Australian Privacy Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

http://www.privacy.org.au/About/Contacts.html

19 January 2015

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
CANBERRA ACT 2600

Dear Secretary,

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

The Australian Privacy Foundations thanks the Committee for the opportunity to make a submission to this inquiry. The Bill poses substantial privacy concerns which we urge the Committee to consider.

Please find attached the APF's Submission to this Inquiry.

Yours sincerely,

Dr David Lindsay
Vice-Chair, for the Board of the Australian Privacy Foundation
(03) 9905 5547
david.lindsay@monash.edu.au

APF's Standing as an Interested Party

The Australian Privacy Foundation (APF) is the country's leading privacy advocacy organisation. A brief backgrounder is attached.

The APF has been a regular contributor to inquiries and reviews concerning the telecommunications interception and national security regimes for more than 20 years. Our submissions can be found at: http://www.privacy.org.au/Papers/.

In particular, we draw attention to recent submissions to the Parliamentary Joint Committee on Intelligence & Security (PJCIS) relating to the *Counter-Terrorism Legislation Amendment Bill (No. 1) 2014* (November 2014), the *Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill 2014* (October 2014) and Potential Reforms of National Security Legislation (August 2012).

We also note that the Senate Legal and Constitutional Affairs References Committee has been conducting an Inquiry into a *Comprehensive Revision of the Telecommunications (Interception and Access) Act 1979.* The issue of data retention was extensively discussed in submissions to that year long Inquiry and in oral evidence to its hearings (APF made two submissions and gave oral evidence on 29 July 2014). We understand that the Senate Committee is due to report on that Inquiry on 12 February. We urge the PJCIS to take into account the evidence given to and findings of that thorough Inquiry which set the proposals for a data retention scheme in the wider context of the interception legislation.

Executive Summary

The Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (the Bill) would amend the *Telecommunications (Interception and Access) Act 1979* (the TIA Act) to require service providers to retain certain types of telecommunications data for a two year period and to introduce certain reforms to the regimes applying to access to stored communications and telecommunications data under the TIA Act. This submission makes the following main points and recommendations:

- The APF opposes mandatory blanket data retention schemes, such as that proposed in the Bill, as they impose a high level of interference that is not necessary nor proportionate to the objectives of law enforcement and national security. The conclusion that blanket data retention breaches human rights, and especially the right to privacy, has been reached by every court and human rights body that has examined the issue.

- Mandatory data retention is not necessary nor proportionate because it entails the indiscriminate collection and retention of all forms of data about all persons, where there is no necessary link to investigations of serious crimes or threats to national security. The aims of the Bill can be achieved by measures that are less intrusive and more highly targeted than blanket retention of telecommunications data.

- Claims that 'metadata' (or non-content telecommunications data) are less intrusive than communications content are misleading, as metadata reveals highly personal information about communications users. Especially when combined with contemporary data analytics, telecommunications data may reveal more about people than communications content. Therefore legal safeguards on the collection of, and access to, telecommunications data should be at least as strong as those that apply to communications content.

- While access to telecommunications data can clearly be helpful to investigations conducted by law enforcement and security agencies, the evidence indicates that claims that mass collection and retention of metadata is essential are often over-stated. Independent analyses suggest that serious crime and terrorism may be just as effectively investigated by more targeted investigation techniques, which do not rely on mass data retention and which, accordingly, are less privacy-intrusive.

- The ready availability of techniques for masking metadata to users with no more than average sophistication suggests that blanket data retention regimes may be counter-productive, as they create an incentive for users to conceal their communications.

- Blanket data retention regimes pose a range of risks, which do not seem to have been taken into account by proponents of the Bill. In particular, the Bill will result in the collection and retention of much more data about users than would otherwise be the case, with the attendant risks associated with such large data sets. These risks include: risks associated with unanticipated uses of the data by service providers; risks associated with disclosures to third parties; and risks associated with the difficulties of adequately ensuring the security of large data sets. The APF submits that the current legal controls on the use, disclosure and security of such data, including those established under the *Privacy Act 1988* (Cth) and Part 13 of the *Telecommunications Act 1997* (Cth), are inadequate.

