Electronic Frontiers AUSTRALIA 20 YEARS

PO Box 1302, Kensington VIC 3031
W www.efa.org.au T +61 3 9013 9492
E email@efa.org.au F +61 3 9013 9468
@efa_oz

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
Parliament House, Canberra ACT 2600

19th January 2015

Via email to: pjcis@aph.gov.au

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

Dear Committee Secretary,

Electronic Frontiers Australia (EFA) appreciates the opportunity to provide this submission in relation to the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014. EFA's submission is contained in the following pages. EFA is happy to appear before the Committee and to provide further information, if required.

About EFA

Established in January 1994, EFA is a national, membership-based non-profit organisation representing Internet users concerned with digital freedoms and rights.

EFA is independent of government and commerce, and is funded by membership subscriptions and donations from individuals and organisations with an altruistic interest in promoting civil liberties in the digital context. EFA members and supporters come from all parts of Australia and from diverse backgrounds.

Our major objectives are to protect and promote the civil liberties of users of digital communications systems (such as the Internet) and of those affected by their use and to educate the community at large about the social, political and civil liberties issues involved in the use of digital communications systems.

Yours sincerely,

Jon Lawrence - Executive Officer
On behalf of EFA's Policy and Research Standing Committee

Submission on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014

1. Executive Summary

This submission is in relation to the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 ("the Bill"). This Bill, and the possibility of a system of mandatory data retention in Australia, serves to substantially change the legal, social and political climate in Australia. EFA believes there are a large number of fundamental issues with such a scheme being implemented.

This submission will cover the core aspects of such a system that require serious consideration and justification before being implemented into law. In summary these issues are that:

- Historically and internationally mandatory data retention regimes have been held to be an unacceptable intrusion into personal freedoms, with emphasis being placed on the requirement for data retention regimes to have a necessary and clearly defined scope.
- The concept of privacy exists within Australia because it has an intrinsic and real value to the individual; forfeiting this right, for whatever reason, must come with a substantial and convincing justification.
- The cost of retaining data is substantial.
- The telecommunications industry is not convinced that this would be the most efficient and inexpensive solution.
- There are serious technical challenges to the proposed system.
- Mandatory data retention has the real possibility of being misused and applied in other enforcement areas.
- Recently there has been a large volume of leaked materials that suggests that such a scheme could be used in conjunction with clandestine intelligence surveillance.

Each of these issues alone provides a justifiable cause for re-consideration of the proposed legislation. This submission commences with a series of recommendations intended to clarify the proposed legislation. The above points are then discussed and finally summarised with an examination of the drafting of the legislation and its 'rushed' and undefined scope. The submission describes in detail the lessons learned from foreign schemes, the intrinsic value of privacy, the technical difficulties anticipated in implementing the scheme, the potential for scope creep, the anticipated implementation costs and relationship between this legislation and surveillance by intelligence agencies.

2. Summary of Recommendations

2.1. General

Recommendation 1: EFA recommends that the Bill be withdrawn. The lack of consideration for civil liberties, the ease with which its effects can be expanded without parliamentary scrutiny and oversight, and the lack of evidence that it will achieve its stated goals combine to make the Bill unacceptable.

Recommendation 2: EFA recommends that legislation concerning data retention or other government surveillance is based on the principles of what is necessary, what is adequate and what is proportionate. The Bill completely ignores the possible negative outcomes for privacy, freedom of expression, and consequences if retained data is misused or leaked. EFA endorses the principles published at necessaryandproportionate.org[1]. EFA believes the proposed Bill falls well short of these principles.

2.2. Proposed Legislation

Recommendation 3: EFA recommends that the full definition of data to be retained must be included in the legislation, and not left for Ministerial regulation. Excluding the full definition from the legislation will enable to the expansion of the data set without proper parliamentary scrutiny.

Recommendation 4: EFA recommends that proposed section 187C paragraph (3) is removed from the Bill. The phrasing indicates service providers are welcome to retain data for longer periods of time than the two years required by the Bill, which is at odds with their responsibilities under the Australian Privacy Principles.

Recommendation 5: EFA recommends that section 187C(3) be removed, and replaced with a provision expressly prohibiting retention of telecommunications data for a period longer than two years.

Recommendation 6: EFA recommends that *implementation plans* are modified to ensure that they can only be used for a small amount of data retention. Implementation plans subvert consistency and parliamentary oversight by allowing a government agency to dictate a provider's obligations on a case-by-case basis. If the full s187A and s187C regulations are difficult or impossible to achieve the result may be that the entirety of data retention will be negotiated on an unpredictable "best-effort" basis.

Recommendation 7: EFA recommends that the Communications Access Co-ordinator should be required to consider proportionality, necessity and privacy impact when determining whether an *implementation plan* is acceptable.

Recommendation 8: EFA recommends that the complete list of agencies which can access data under the *Telecommunications (Interception and Access) Act 1979* are named explicitly in the Act. Which agencies have access to retained data is an important decision that should be under control of parliament. If this recommendation is not taken, the declaration test for an *enforcement agency* should at least include "gravity of conduct" as a factor, as previously recommended by the PJCIS.

---

[1] Necessary and Proportionate, *International Principles on the Application of Human Rights to Communications Surveillance* (May 2014), available at: https://en.necessaryandproportionate.org/text.

3. Specific Issues in Proposed Bill

3.1. Web Browsing Exemption - *TIA Act* s 187A

The proposed section 187A paragraph (4)(b) in the *TIA Act* is an attempt to "[put] beyond doubt that service providers are not required to keep information about subscribers' web browsing history," according to the note beneath it[2]. In doing so it casts doubt on how retention of several other types of data is supposed to function.

To pick one example from the draft data set, which is fully analysed later in this submission, the government wishes to retain "the destination of a communication":

> *This will include destinations for online services, such as the user name, number and/or IP address of the recipient of a Voice over IP (VoIP) call.*[3]

Paragraph (4)(b) clearly applies to the IP address of a recipient and would make this retention impossible:

> *(4) This section does not require a service provider to keep, or cause to be kept:*
> *...*
> *(b) information that:*
> *(i) states an address to which a communication was sent on the internet, from a telecommunications device, using an internet access service provided by the service provider; and*
> *(ii) was obtained by the service provider only as a result of providing the service;*[4]

The "destination IP address" of any communication is sensitive information. The circumstances under which it must be retained must be clearly and unambiguously defined in order for service provider obligations and customer privacy to be well understood.

EFA notes that the wording of this section, in its current form, runs contrary to the government's earlier intentions to avoid the retention of web browsing history[5]. Section 187A, as it is currently drafted, makes allowance for retention of same, and EFA strongly recommend that any reference to same be removed, or retention of web browsing history be expressly prohibited.

3.2. Retention Beyond Two Years - *TIA Act* s187C

TIA Act section 187C paragraph (3) makes clear that retention of data for periods of time longer than the stated two years is acceptable under that section. Service providers should in fact be obligated to delete the data in accordance with the Australian Privacy Principles (APP), specifically Principle 11:

> *11.2 If:*
> *...*

---

[2] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 at page 5.
[3] Draft Data Set at page 2.
[4] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 at page 4.
[5] "On Wednesday, Mr Abbott said authorities would be able to see what internet sites people were viewing.
'It is not what you're doing on the internet, it's the sites you're visiting,' he told Channel Nine"
See *Data retention laws: Tony Abbott says Government 'seeking metadata', not targeting people's browsing history* (7 August 2014) ABC http://www.abc.net.au/news/2014-08-06/security-laws-abbott-browsing-history-not-collected/5652364

(d) the entity is not required by or under an Australian law, or a court/tribunal order, to retain the information;

the entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.[6]

Paragraph (3) serves no useful purpose and will only confuse service providers' obligations. EFA recommends that it is removed.

Further, EFA recommends that retention of telecommunications data beyond the period of two years be expressly prohibited in the Act.

3.3. Implementation Plans - *TIA Act* Division 2

EFA has grave concerns about the *implementation plans* described in Division 2. They appear to be a middle-of-the-road agreement that can be reached between a service provider and the government about what will be retained about a particular service when it is impractical to meet all the requirements of s187A and s187C.

This type of flexibility may serve a useful purpose if it was used infrequently to deal with abnormally difficult situations, and always resulted in lesser retention than would be required under s187A and s187C.

