2011 report revealed that, over a 4 year period, 74%+ of disclosures to law enforcement agencies, where the age of data being sought was known, related to data that was less than 3 months old.[41]

In Australia, Communications Alliance noted that "CSPs report that the vast majority of warrantless requests they receive from Australian agencies relate to data that is 6 months old or younger". In this context, it would seem that a blanket two-year retention period is not necessary or proportionate.

If the Parliament proceeds with a data retention scheme, more appropriate retention periods would be in the order of three months, given that this would cover a majority of the current requests for access to this data.

[41] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:en:PDF

Conclusions

FutureWise's position is that the government's proposals for mass data retention as articulated in the Bill are neither necessary and proportionate[42] and that this Committee should recommend it not be passed by the Parliament.

The existing Telecommunications Interception and Access Act 1979[29] already allows for the targeted retention of telecommunications data where a need exists. The data preservation notice scheme was only introduced into the Act in 2012. Why there is a need for such a privacy-intrusive and non targeted approach has not been demonstrated. Legal opinion - including that of the Government-appointed Independent National Security Legislation Monitor - has recommended that access to this data require a warrant. FutureWise believes that this is one appropriate safeguard for access and that all telecommunications data access should require a warrant.

We reject absolutely the assertion that telecommunications data is less privacy intrusive than content as this is clearly incorrect as has been stated and demonstrated in this submission and elsewhere.

We believe that there is an urgent need for a comprehensive review of the legislation surrounding Telecommunications Interception and Access. We are in agreement with the Attorney-General only insofar as we believe that the the current laws are outdated and fail to accurately reflect the significant change in communication that has been brought about by the Internet. The changes in this Bill reflect an outdated attitude to the Internet and should not progress without substantial modification - in consultation with internet service providers and the general public.

Summary of Recommendations

i. **The Bill not be passed**

ii. **The period of consultation for the Bill be extended to allow more input from stakeholders but also the general public**

iii. **The Committee recommend a wide-ranging review into the status of legislation surrounding telecommunications intercept and access and that this proposal not be reconsidered until after this is complete.**

---

[42] https://en.necessaryandproportionate.org

If the Committee is not persuaded of this position, we urge the Committee to at a strict minimum, make the following recommendations:

- Remove the requirement to “create” data
- The data set must be defined in the primary legislation not regulation.
- Any discretion to make changes to the scheme via Declaration or Regulation should be removed. The obligations and scope of the scheme should be subject to parliamentary oversight, certain, and transparently set out in the primary legislation
- The retention period should not be a blanket 2-year period. This will represent a major cost and change in business practices for internet service providers, and has not been shown to be necessary. Any retention should be for a maximum period of three months
- The government engage in a comprehensive review of the existing scheme for disclosure of telecommunications data including:
    - a warrant be required to access communications data
    - a threshold of gravity of conduct be imposed so access to communications data can only be sought in relation to serious crimes or serious offences
    - address the need to protect confidentiality of communications and communications data relating to lawyers, journalists and medical professionals
- There be an express requirement in the primary legislation that the government contribute to the up-front and ongoing cost of complying with the TIA Act. The amendment to section 314 of the Telecommunications Act should also be removed from the Bill.
- Data set: each item in the data set must be necessary for law enforcement. For example, it is not necessary or proportionate to retain plan descriptions/features of the service as required in draft category 5
- Oversight: record keeping requirements of the law enforcement agencies that can access communications data needs to include the type of data requested, the age of the data requested, how that data was used, whether it altered the outcome of the investigation in a material way, a log of staff who accessed the data and confirmation that the data was deleted in a secure manner such that it can no longer be accessed once the investigation is complete

- Safeguards: a requirement to securely store the data and provide confirmation that deleted data is deleted in a secure manner, along with mandatory breach notifications and adequate penalties

- Sunset clause or mandatory review of the legislation.