- Further risks posed by the mass collection and retention of telecommunications data include risks arising from Australians feeling they may be subject to constant mass surveillance and the potential for scope creep, including the use of such data in litigation unrelated to crime prevention and national security.

- The APF submits that there are a number of problems with the way in which the proposed data set is dealt with in the Bill. In particular, the data set is not appropriately limited to that which is necessary and proportionate for law enforcement and national security and the statutory categories in the Bill are too broad and uncertain, leaving too much detail to the regulations.

- The APF recommends the introduction of a definition of 'telecommunications data' for the purposes of the access regime in Chapter 4 of the TIA Act. Such a definition is required to remove uncertainty about the data that can be accessed under that regime.

- The APF submits that there are serious problems with the way in which browsing history is dealt with in the Bill, including in proposed s 187A(4(b). In particular, as there is no prohibition on service providers collecting and retaining Internet browsing history, which may be accessed as telecommunications data under Chapter 4 of the TIA Act, claims that the exclusion of browsing history from the data set means that the Bill is not privacy-intrusive are disingenuous. Moreover, as some technologies currently deployed by service providers require the logging of destination IP addresses in order to determine the source of a communication, the collection and retention of some browsing history data may be required in order for service providers to comply with their data retention obligations. The APF therefore recommends that the 'browsing history' exclusion be revisited with a view to addressing these problems.

- The APF submits that the two year retention period is excessive in relation to the objectives of the Bill, and recommends that this be reduced to six months.

- The APF submits that too much discretion is given to the Attorney-General to declare bodies or authorities to be a 'criminal law-enforcement agency' for the purposes of the stored communications regime in Chapter 3 of the TIA Act. The APF recommends that

the ability to seek a stored communications warrant, or authorise access to historical telecommunications data, should be confined to authorities or bodies responsible for investigating serious criminal offences, serious allegations of public corruption, or serious threats to national security. The APF further recommends that, in exercising the determination-making power, the Attorney-General be specifically required to take into account the effect of a determination on the right to privacy.

- The APF submits that, given the highly privacy-intrusive nature of metadata, the definition of an 'enforcement agency' for the purposes of access to historical telecommunications data is too broad. The APF therefore recommends that access to telecommunications data for the purposes of Chapter 4 of the TIA Act should be confined to authorities or bodies responsible for investigating serious criminal offences, serious allegations of public corruption, or serious threats to national security.

- The APF submits that the thresholds for access to stored communications and telecommunications data under the TIA Act are too low. The APF recommends that the threshold for access to stored communications should be brought into line with the threshold for interceptions of real-time communications such that access must relate to investigations of offences punishable by imprisonment for at least 7 years. The APF further recommends that the same thresholds should apply to access to telecommunications data under Chapter 4 of the TIA Act.

- The APF submits that, given the highly privacy-intrusive nature of metadata, the procedural safeguards for access to telecommunications data under Chapter 4 of the TIA At are inadequate. The APF therefore recommends that procedural safeguards be introduced to regulate access to non-content telecommunications data, which involve a decision of an independent body required to balance the objectives of access against the intrusion on the right to privacy. The safeguards should involve a process analogous to applications for a warrant for access to real-time communications and stored communications.

- The APF welcomes the enhancement to the oversight and accountability mechanisms for access to stored communications and telecommunications data, including the enhanced role of the Commonwealth Ombudsman, contained in Schedule 3 of the Bill. Especially given the highly privacy-intrusive nature of both stored communications and metadata, the APF recommends that consideration be given to establishing a Commonwealth Public Interest Monitor (PIM), who would be empowered to appear and make submissions on applications for warrants and access.

- The APF submits that, in proposing a mandatory blanket data retention regime, the government has given insufficient consideration to the potential benefits of a targeted data preservation regime, in which relevant agencies may selectively require the preservation of telecommunications data, provided that satisfactory procedural safeguards are met. The APF therefore recommends that:
  (a) The mandatory blanket data retention regime embodied in the Bill be abandoned, on the basis that it is neither necessary nor proportionate, and its effectiveness is questionable, at least in the light of the very high level of interference with privacy entailed by such a regime; and
  (b) Consideration be given to the introduction of a more targeted and circumscribed data preservation regime, which may include a modified version of the preservation notice regime established under Chapter 3 of the TIA Act.