As will be described later, in many circumstances it will be technically impossible for a service provider to retain most of the types of data that the government is proposing for its data set.

There is therefore a significant risk that implementation plans will be used for *everything*. That is, all retention that takes place will be negotiated on a case-by-case basis between a government co-ordinator and a given service provider. The criteria for determining whether an implementation plan is acceptable are extremely broad—they go so far as s187F(2)(f): "any other matter that the Co-ordinator considers relevant."

Although an extensive list of criteria is provided for consideration of an implementation plan, the potential privacy impact for users of that service is not among them. This is an incredible omission, particularly for retention plans which are negotiated outside the ordinary law defined by the legislation. Privacy concerns must be addressed insofar as the level of privacy intrusion or damage to individuals if the data were accidentally exposed are no worse than would apply for ordinary retention under s187A and s187C.

3.4. Ministerial Declarations of Enforcement Agencies - *TIA Act* s176A

Section 176A of the Bill contains provisions for expanding the range of government agencies which are able to access telecommunications data, without parliamentary oversight.

The Explanatory Memorandum suggests that this approach was recommended by the Parliamentary Joint Committee on Intelligence and Security (PJCIS) in their *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*:

[6] Australian Government - OAIC, *Australian Privacy Principles Fact Sheet 17* (January 2014) OIAC http://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-fact-sheets/privacy-fact-sheet-17-australian-privacy-principles_2.pdf at page 9.

> *7. The Bill will give effect to several of the PJCIS' recommendations including:*
>
> *…*
>
> *Confining agencies' use of, and access to, telecommunications data through refined access arrangements, including a ministerial declaration scheme based on demonstrated investigative or operational need (Recommendation 13).*[7]

Recommendation 13 was in fact unrelated. It stated:

> *The Committee recommends that the Telecommunications (Interception and Access) Act 1979 be amended to include provisions which clearly express the scope of the obligations which require telecommunications providers to provide assistance to law enforcement and national security agencies regarding telecommunications interception and access to telecommunications data.*[8]

More relevant is Recommendation 5:

> *The Committee recommends that the Attorney-General's Department review the threshold for access to telecommunications data. This review should focus on reducing the number of agencies able to access telecommunications data by using gravity of conduct which may be investigated utilising telecommunications data as the threshold on which access is allowed.*

Section 176A paragraph (4) outlines the items which must be considered by the Minister when making a declaration of an enforcement agency. None of these factors relates to "gravity of conduct".

The number of agencies which have access has been a significant aspect of data retention policy, borne out by the attention it received in the Bill and Explanatory Memorandum.

EFA recommends that the list of agencies be defined solely in legislation such that any changes to the list must be approved by parliament. If this is considered unfeasible, at the very least the declarations should be required to consider the gravity of conduct as was actually recommended by the PJCIS. The PJCIS' Recommendation 6 is also important in this context:

The Committee recommends that the Attorney-General's Department examine the standardisation of thresholds for accessing the content of communications. The standardisation should consider the:

- *privacy impact of the threshold;*
- *proportionality of the investigative need and the privacy intrusion;*
- *gravity of the conduct to be investigated by these investigative means;*
- *scope of the offences included and excluded by a particular threshold; and*
- *impact on law enforcement agencies' investigative capabilities, including those accessing stored communications when investigating pecuniary penalty offences.*[9]

EFA strongly agrees with this recommendation and recommends that it be applied when reviewing the proposed section 176A.

---

[7] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, Explanatory Memorandum at page 3.

[8] The Parliamentary Joint Committee on Intelligence and Security, Report of the Inquiry into Potential Reforms of Australia's National Security Legislation, (2013) at page xxvi.

[9] The Parliamentary Joint Committee on Intelligence and Security, Report of the Inquiry into Potential Reforms of Australia's National Security Legislation, (2013) at page xxiv.

4. History and Context

4.1. Europe

Various references in the course of the Australian debate on data retention have been made to the European experience with data retention and in particular the EU's 2006 Data Retention Directive and the UK's Data Retention and Investigatory Powers Act from 2014. EFA believes that these developments require closer attention than that which has already been paid in the context of the Australian discussion, given the problematic nature of these laws for fundamental rights, and, accordingly, the challenges which have been mounted to them. Thus EFA does not view them as appropriate examples for Australia to follow.

The EU's Data Retention Directive (DRD) seems to have arisen in response to the terrorist attacks in Madrid in 2004 and London in 2005. It aimed to harmonise EU efforts to combat crime and terrorism. It required telecommunication service providers to retain some types of traffic and location data for between six months and two years. This data excluded the content of the communications and was to be made available to law enforcement for the purpose of investigating, detecting and prosecuting serious crime and terrorism.

Since the DRD's enactment, there had been concerns that it was unduly intrusive of EU citizens' privacy and other fundamental rights. Indeed, there have been a series of judgements by the national courts of EU Member States (notably the German Constitutional Court), which found the implementation of the DRD into their national law to be unconstitutional and a breach of rights including privacy mainly due to a lack of adequate safeguards for the access and use of the data retained.

Yet, an 2011 evaluation report on the Directive concluded that the EU should continue to support and regulate the storage of, access to and use of telecommunications data but that rules needed to be improved to remove business obstacles for operators and to ensure that high levels of respect for privacy and the protection of personal data are applied consistently.

This is the backdrop to the Court of Justice of the European Union's (CJEU) decision from 8 April 2014 in which it declared the DRD invalid.[10] The Court looked at whether the measure was appropriate to achieve its objectives and did not go beyond what was necessary to achieve them. It found that although the Directive was suitable to achieve its purpose, it lacked clear substantive and procedural rules. By applying to all traffic data of all users of all means of electronic communications the Directive involved 'an interference with the fundamental rights of practically the entire European population'[11] and did not require a relationship between the data retained and serious crime or public security.[12]

---

[10] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* (CJEU, 8 April 2014)

[11] *ibid* at 56.

[12] This distaste for the blanket nature of data retention also follows a previous CJEU decision in Case C-70/10 *Scarlet Extended v Societe belge des auteurs, compositeurs et editeurs (SABAM)* [2012] ECDR 4 on the legality of Internet Service Providers having an obligation to engage in the mass monitoring of their users' communications in order to detect potential copyright infringements. The CJEU expressed concerns with the fact that all communications were being monitored, which led, in part, to the CJEU finding such monitoring obligations to be a breach of users' fundamental rights including the right to the protection of personal data and the freedom to send and receive information.

While the Court considered that data retention could be an appropriate tool to fight serious crime, it found that the DRD did not meet the principle of proportionality and should have provided more safeguards to protect the fundamental rights to respect for private life and to the protection of personal data.

4.2. British Response

The UK originally implemented the DRD in the *Data Retention (EC Directive) Regulations 2009*. In response to the CJEU's decision, it then fast-tracked its *Data Retention and Investigatory Powers* (DRIP) Bill 2014 into law to replace the Regulations. While British Prime Minister David Cameron asserted that the DRIP Act did not introduce any new powers or capabilities,[13] in practice the Act seems to have extended the UK government's surveillance capacities as well as not addressing the CJEU's criticisms of the DRD, especially those around the disproportionate interferences with privacy.[14]

The UK's conduct in reaffirming data retention through this recent legislation seems to have been taken in Australia as a sign that mandatory data retention laws are a trend in similar Western jurisdictions. However, at the time of writing, an application for judicial review of the DRIP Act before the UK High Court is pending, on the basis that the DRIP Act does not sufficiently protect individuals' right to privacy. The DRIP Act has also been the subject of complaints to the European Commission that through its implementation, the UK is breaching EU law. Furthermore, the European Parliament's Legal Service recently issued an Opinion on the aftermath of the CJEU's decision to invalidate the Data Retention Directive, suggesting that national data retention legislation in EU Member States such as the UK is even more susceptible than before to being annulled based on a lack of compatibility with the CJEU's decision and fundamental rights including privacy.[15]

On this basis, the UK's example through the DRIP Act can hardly be viewed as a robust trend in favour of mandatory data retention laws given the possibility of it being declared in breach of EU law and fundamental rights - and not an example that Australia should follow given the profound invasion of law-abiding citizens' privacy these laws entail.