Mandatory Data Retention Breaches Human Rights

The Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (the Bill) would amend the *Telecommunications (Interception and Access) Act 1979* (the TIA Act) to require service providers to retain certain types of telecommunications data for a two year period. The APF considers that, contrary to claims made in the Explanatory Memorandum, the Bill is incompatible with fundamental human rights and freedoms, and especially the right to privacy. A considerable body of legal opinion has concluded that laws mandating blanket retention of 'metadata' (also referred to as 'telecommunications data') are in breach of international human rights law. As this submission explains, blanket data retention of the kind proposed in the Bill breaches the fundamental right to privacy, in that it is neither necessary nor proportionate to legitimate national security and law enforcement objectives. Moreover, there is significant community opposition to proposals for mandatory data retention, as indicated by the strong objections to past data retention proposals, including by the majority of submissions to the PJCIS's 2012/13 inquiry into potential reforms of national security legislation.[1] The aims of the Bill can be achieved by measures, explained later in this submission, that are less intrusive and more highly targeted than the blanket data retention proposed in the Bill. Furthermore, the disproportionate impact of the Bill on human rights is exacerbated by the extent to which it fails to clearly specify:

(i) the data to be retained, which is left to be defined by regulations;
(ii) who is subject to the regime, which can be extended by regulations; and
(iii) the agencies entitled to access the data, which can be declared by the Attorney-General.

The conclusion that mandatory blanket data retention breaches human rights, and especially the right to privacy, has been reached by every court and human rights body that has examined the issue. In particular, this conclusion is supported by a report by the UN High Commissioner for Human Rights, a significant judgment of the Court of Justice of the European Union (CJEU), and by judgments of national courts in EU member states. Moreover, although blanket data retention laws have been rejected in Canada, it appears highly likely that any such proposals would be found to be in breach of the Canadian Charter of Rights and Freedoms.

In December 2013, following reports of large-scale covert surveillance of Internet traffic (the 'Snowden revelations'),[2] the UN General Assembly adopted Resolution 68/167, which expressed deep concern at the negative impact that mass surveillance and interception of communications may have on fundamental human rights; and called on all States to respect and protect the right to privacy in digital communications. The Resolution also requested the UN High Commissioner for Human Rights to submit a report on the protection and promotion of the right to privacy in the context of mass surveillance and interception of digital communications to the Human Rights Council and to the General Assembly. The report, presented to the Human Rights Council in June 2014, specifically considered the extent to which laws mandating mass data retention may be necessary and proportionate to the legitimate aims pursued – such as national security and crime prevention - and therefore in compliance with international human rights law. In this respect, the report concluded that:

> Concerns about whether access to and use of data are tailored to specific legitimate aims … raise questions about the increasing reliance of Governments on private sector actors to retain data "just in case" it is needed for government purposes.

[1] Parliamentary Joint Committee on Intelligence and Security, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation* (May 2013) 147-150.

[2] Glenn Greenwald, 'NSA Collecting Phone Records of Millions of Verizon Customers Daily', *The Guardian,* 5 June 2013.

> Mandatory third-party data retention – a recurring feature of surveillance regimes in many States, where Governments require telephone companies and Internet service providers to store metadata about their customers' communications and location for subsequent law enforcement and intelligence agency access – appears neither necessary nor proportionate.[3]

In 2006, the European Union adopted a mandatory blanket data protection law in the form of the Data Retention Directive[4] which, in some respects, was regarded as a model for the Bill. As set out in the Attachment to this submission, which explains the European experience with data retention, national laws implementing the Directive were challenged in courts in EU member states, namely Bulgaria, Romania, Germany, Cyprus and the Czech Republic. In each case, the challenges were largely successful on the basis that the national laws were disproportionate.