4.3. United Nations

Article 12 of the Universal Declaration of Human Rights (1948) and Article 17 of the International Covenant on Civil and Political Rights (1966) state that no one shall be subjected to arbitrary interference with one's privacy, family, home or correspondence, and that everyone has the right to the protection of the law against such interference or attacks.[16]

---

[13] United Kingdom Government, 'PM and Deputy PM to announce emergency security legislation' (Press Release, 10 July 2014) https://www.gov.uk/government/news/pm-and-deputy-pm-to-announce-emergency-security-legislation.

[14] Open Letter from UK internet law academic experts to all Members of Parliament (15 July 2014) https://paulbernal.wordpress.com/2014/07/15/open-letter-from-uk-legal-academic-experts-re-drip/

[15] European Parliament Legal Service, Opinion on 'Questions relating to the judgment of the Court of Justice of 8 April 2014 in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* and *Seitlinger and others* - Directive 2006/24/EC on data retention - Consequences of the judgment' (January 2015) https://s3.amazonaws.com/access.3cdn.net/27bd1765fade54d896_l2m6i61fe.pdf

[16] Universal Declaration of Human Rights, GA Res 217A (III), UN GAOR, 3rd session, 183 plen mtg, UN Doc A/810 (10 December 1948), Article 12; International Covenant on Civil and Political Rights, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976), Article 17.

In 2013, the United National General Assembly adopted a consensus resolution on the Right to Privacy in the Digital Age strongly supporting the right to privacy, calling it a fundamental "tenet of a democratic society." The resolution "affirms that the same rights that people have offline must also be protected online, including the right to privacy." The resolution expresses concern at the negative impact of surveillance, "in particular when carried out on a mass scale, may have on the exercise and enjoyment of human rights." It refers to mass surveillance as a "dangerous habit" of some governments and notes that "mass surveillance technologies are now entering the global market, raising the risk that digital surveillance will escape governmental controls". The resolution recognised the impact of mass surveillance on both privacy and freedom of opinion and expression:

"Even the mere possibility of communications information being captured creates an interference with privacy, with a potential chilling effect on rights, including those to free expression and association. The very existence of a mass surveillance programme thus creates an interference with privacy. The onus would be on the State to demonstrate that such interference is neither arbitrary nor unlawful."

In this light, EFA is concerned that the Government's proposals may be incompatible with Australia's human rights obligations as an unwarranted interference with the privacy rights of Australian citizens and residents.

5. The Right to Privacy

5.1. Introduction

A predominate Australian court is yet to recognise a tort of privacy, but the Australian Law Reform Commission has set out the requirements for the enactment of a statutory cause of action for invasion of privacy in September 2014.[17] Although their recommendation appears to be gaining consideration in light of the recent shift in the public zeitgeist, their view is not new by any means, with a recommendation in 1983 by the Commission to define the values of privacy that are to be protected in a report.[18]

Society's value of privacy is as much a philosophical discussion as it is a legal debate. Privacy allows individuals to find and define themselves, whereas transparency creates uniform conduct—a trait useful in governance and business, but not in individuals. What can be lost in transparency? It is possible we lose our capacity to develop creativity and eccentricity, as well as development of self, understanding and our interpersonal relationships.[19]

The concept of privacy suffers from definitional problems. It is explicitly protected by a number of international documents (ICCPR and UDHR for example), but within a different context it has inconsistent variations (e.g., social compared to technological).[20]

5.2. Australian Context

The *Telecommunications Act 1997*, *Telecommunications (Interception and Access) Act 1979* and the *Privacy Act 1988* together make up the legislative authority for our privacy rights and the exceptions to these rights. The *Privacy Act* works in tandem with the *Australian Privacy Principles (APPs)* —13 enforceable sections to provide more clarity to businesses and individuals.

There is a significant privacy contradiction between the proposed data retention regime and the *APPs*. This can be highlighted where on one hand where the *APP* 3.2 states:

> *If an APP entity is an organisation, 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.*[21]

Yet the proposed data retention amendment will require businesses like ISPs to retain information unnecessary for their current operational requirements.

Furthermore most small businesses with an annual turnover of $3 million or less will not have to comply with the Privacy Act 1988. However, there are exceptions to this rule. Such small businesses will have to comply with the Privacy Act if:[22]

---

[17] Barbara McDonald, 'Tort's Role in Protecting Privacy: Current and Future Directions' (2013) No. 13/19 Sydney Law School Research Paper.

[18] Australian Law Reform Commission, *Privacy*, Report No. 22 (1983).

[19] Glenn Negley, 'Philosophical Views on the Value of Privacy' (1966) 31 Law and Contemporary Problems 319-325; See also: Philosophical Society, *On the Value of Privacy*, (Unknown date) Philosophical Society: http://www.philosophicalsociety.com/on_the_value_of_privacy.htm.

[20] Australian Communications Consumer Action Network, *Hacking the Grapevine* (15 July 2014) ACCAN https://www.accan.org.au/our-work/research/865-hacking-the-grapevine.

[21] Privacy Amendment (Enhancing Privacy Protection) Act 2012 (No. 197, 2012) s 3.2.

- a health service provider
- trading in personal information (e.g. buying or selling a mailing list)
- a contractor that provides services under a Commonwealth contract
- a reporting entity for the purposes of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act)
- an operator of a residential tenancy database
- a credit reporting body
- employee associations registered or recognised under the *Fair Work (Registered Organisations) Act 2009*
- businesses that conduct protection action ballots
- businesses that are related to a business that is covered by the Privacy Act
- businesses prescribed by the Privacy Regulation 2013. or
- businesses that have opted in to be covered by the Privacy Act.

In addition, it is also noted that Section 180F of the *Telecommunications (Interception and Access) Act 1979* (Cth) provides that the authorised officer accessing the data must consider whether interference with privacy is justifiable.

There is the potential for the retention of large amounts of data to contain or reveal a great deal of information about people's private lives, and that this data could be considered "personal information" under the *Privacy Act*.

5.3. Review of Memorandum on Privacy

Consistent throughout the *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* Explanatory Memorandum is a downplaying of metadata. This shows a lack of understanding regarding this type of information.

The Snowden leaks have demonstrated that agencies in many cases prefer to work with this type of data as opposed to content due to the inability for misinterpretation or the human ability to lie. A significant argument put forward in favour of this Bill is that metadata is not very revealing and therefore is not an invasion of privacy. This notion is false—it is precisely because it is so revealing that agencies want to access it.

Metadata cannot lie like a person on a conventional PSTN telephone call can. A connection between A and B, the length of that connection and the locations of the connection may be considered metadata, and its significance is being brushed aside as a mere tool to "enhance" enforcement. These connections reveal more than content in many cases. A Stanford University study has shown that the data could reveal private information such as medical conditions, financial connections and legal connections. [23]

[22] Office of the Australian Information Commissioner http://www.oaic.gov.au/privacy/privacy-topics/business-and-small-business/small-business

[23] W. Ockenden, 'Metadata mining: Stanford University researchers shocked by success of NSA-style phone data trawl' *ABC News* (online) 14 March 2014, http://www.abc.net.au/news/2014-03-13/metadata-reserachreveals-phone-piracy-risks/5319486

It is nearly impossible to approve of an amendment to the Bill where the proposed changes are mere ideas of data retention, without showing exactly what would be collected. EFA therefore believes it is essential that the full data set to be retained must be specified in the legislation itself.

A large number of privacy-related flaws appear in the Explanatory Memorandum as described below.