In April 2014, following requests for a ruling from courts in Ireland and Austria, the CJEU held that the Data Retention Directive was invalid as it was in breach of EU human rights law, and especially the fundamental rights to privacy and data protection, enshrined in Articles 7 and 8 of the EU Charter of Fundamental Rights.[5] In reaching this conclusion, the CJEU made the following points:

- Requiring the mass retention of the relevant data, and allowing national authorities to access such data, constitutes a particularly serious interference with the right to privacy and the right to data protection. In the particular, the mass retention and use of data without the subscriber or user being aware 'is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance'.[6]
- Data relating to the use of electronic communications are an increasingly important and valuable tool in the prevention of offences and the fight against crime, especially organised crime, and terrorism.[7] Nevertheless, the retention measures prescribed by the Data Retention Directive were not necessary nor proportionate.
- By requiring the retention of data effectively relating to all means of electronic communication, the Directive interfered with the right to privacy to an extent that was not strictly necessary. Moreover, the measures in the Directive were not necessary in so far as they indiscriminately applied to all persons, and to all data, including where there was no evidence of any link with serious crime or any relationship to a threat to public security.[8]
- Apart from the over-broad requirements to retain data, the Directive was invalid as it failed to adequately specify any objective criterion to limit access to the data, or uses of the data, by competent national authorities. Furthermore, the Directive did not contain adequate substantive or procedural safeguards on access to the retained data. In

[3] UN High Commissioner for Human Rights, *The right to privacy in the digital age,* 30 June 2014, A/HRC/27/37, [26].

[4] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (the 'Data Retention Directive').

[5] Court of Justice of the European Union, Judgment in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others,* Judgment of 8 April 2014.

[6] Court of Justice of the European Union, Judgment in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others,* Judgment of 8 April 2014, para. 37.

[7] Court of Justice of the European Union, Judgment in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others,* Judgment of 8 April 2014, paras. 43, 49, 51.

[8] Court of Justice of the European Union, Judgment in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others,* Judgment of 8 April 2014, paras. 56-59.

particular, access to the data was not conditional on a prior review by an independent body, such as a court.[9]
- The period specified for the retention of the data, which was set at between 6 and 24 months, did not sufficiently distinguish between categories of data on the basis of their possible usefulness.[10]
- The Directive did not provide sufficient safeguards to ensure the security and protection of the data required to be retained, nor impose specific obligations on member states to impose such rules. Neither did the Directive impose an obligation to ensure the destruction of the relevant data at the end of the retention period. Moreover, the Directive failed to require that the relevant data be retained in the EU.[11]

As explained in the Attachment to this submission, to date there have been a variety of responses to the CJEU ruling by EU member states: while some states have repealed their data retention laws, others have placed their laws under review, while yet others have introduced new laws. In the UK, a blanket data retention law, the *Data Retention and Investigatory Powers Act 2014* (UK) (the 'DRIP Act') was controversially rushed through in July 2014. Given the strong indications in the CJEU ruling that mass, indiscriminate data retention is impermissible, it is highly arguable that the DRIP Act is invalid, and it is currently being challenged in the UK High Court. As pointed out in the Attachment, in addition to the challenge to the DRIP Act, data retention laws are currently subject to legal challenges in Belgium, Bulgaria, Ireland, the Netherlands, Poland and Slovakia.

In Canada, proposals for blanket data retention laws have faltered, largely as a result of widespread opposition from the public, privacy commissioners, academics, the legal profession and industry.[12] While it seems likely that legislation will be passed in 2015, the current proposal implements an approach based case-specific preservation orders, but without judicial oversight. Given Canadian case law in this area, it remains possible that even these more circumscribed data retention requirements may be subject to successful legal challenge as contrary to the Canadian Charter.

- *The APF opposes mandatory blanket data retention schemes, such as that proposed in the Bill, as they impose a high level of interference that is not necessary nor proportionate to the objectives of law enforcement and national security. The conclusion that blanket data retention breaches human rights, and especially the right to privacy, has been reached by every court and human rights body that has examined the issue.*

- *Mandatory data retention is not necessary nor proportionate because it entails the indiscriminate collection and retention of all forms of data about all persons, where there is no necessary link to investigations of serious crimes or threats to national security. The aims of the Bill can be achieved by measures that are less intrusive and more highly targeted than blanket retention of telecommunications data.*

[9] Court of Justice of the European Union, Judgment in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others,* Judgment of 8 April 2014, paras. 60-62.

[10] Court of Justice of the European Union, Judgment in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others,* Judgment of 8 April 2014, para. 63.

[11] Court of Justice of the European Union, Judgment in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others,* Judgment of 8 April 2014, paras. 66-68.