Outline

- Paragraph 10 claims that telecommunications data is less privacy intrusive than content. In fact, metadata has been shown to be more revealing than content.
- Paragraph 15 claims that telecommunications providers were consulted in the development of the Bill. Despite this, major providers including iiNet have publicly stated opposition to the proposed amendment due to privacy concerns, changes to information collection, and ambiguity.[24]

Statement of Compatibility with Human Rights

- Paragraph 5 claims that access to telecommunications data infringes less on privacy personal privacy compared with other covert investigative methods as it does not include the content or substance of the communication. The UN General Assembly has shown this information collection method to be a threat to personal privacy, going so far as to adopt a Right to Privacy in the Digital Age—alluding to the potential of scope creep.[25]
- Paragraph 9 states the Bill will limit agencies that can apply to access the data. It does not indicate what the limits to these agencies are and what the data could be used for beyond serious criminal investigations.
- Paragraph 29 indicates that the Bill is intended to align with ICCPR articles. It fails to take into account recent activity in the EU, where data retention in April 2014 was declared invalid, as discussed above. The court showed a lack of substantive and procedural rules, akin to the omission of actual regulations within the Australian bill.[26]
- Paragraph 31 describes how the UNHRC has interpreted "reasonableness" to imply that any interference with privacy must be proportionate to need. Despite this, it has not been revealed publicly why these measures are necessary, and why the current laws are no longer adequate.
- Paragraphs 32 and 33 describe how the right to privacy under Article 17 of the ICCPR can be permissibly limited provided it is in order to achieve a "legitimate objective". National security and public safety needs to be seriously weighed against the possible breach of Article 17 within Australia if this Bill is to be amended.
- Paragraph 35 states that the privacy limitation is "proportionate" because the measures are precisely directed to the legitimate aim being pursued. This is simply incorrect—just because an action supports an aim does not make it proportionate. Additionally, the measures have

[24] iiNet, 'iiNet's response to Industry Consultation Paper – Telecommunications data retention - statement of requirements September 2014' (Open Letter, 8 October 2014) Available at URL: http://www.iinet.net.au/about/mediacentre/papers-and-presentations/industry-consultation-paper-data-retention.pdf.

[25] UN News Centre, *General Assembly backs right to privacy in digital age* (19 December 2013) UN News Centre http://www.un.org/apps/news/story.asp?NewsID=46780#.VLmt5WM92vg.

[26] *Digital Rights Ireland Ltd*, Joined Cases C-293/12 and C-594/12.

been shown to be untargeted. This may have serious effect on the psyche of a population, creating a presumption of guilt instead of a presumption of innocence.[27]

- Paragraph 40 states that exceptions to retention may be granted to ease privacy intrusions. It appears that these exceptions are geared towards the technical complications associated with data retention. They are to help resolve contradictions within the proposed amendment, not to resolve easy privacy concerns.
- Paragraph 42 suggests that privacy and civil rights implications are minimised because:
    - The data is non-content
    - The scheme is supported by the Ombudsman; and
    - The scheme will be reviewed in three years;

  Yet:

    - metadata impinges on privacy as much, if not more than actual content;
    - the scheme contradicts current regulations including the APP because ISPs have to extend their retention beyond what they would otherwise need to keep; and
    - there is plenty of potential for scope creep within the first three years.
- Paragraph 45 states that server providers are required to 'do their best' to comply with APPs in their protection of personal information. Some providers do not retain information such as IP address as there is no need for billing reasons.[28] This Bill will change that.
- Paragraph 46 states that service providers currently have privacy practices in place, which can be used to protect the new required data sets. As some ISP's do not retain this information, there are no systems in place for the protection of this information.[29] This increases the risk that something will go wrong.

During the first public hearing the Joint Parliamentary Committee on Intelligence and Security probed a technical gaping hole: public network access points such as libraries, university networks, and café "hotspots" would be exempt. Data retained as a result of this amendment looks set to be solely for individual internet account holders, due to the technical complications. Therefore the question must be asked: what is the goal of security and intelligence community members when an overwhelming majority of general citizens are swept up in the dragnet data retention?

Furthermore, there should be better checks and balances on the use of metadata as it has been accessed very extensively. Law enforcement agencies can request for communications data without a warrant under the *Telecommunications (Interception and Access) Act 1979* (Cth).[30] In 2012–2013, there were a total of almost 313,000 requests which were made by law enforcement agencies.[31] Law

---

[27] Katerina Hadjimatheuo, "The Relative Moral Risks of Untargeted and Targeted Surveillance" (2014) 17(2) Ethical Theory and Moral Practice 187, 188.

[28] iiNet, 'iiNet's response to Industry Consultation Paper – Telecommunications data retention - statement of requirements September 2014' (Open Letter, 8 October 2014) Available at URL: http://www.iinet.net.au/about/mediacentre/papers-and-presentations/industry-consultation-paper-data-retention.pdf.

[29] Ibid.

[30] See sections 175 and 176 in Chapter 4 of the *Telecommunications (Interception and Access) Act 1979* (Cth). Chapter 4 also provides that the authorised officer accessing the metadata must consider whether interference with privacy is justifiable. The *Telecommunications Act 1997*, the *Telecommunications (Interception and Access) Act. 1979* and the *Privacy Act 1988* work in tandem to ensure the privacy rights of Australians and also provide for certain exceptions to these rights.

[31] Telecommunications (Interception and Access) Act 1979 Annual Report 2012–2013:

enforcement, Commonwealth and State and Territory agencies have accessed data in a total of 319,874 occasions in the financial year of 2012–2013.[32]

5.4. Summary

Privacy is more than a valued right within democratic societies; it is an encompassing philosophical concept. The mere idea of privacy in individuals can create changes in behaviour and conversely, the idea of untargeted surveillance can alter a nation's behaviours. Without privacy people cannot freely express their opinions or seek information. The basic concept of the presumption of innocence can be seen as undermined and reversed towards a presumption of guilt were these changes to go ahead and possibly lead to an erosion of privacy rights. This could have serious effects on the population's idea of privacy and ultimately freedom.

---

http://www.ag.gov.au/NationalSecurity/TelecommunicationsSurveillance/Pages/Annualreports.aspx (accessed on 15 January 2015); see also S. Davies, *Australia Pushes Data Retention Law, Despite Using Metadata at Twice the UK Level* http://www.privacysurgeon.org/blog/incision/australia-pushes-data-retentionlaw- despite-using-metadata-at-twice-the-uk-level/ (accessed on 1 July 2014).

[32] Telecommunications (Interception and Access) Act 1979 Annual Report 2012–2013: http://www.ag.gov.au/NationalSecurity/TelecommunicationsSurveillance/Pages/Annualreports.aspx (accessed on 15 January 2015); see also Taylor, J., Australian government agencies access more metadata, *ZDNet* (online) 12 December 2013 http://www.zdnet.com/au/australian-government-agencies-access-more-metadata-7000024255/. (accessed on 1 July 2014).

6. Technical Difficulties of Data Retention

6.1. Introduction

The draft data set reveals that it was written by people who do not have a solid understanding of computer networking. Some requirements are contradictory; some are impossible for ISPs to collect. Where it describes use of the Internet, most of the described data can be easily obfuscated such that ISPs are unable to identify or collect the information in the first place.

It is important to realise that these are not merely wrinkles that can be ironed out in the industry consultation phase. A substantial amount of what the Government wishes to achieve is practically impossible. Later in this section is described what is required for the Government to retain the level of detail described – the result would be a totalitarian dystopia.

By far the most likely result of applying these regulations is that ISPs, at considerable expense, will haphazardly collect mostly useless information about Australians who are doing nothing related to crime. Terrorists will continue to use encryption and other operational security techniques that result in minimal useful information being retained. Ever eager to demonstrate that they actually need these new powers, law enforcement agencies will take every opportunity to access the stored data and sift through it. Having failed to find any convincing terrorist plots they will turn to low-level crime or speculative profiling, espousing this stream of data as a way to categorise the risk of individuals. This may result in programs like the secretive and unjust *No Fly List* in the United States[33].

With so much uncertainty surrounding the privacy impact and application of these specifications it is absolutely inappropriate that they are relegated to regulation. If all of the difficult parts were struck out very little data would be retained; if every possible thing were done to collect it all we would find ourselves in the world of *Orwell's Nineteen Eighty-Four*. The scope must be put forward in legislation for proper parliamentary scrutiny.

This section explores some of the technical practicalities that EFA believes will make it difficult for ISPs to retain the described data.

6.2. Incidental Circumvention of Data Retention

A Hotel Scenario

Consider a travelling businessperson who does the following:

1. Checks in to a hotel and logs on to the hotel's provided WiFi;
2. Sends an email using Gmail;
3. Sends a text message using an iPhone;
4. Connects to the server back at the office to download some documents;
5. Makes a call to a colleague using Skype.

A reading of the draft data set suggests that the following data should be retained about this session: (some similar items have been omitted)

[33] American Civil Liberties Union, *Grounded: Life on the No Fly List* (2014) ACLU https://www.aclu.org/national-security/grounded-life-no-fly-list.

- Location of the WiFi access point;
- Location of the iPhone;
- IP address used to access the Internet;
- Physical identifier of the iPhone and its phone number;
- Identity of the recipient of the text message;
- Time the text message was sent;
- Identity of the recipient of the email;
- Time that the email was sent;
- That a "file download" service was in use when connected to the office;
- Identity of the Skype call recipient including their IP address;
- Time and duration of Skype call;
- How much bandwidth was allocated to the Skype call;
- How much data was downloaded and uploaded during the session.

Without even trying, this person has in some way circumvented the retention of every single item in this list.

Using Hotel Wi-Fi

A typical arrangement would be that the hotel has a single ADSL connection which terminates at a router. The hotel's internal network includes multiple Wi-Fi access points, spread out to ensure coverage across all of the rooms.

When a computer connects to the network the router will automatically assign a random IP address to that computer. This will be a private address—it will only make sense and is only guaranteed to be unique within the hotel.

When the computer tries to access a website such as Google, it will send the request to the router. The router has been assigned a single Internet IP address. This is a non-private address assigned by the ISP. Since the computer's private address doesn't make any sense on the Internet at large, the router substitutes its own address and requests the webpage on behalf of the computer. This is called *network address translation* (NAT)[34].

This happens for every computer that is connected. If there are fifty people using the Wi-Fi simultaneously their traffic will be mixed together. From the perspective of the ISP all communications originate from the single IP address.

It will clearly be impossible for the ISP to associate any retained data with a particular person at the hotel.

The same thing happens on a smaller scale with most home Internet connections. A typical Internet-connected home has an ADSL router with Wi-Fi. Again, there is only one IP address and NAT is used. This means it is impossible to tell which person in the household is communicating or what type of device they are using. If a neighbour has managed to guess the Wi-Fi password then their communications may also be mixed in.

[34] For a more thorough explanation of NAT see: Jeff Tyson, *How Network Address Translation Works* (2015) How Stuff Works http://computer.howstuffworks.com/nat.htm/printable.

Many people fail to secure their Wi-Fi networks with up-to-date encryption and good passwords[35]. Tools are freely downloadable that automatically attempt to guess Wi-Fi passwords or actively attack computers wirelessly in order to weaken the encryption[36].

Due to NAT and the insecurity of Wi-Fi it is extremely difficult to identity somebody reliably based only on their IP address[37]. Furthermore, no information is revealed to the ISP about the structure of the internal network. They are unable to retain information about whether a computer is using a wired connection or Wi-Fi or where it is physically located within the hotel.

It is alarming that the Government believes that this information is critical for counter-terrorism efforts. Policing decisions rely on accurately determining the identity of all people involved. It is hard to see how that will be achieved with ISP data retention.

Emailing using Gmail

In the earlier days of the Internet it was typical that individuals used email addresses that were provided by their ISP. These addresses are recognisable because they end with the name of the provider such as fred@bigpond.com or sally@internode.on.net.

When a customer communicates using this email address all emails are sent and received via that ISP's servers. Doing so would enable an ISP to comply with many of the draft data set requirements relating to email, including the sender and recipient and the sender's IP address at the time that the message was sent.

Nowadays it is much more common for individuals to use personal email addresses provided by a third party. Cost-free options include Gmail and Outlook.com. These third parties are often not subject to Australian jurisdiction. They may choose not to retain or provide data at the behest of the Australian Government.

Furthermore these services are typically accessed using a web browser. This means that the emails sent and received are not transmitted using normal email protocols. Their contents are transmitted using the protocol of the web, HTTP, and delivered through an encrypted tunnel between the overseas email provider and the individual's computer.

At best an ISP might be able to use traffic analysis to guess that a customer is accessing a particular email provider. Due to the encryption it is impossible for them to extract any information about individual emails, or even if any email is being sent.

This problem is not limited to personal Gmail addresses. Many Australian businesses and universities have their own mail servers, which may not be located in Australia. In this case the sent and received emails travel in and out of the country in an encrypted form and the customer's ISP is again unable to extract useful information.

---

[35] The statistics at wigle.net show that of approximately 170 million recorded networks more than 10% are unencrypted and about 15% use WEP, an easily broken form of encryption. See: Wigle Stats, *Statistics* (2015) Wigle Stats https://wigle.net/stats.

[36] Aircrack-ng is one of the most popular tools. It is intended for conducting security audits but like all tools it can also be used for malicious purposes.See: http://www.aircrack-ng.org/.

[37] This issue has been explored previously in United States copyright infringement cases. See: *K-Beech, Inc. v. John Does 1-37*, Case No. 2:2011cv03995 (E.D.N.Y, 2011) where it was noted that: "it is no more likely that the subscriber to an IP address carried out a particular computer function… than to say an individual who pays the telephone bill made a specific telephone call." Cf. *ELF-MAN, LLC v Eric Cariveau et al*, (W.D. Wash, C13-0507RSL, Document 78, 17 January 2014).

Text message using iPhone

Short Message Service (SMS) messages are one of the most straightforward items to surveil. They are sent over the cellular network rather than the Internet, placing their transmission and reception under full control of Australian telecommunications carriers.

A trend with modern smartphones has been to replace the use of traditional SMS messages with Internet-based equivalents due to carrier-imposed costs and various technological shortcomings. Apple's service is called iMessage and it is specifically engineered to provide end-to-end encryption, such that even Apple is unable to read the content of messages[38]. Similarly, Google encourages users of Google Plus to use Hangouts for sending messages via the Internet[39].

Other popular phone messaging services such as Snapchat and WhatsApp are also Internet-based and encrypted, placing them out of the reach of ISP data retention. New services and apps are being released constantly and all of them will circumvent this retention.

In short, SMS is a dying technology. The attributes that make it so easy to monitor are leading to its own natural demise.

Office VPNs

In this example it is assumed that the businessperson is using a *virtual private network* (VPN) to access the server at the office. This creates an encrypted tunnel through which other communications, like file downloads, can pass without eavesdropping being possible. This technique is used widely by organisations that need to make IT resources available to remote workers.

In this situation the ISP will see a connection created to the business from the hotel. At best they will see how much data is being transferred in each direction but not what type of service is in use or any other information about it.

Some businesses configure their laptops to route all Internet traffic including web browsing and email via the VPN. In this case the ISP would retain very little of value from the hotel's Internet connection.

Skype calls

Similarly to ISP-provided email addresses, retention of data about VoIP calls is only feasible if the customer chooses to use an ISP-provided product such as iiNet's *Netphone*[40]. The ISP runs the infrastructure that routes the calls so it is able to retain data about whom the customer calls, call duration and so on.

Retention fails when a third party VoIP solution is used such as Microsoft Skype or Apple Facetime. These transmit the call data over encrypted links. These links do not necessarily reveal to whom the customer is talking. Skype sometimes establishes direct connections between users; at other times it

[38] Apple, *iOS Security Guide*, (October 2014), https://www.apple.com/privacy/docs/iOS_Security_Guide_Oct_2014.pdf at page 30; Note: Some researchers disagree with Apple's claim that they cannot decrypt the data on the grounds that they could do so by modifying the infrastructure; Cf. Quarkslab's Blog, *iPrivacy Message* (17 October 2013) http://blog.quarkslab.com/imessage-privacy.html.

[39] See: 'Google+ Hangouts', https://www.google.com/+/learnmore/hangouts/.

[40] iiNet, *VOIP Plans - Netphone* (2014) iiNet http://www.iinet.net.au/phone/netphone-voip/.

routes calls via so-called "supernodes"[41]. With careful analysis an ISP might at best be able to guess that Skype or Facetime is in use.

If a customer uses one of these third party services the ISP will not be able to retain any of the information required by the proposed data set.

6.3. Active Circumvention of Data Retention

It has been shown above that data retention efforts can largely be avoided simply by choosing to use certain popular products instead of others. Data retention fares even worse if the user actively works to minimise their online footprint. The criminals and terrorists whom ASIO wants to catch may use these techniques. However the techniques themselves are not cause for suspicion; many people use these techniques overtly for legitimate business or personal reasons.

Virtual Private Networks (VPN)

VPNs are a widely used technology for securely connecting a computer to a remote network via the Internet. When a VPN is in use the ISP is unable to identify or retain information about any of the communications within the encrypted link.

This has already been discussed in the context of a remote worker accessing company resources. VPNs are also used by individuals to securely access their own networks, to prevent eavesdropping on their communication or to access the Internet via a different country.

This last use case is common for circumventing geoblocking. The ethics of this particular activity are up for debate (EFA would support the circumvention) but it is clear that hundreds of thousands of Australian home internet customers use VPN technology for this relatively harmless activity[42].

The Onion Router (Tor)

Tor is free software for obscuring your Internet access via a series of intermediate destinations. Each outgoing connection is bounced between a series of nodes spanning multiple countries before arriving at its final destination. A Tor user's ISP cannot see what they are doing; any activity performed on a website is also extremely difficult to trace back to the Tor user.

Tor has been in the spotlight for law enforcement agencies for some time, both because of its special abilities to hide digital trails and because some use it to conduct illegal activities such as drug trading and distributing child pornography[43].

However like any tool Tor is also used for many noble and legitimate reasons. The technology was originally developed by the US Navy to protect government communications[44]. Dissidents in oppressive regimes use it to communicate with less risk of being caught and arrested. Chinese use it to bypass their national firewall.

---

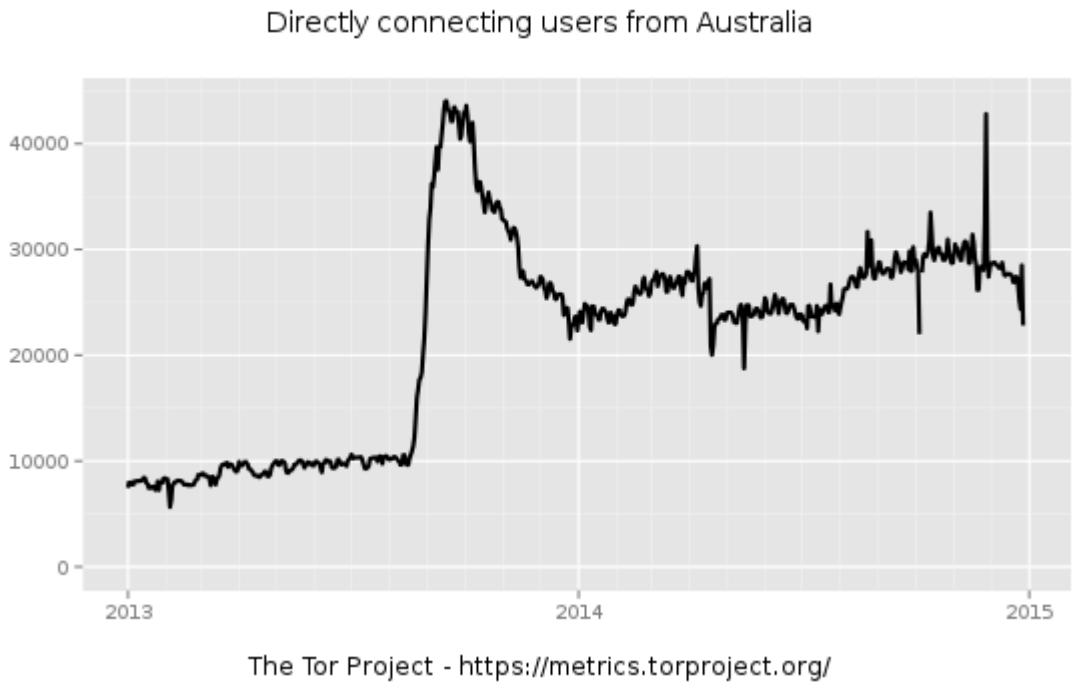
[41] Skype, *What are P2P Communications?* (2014) Skype https://support.skype.com/en/faq/fa10983/what-are-p2p-communications.

[42] A survey conducted by Choice suggests that 340,000 Australian households use Netflix even though circumvention measures such as VPNs are required to access it in Australia. See: Lifehacker, *What Will The 340,000 Australians Already Using Netflix Do Now?* (21 November 2014) Lifehacker http://www.lifehacker.com.au/2014/11/what-will-the-340000-australians-already-using-netflix-do-now/.

[43] The Guardian, *NSA and GCHQ target Tor network that protects anonymity of web users*, (5 October 2013) The Guardian http://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption

[44] Tor Project, *Tor Project: Overview* (2014) TOR https://www.torproject.org/about/overview.html.en#inception.

Most importantly, many individuals choose to use Tor as a matter of principle—they are simply taking steps to maintain their right to privacy. This is most clearly demonstrated by the records of Tor usage in Australia. An enormous increase occurred in mid 2013, corresponding to when Edward Snowden's leaks were published by Glenn Greenwald in *The Guardian*[45]. There are currently about 30,000 users of Tor every day in Australia[46].



Using Tor has a similar effect to using a VPN. ISPs are unable to retain any meaningful information about communications routed through Tor.

6.4. Destination IP Addresses and the Web-Browsing Exception

In an attempt to placate privacy advocates the Government explicitly ruled out web browsing history in the data set: "The Bill explicitly excludes anything that is web-browsing history or could amount to web-browsing history, such as a URL or IP address to which a person has browsed."[47]

Although it gratifying to see an attempt at limiting the scope of this surveillance, two major inconsistencies result.

The draft data set clearly states that the destination IP address of VoIP calls must be retained. This implies that an ISP must be capable of recording all destination IP addresses for each customer, at least momentarily. The ISP must also be able to reliably filter out which destinations are related to

[45] The Guardian, *NSA Prism program taps in to user data of Apple, Google and others* (8 June 2013) The Guardian http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

[46] Tor Project, *Tor Project* (2014) TOR https://metrics.torproject.org/userstats-relay-country.html?graph=userstats-relay-country&country=au.

[47] Draft Data Set at Page 2.

VoIP calls. This is demonstrably impossible. Skype can be configured to use an HTTPS proxy[48]. This makes the VoIP connection appear exactly the same as secure web browsing.

An ISP faced with this problem might choose to over-retain data to ensure compliance. They might record every destination IP address, despite web browsing being excluded from the requirements. The large amount of data generated would significantly increase the cost of data retention and also raise all of the privacy and security concerns about individuals' web browsing data being stored for two years.

The other inconsistency stems from the requirements under section 5, specifically "the type of communication; Examples: Voice, SMS, email, chat, forum, social media."

All HTTP/HTTPS web browsing traffic looks essentially the same regardless of whether it is a chat website, forum or social media being visited. The only way an ISP can perform this classification is to record destination IP addresses and try to associate them with particular "types" of websites. For example, if a customer visits 173.252.120.6 the ISP might see that that belongs to Facebook and classify that communication as "social media". Any such translation list will always be woefully incomplete. The results will be unreliable. Even then, this processing is only possible by surveilling the destination IP addresses, which are supposed to be excluded.

7. Long-term Location Data Available Without a Warrant

It is a concerning development that equipment locations are included in the draft data set. A mobile phone user is likely to have their location retained multiple times per day. Even though this is limited to approximate positions such as which cell tower is in use, this is sufficient to reveal all of a person's travels for the two year retention period to suburb granularity. The significance of this sensitive information is presumably why it is included in the draft data set at all.

A person's location history has significant privacy implications by itself, even separate from the communications with which each location was recorded. It is highly inappropriate that this information be made available without a warrant. If this proceeds there is a risk that law enforcement will engage in speculative behaviour, e.g., "everybody who connected to this cell tower yesterday is now a suspect", or conduct LOVEINT, the misuse of surveillance data pertaining to partners or prospective partners.

8. Dystopia: Getting All the Data

Above, it has been discussed in detail why the draft data set is irreconcilably impractical. It is worthwhile to ponder briefly what would be required to record all of the data proposed in the draft.

The fundamental problems are encryption and the use of foreign third party services outside the Australian jurisdiction. To ensure nothing slipped through the cracks Australia would have to do the following:

- All encryption (including VPNs) must be banned, unless it is intentionally weakened so that it is within the capability of the Government (and therefore criminals) to defeat it;

[48] Skype, *Can I connect to Skype Through a Proxy Server?* (2014) Skype https://support.skype.com/en/faq/FA1017/can-i-connect-to-skype-through-a-proxy-server.

- Australians can only use a Government-run or approved email service;
- Australians can only use a Government-run or approved VoIP service;
- Use of steganography to hide secret messages in plain sight must be criminalised;
- Deep packet inspection and data retention by all ISPs;
- Ban all digital communications that do not comply with Government surveillance standards (point-to-point radio links, for example).

Clearly this is an implausible scenario. Yet anything less than this would result in merely a "best-effort" surveillance. In doing so we acknowledge that smart criminals will not show up in this data. That means the data that *is* retained is simply data belonging to the innocent majority. It is not going to help catch terrorists. It will be used for something else.

9. Costs and Industry Response

EFA is concerned that this data retention scheme will place a heavy financial burden on service providers which will then be passed on to Australians. The Australian Mobile Telecommunications Association has estimated the cost of the scheme with a similar data set to Europe would be $500-700 million[49]. iiNet's estimated cost to the industry was $400 million[50].

This cost will be borne either by the taxpayer or by Internet customers in their bills—all for a dysfunctional surveillance scheme.

These estimates are likely to be unreliable because they require accurate specifications of what types and quantities of data must be retained. The draft data set is too flawed to be a good indicator of what will be required in reality. The Government should be defining the data set thoroughly enough in advance that the cost of the scheme is well understood before the legislation is passed.

It also appears that the Government is uncomfortable discussing the cost. They commissioned an analysis of the costs of data retention from PricewaterhouseCoopers, whose report has been kept confidential. Despite two Senate orders moved by Senator Scott Ludlam, the Attorney-General has refused to table even a redacted form of the report[51]. EFA believes the reasons for refusal are extremely flimsy. The Government has a duty to explain the costs accurately but it appears they would prefer to leave Australians in the dark.

10. Misuse and Scope Creep

As it has been previously discussed, Australia is not unique in attempting to legislate a system of mandatory data retention nor are the claims that such a system would be quickly used as a tool for copyright enforcement. Globally and historically the primary issue is that the seemingly simple question; 'will information retained under a scheme of mandatory data retention be used for copyright enforcement?', is not so simply answered. The question requires discussions of, *inter alia*,

[49] AMTA, *Better targeting is key to cost-effective data retention approach* (2014) AMTA: http://www.amta.org.au/articles/Better.targeting.is.key.to.cost-effective.data.retention.approach.

[50] iiNet, *Data retention proposals make cybercrime suspects of us all* (2014) http://blog.iinet.net.au/data-retention-proposals-cybercrime-suspects/

[51] Nigel Brew, *As long as a piece of string—costing data retention* (2014) FlagPost, Parliament of Australia http://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/FlagPost/2014/December/Costing_data_retention

issues around justifications for the undermining of the presumption of innocence, speculative invoicing and the balance of rights.

In relation to the undermining of the presumption of innocence, a system of mandatory data retention would affect all Australians. Such a proposed solution is effectively a drag net approach implemented in response to a complicated issue, and all Australians, not just those liable for criminal offences, will be subject to it. Ironically, the prompt response to censor[52] the Attorney-General's Telstra bill underscores his recognition of the invasiveness of the data retention scheme on an individual's freedom.

A point worth noting is that the proposed legislation has not received enough scrutiny from both the public and within the government. One of the critical elements that was fundamental to the invalidation of data retention legislation in Europe is the concept of proportionality. This is a fundamental concept commonly discussed in the European Union, but rarely raised in Australia, and should be instrumental in assisting an assessment as to whether the proposed system of mandatory data retention will be 'good law'.

To elaborate further, this concept of proportionality is specifically enshrined under Article 5 of The Treaty on the European Union[53] and has also been discussed in the CJEU's decision to invalidate the Data Retention Directive (DRD) in April 2014, discussed above. When assessing whether *Part 7 of the Criminal Justice (Terrorist Offences) Act 2005,* which requires telephone communications service providers to retain traffic and location data relating to those providers for a period specified by law in order to prevent, detect, investigate and prosecute crime and safeguard the security of the State, has exceeded the limits imposed by the compliance with the principle of proportionality:[54]

> *"The Court [took] the view that, by requiring the retention of those data and by allowing the competent national authorities to access those data, the directive interferes in a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal data".*

The DRD was therefore declared to be invalidated as its incursion to fundamental rights is not sufficiently limited to what was strictly necessary. Although the above CJEU judgment does not expressly cover the possibility of mandatory data retention being used for copyright enforcement, the concept of proportionality can still guide us in our evaluation of the data retention scheme as 'good law' from the angle of copyright enforcement.

In Australia, while the Attorney-General's Department's FAQs[55] assures Australians that:

> *"The Telecommunications (Interception and Access) Act 1979 only allows access for limited purposes, such as criminal law enforcement matters. Breach of copyright is generally a civil law wrong. The proposed data retention regime does not change this in any way,"*

---

[52] Sydney Morning Herald, *George Brandis hides his metadata* (27 November 2014) SMH http://www.smh.com.au/digital-life/digital-life-news/george-brandis-hides-his-metadata-20141127-11v3da.html.

[53] Treaty on European Union, signed in 1992.

[54] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* (CJEU, 8 April 2014) at 56.

[55] Australian Government - Attorney-General's Department, *Frequently Asked Questions* (2015) AG Department http://www.ag.gov.au/NationalSecurity/DataRetention/Pages/Frequentlyaskedquestions.aspx.

it should be highlighted that copyright infringements on a commercial scale can constitute criminal offences under the *Copyright Act 1968.*[56] Moreover, there is a risk of flagrant abuse of the data retention scheme for civil wrongs given that the Federal Police Commissioner[57], Andrew Colvin's admission that:

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

Therefore, the data retained under the proposed system could be used for a wide range of purposes, including the investigation of non-criminal (or civil) copyright infringement. This claim is made despite the provision in the explanatory memorandum accompanying the proposed Bill that access to data is reserved for specific purposes[58] outlined in the *Telecommunications (Interception and Access) Act 1979.*[59] All of the above further highlights the seemingly rushed and poorly considered nature of the proposed system of mandatory data retention.

Just over a decade ago in the United States, there was a 2003 court case concerning the legitimacy of the request for subscriber information made by the Recording Industry of America ('RIAA') to internet service provider ('ISP') Verizon Online ('Verizon') to investigate copyright infringement. Although in the first instance, the court held that Verizon was required to release the information of two users, on appeal, the earlier decision was overturned by the Court of Appeals, which agreed that Verizon presented some compelling arguments. Verizon's arguments were that:

> *"(1) § 512(h) does not authorize the issuance of a subpoena to an ISP acting solely as a conduit for communications the content of which is determined by others; if the statute does authorize such a subpoena, then the statute is unconstitutional because*
>
> *(2) the district court lacked Article III jurisdiction to issue a subpoena with no underlying "case or controversy" pending before the court; and*
>
> *(3) § 512(h) violates the First Amendment because it lacks sufficient safeguards to protect an internet user's ability to speak and to associate anonymously."*[60]

The concern over an unjustified invasion into the fundamental freedoms of internet users (ie, including the ability to act anonymously) also surfaces in the recent application filed by Dallas Buyers Club LLC ('Club') against five Australian ISPs for the preliminary discovery of personal information attached to IP addresses recorded to have downloaded the company's film 'Dallas Buyers Club'. In this respect, it should be noted that the first full hearing between iiNet Limited ('iiNet'), one of the ISPs, and the Club, will take place in February 2015[61]. Facilitating the unfair practice of 'speculative

---

[56] *Copyright Act 1968* (Cth) Part V (Remedies and Offences), Division 5.

[57] Hon. George Brandis, 'Press conference announcing the introduction of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 with Mr Duncan Lewis, Director-General of Security, and Mr Andrew Colvin, Commissioner of the Australian Federal Police' (30 October 2014). Available at URL: http://www.attorneygeneral.gov.au/transcripts/Pages/2014/FourthQuarter2014/30October2014-PressConferenceAnnouncingIntroductionOfTelecommunicationsInterceptionAndAccessAmendmentDataRetentionBill.aspx.

[58] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, Explanatory Memorandum at *s.64.*

[59] Telecommunications (Interception and Access) Act 1979 (Cth).

[60] Recording Industry Association of America Inc. v. Verizon Internet Services Inc. 359 U.S. App. D.C. 85; 351 F.3d 1229.

[61] Sydney Morning Herald, *February date set for iiNet's court battle over Dallas Buyers Club* (10 November 2014) SMH http://www.smh.com.au/business/february-date-set-for-iinets-court-battle-over-dallas-buyers-club-20141110-11joa8.html.

invoicing', which has direct and serious ramifications for all Australian internet users, is a concern of ISPs such as iiNet[62].

Speculative invoicing can occur when the end users of IP addresses associated with downloads of infringing copies of any copyright protected work (such as a film) are demanded from ISPs by the relevant copyright holders, who use these details to identify the users, thereafter sending them intimidating letters of demand seeking exorbitant and disproportionate sums for the alleged infringements, to 'pay up or else'. Such letters often threaten court actions and higher monetary penalties if the demands are not met, and ordinary users may well cave in to such demands. Such letters are premised on the assumption that any initiated copyright infringement action will be successful and are henceforth speculative. This sentiment is effectively a reversal of the presumption of innocence and constitutes a situation wherein large rights holders are effectively able to enforce their copyright without court quantified damages. In light of this growing practice, there is a real possibility that everyday internet users who fear the threat of court proceedings will increasingly be bullied into entering into unreasonable and excessive settlements. The introduction of a mandatory data retention scheme as proposed could further contribute to this unwelcome practice.

11. Interplay with Foreign Surveillance

Any discussion of data retention within Australia is incomplete without considering the existing retention regimes that affect Australian communications. It is now well known and documented that the signals intelligence agencies of the Five Eyes nations[63] cooperate in large-scale data retention, which includes the participation of the Australian Signals Directorate (ASD). Leaked documents have shown that that these agencies conduct programs which overlap considerably with the types of data retention and access proposed by this Bill.

Terrorism is frequently cited as a reason for which data retention is required[64]. National security is the domain of our intelligence community and therefore their roles, responsibilities and activities must be considered jointly if both the security and privacy outcomes that Australians require are to be achieved.

EFA's concerns are two-fold. First, the role of the ASD in particular has not been subjected to significant parliamentary scrutiny or discussion with respect to what types and quantities of information they should be collecting and sharing, where it concerns ordinary innocent Australians. Whether this data retention bill is necessary and proportionate is a highly contested matter. It is the responsibility of the Australian parliament to submit the intelligence programs to the same

---

[62] Mike Masnick, *Australian ISP iiNet Takes A Stand Against Copyright Trolling By Producers Of Dallas Buyers Club* (24 October 2014) TechDirt https://www.techdirt.com/articles/20141023/06561028922/australian-isp-iinet-takes-stand-against-copyright-trolling-producers-dallas-buyers-club.shtml.

[63] The *Five Eyes* intelligence community comprises the United States, Canada, the United Kingdom, Australia and New Zealand.

[64] "Mandatory retention of metadata is an international best practise standard for counter-terrorism and the investigation of serious crimes, for instance; paedophile networks"
"As the then Director-General of ASIO said at the time, access to metadata is an absolutely crucial tool for counter-terrorism." See: Hon. George Brandis, 'Press conference announcing the introduction of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 with Mr Duncan Lewis, Director-General of Security, and Mr Andrew Colvin, Commissioner of the Australian Federal Police' (30 October 2014). Available at URL:
http://www.attorneygeneral.gov.au/transcripts/Pages/2014/FourthQuarter2014/30October2014-PressConferenceAnnouncingIntroductionOfTelecommunicationsInterceptionAndAccessAmendmentDataRetentionBill.aspx.

analysis—the level of secrecy is different but the impact on Australians' security and privacy is the same.

Second, the interaction between these programs must be clearly defined. It is important to ask, for example, whether data retained by an ISP will be delivered to the National Security Agency in the US upon request, or whether this domestic program is in some way separated. It would be farcical if the standards for sharing information with our foreign allies—at which point control is lost over that data—were lower than the standards applied to our own law enforcement agencies. The government has a responsibility to conduct this analysis and to explain to Australians how their rights are protected.

This section describes two such intelligence programs and their impact on the same concerns as the Data Retention Bill.

11.1. ASD's Offer

Among *The Guardian*'s reports on Edward Snowden's leaked NSA documents, which typically described the activities of the *Five Eyes* alliance as a whole, one such report mentioned the ASD by its former name, the Defence Signals Directorate (DSD). A leaked memo from 2005 states:

> *DSD can share bulk, unselected, un-minimised metadata as long as there is no intent to target an Australian national – unintentional collection is not viewed as a significant issue.*[65]

In response, Geoffrey Robertson QC wrote for *The Guardian*:

> *The Intelligence Services Act sets strict limits on any DSD (now ASD) activity "likely to have a direct effect on an Australian person or produce intelligence on an Australian person". In such cases, ministerial authorisation is required (section 8) and before giving it, the minister must be satisfied that the Australian is "a person of interest" – ie involved in terrorism or espionage or serious crime. This is a vital safeguard and any unauthorised or unnecessary surveillance of an Australian is in breach of the Act (section 12).*[66]

It is therefore possible that one of Australia's own agencies has been collecting and supplying complete contents of Australians' communications to foreign partners for the last ten years, against Australian law and with no safeguards for Australians' privacy like those which were required by Canada[67].

Even proponents of the data retention bill emphasise that judicial warrants remain a requirement for law enforcement to access the content of communication[68]. For our intelligence agency to collect

---

[65] The Guardian, *Revealed: Australian spy agency offered to share data about ordinary citizens* (2 December 2013) The Guardian http://www.theguardian.com/world/2013/dec/02/revealed-australian-spy-agency-offered-to-share-data-about-ordinary-citizens.

[66] Geoffrey Robertson, *The privacy of ordinary Australians is under serious threat* (2 December 2013) The Guardian http://www.theguardian.com/commentisfree/2013/dec/02/privacy-australians-surveillance-metadata.

[67] Ibid.

[68] *"If we wish to access content, then we currently—and nothing will change—need to get a warrant to do that."* See: Hon. George Brandis, 'Press conference announcing the introduction of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 with Mr Duncan Lewis, Director-General of Security, and Mr Andrew Colvin, Commissioner of the Australian Federal Police' (30 October 2014). Available at URL: http://www.attorneygeneral.gov.au/transcripts/Pages/2014/FourthQuarter2014/30October2014-PressConferenceAnnouncingIntroductionOfTelecommunicationsInterceptionAndAccessAmendmentDataRetentionBill.aspx.

data that includes Australian communications (by methods unknown) and provide it to an foreign nation without any privacy protections or oversight—in fact, blind trust that the data will only be used for a specific purpose—is wildly inconsistent with the types of protections being discussed for this Bill. Since both our intelligence agencies and this data retention bill are purported to be used for counter-terrorism, it is critical that data protection standards are consistent, clearly explained and well-enforced in both cases.

11.2. The Five Eyes and XKeyScore

Perhaps the most egregious Five Eyes program revealed by Edward Snowden's leaks is that known as *XKeyscore*. The leaked slides boast that web browsing history, usernames, email communications and Facebook chats can all be searched with ease.

> *"I, sitting at my desk," said Snowden, could "wiretap anyone, from you or your accountant, to a federal judge or even the president, if I had a personal email".*[69]

One slide specifically describes the importance of capturing HTTP traffic (web browsing), decorated with the logos of Facebook, Twitter, Wikipedia and other popular websites.

From this it is clear that Australian countenances, if not actively participates in, the mass collection of communication content including web browsing history. In light of this, excluding web browsing history from the data retention bill is at best inconsistent; at worst deceptive. If web browsing history is already available to Australian intelligence analysts, as appears to be the case, then it is simply unnecessary to include it in this data retention Bill. Its omission will not affect the privacy outcomes at all. This inconsistency in Australia's activities must be explained.

11.3. Conclusion

These examples demonstrate that it is impossible to separate our domestic data retention policies from those of our international partnerships and intelligence agencies. The techniques of collection are different but the privacy impact for Australians and the importance of proper warrant systems and oversight remain the same. EFA believes that the government has a responsibility to provide clear policy in these areas. In doing so, Australians will have a true understanding of how much privacy they have and what activities the government can undertake in what circumstances.

[69] Glenn Greenwald, *XKeyscore: NSA tool collects 'nearly everything a user does on the internet'* (31 July 2013) The Guardian http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.