[12] Christopher Parsons, 'Stuck on the Agenda: Drawing lessons from the stagnation of 'lawful access' legislation in Canada' in Michael Geist and Wesley Wark (eds.), *Law, Privacy and Surveillance in Canada in a Post-Snowden Era* (University of Ottawa Press), Forthcoming 2015.

The False Distinction between Content and Metadata

In supporting proposals for mandatory data retention, and for access to such data, governments routinely offer re-assurance that access is 'only to metadata' and seek to contrast this with the 'content' of communications, which is commonly subject to more rigorous access regimes. Official justifications for the Bill repeat claims that telecommunications metadata is less privacy intrusive than content. For example, the Explanatory Memorandum to the Bill states that:

> Access to telecommunications data … infringes less on privacy compared to other covert investigative methods as it does not include the content or substance of the communication.[13]

This purported distinction completely overlooks how much 'metadata' can reveal about a person, especially when combined with contemporary data analytics. As the CJEU found in *Digital Rights Ireland,* metadata 'taken as a whole may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained.'[14] Similarly, in ruling that the blanket collection of Internet metadata by the NSA likely violates the Fourth Amendment of the US Constitution, District Judge Leon referred to the changing nature of metadata, especially in a communications culture dominated by mobile phones, to conclude that:

> Records that once would have revealed a few scattered tiles of information about a person now reveal an entire mosaic – a vibrant and constantly updating picture of the person's life.[15]

This conclusion is supported by the report of the UN High Commissioner for Human Rights which, in finding that the distinction between 'metadata' and content is 'not persuasive', pointed out that:

> The aggregation of information commonly referred to as "metadata" may give an insight into an individual's behaviour, social relationships, private preferences and identity that go beyond even that conveyed by accessing the content of a private communication.[16]

Moreover, respected security analysts agree that metadata often reveals more about a person than communications content. For example, Stewart Baker, the former general counsel of the NSA, is reported as stating that, 'Metadata absolutely tells you everything about somebody's life. If you have enough metadata, you don't really need content.'[17]

Therefore, in the current communications environment it is completely misleading to claim that telecommunications metadata are less intrusive than communications content. Given the ubiquitous nature of metadata, and especially metadata collected from the use of mobile phones, in many (if not most) cases metadata is more revealing than the content of a communication. From the point of view of the right to privacy, the distinction between metadata and content simply no longer makes sense. Furthermore, given the capabilities of

---

[13] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, Explanatory Memorandum, Statement of Compatibility with Human Rights, [5].

[14] Court of Justice of the European Union, Judgment in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others,* Judgment of 8 April 2014, paras. 26-27, and 37.

[15] *Klayman v Obama,* 957 F Supp 2d 1 (DDC 2013).

[16] UN High Commissioner for Human Rights, *The right to privacy in the digital age,* 30 June 2014, A/HRC/27/37, [19].

[17] Stilgherrian, 'Can Snowden Finally Kill the Harmless Metadata Myth?', ZDNet, 16 September 2014, http://www.zdnet.com/can-snowden-finally-kill-the-harmless-metadata-myth-7000033717/.

contemporary data analytics,[18] it is inaccurate to claim that metadata is invariably anonymous as, in many cases, the potential for re-identification means that it will amount to 'personal information', as that term is defined under the *Privacy Act 1988* (Cth).[19]

In short, it is clear that metadata has assumed a central role in surveillance practices, increasingly replacing the role of surveillance of communications content. This is confirmed by the high value placed on access to, and use of, metadata by security and law enforcement agencies. Moreover, in many (if not most) circumstances, metadata may reveal more than communications content. For example, communications content, such as audio fragments, email texts, or video frames, commonly require a human observer (or imperfect software applications) who is able to determine the relevance of the data. However, in relation to metadata, such as 'number called', 'time started', 'GPS coordinate' or 'IP address', the meaning is immediately apparent. Given this distinction, it is comparatively easy for data analytic software to retrieve, classify, process and analyse large sets of metadata in order to derive meaningful information. It is therefore less than accurate to make claims such as 'metadata is less privacy invasive than content' or 'we are only collecting metadata', when the collection and analysis of metadata is often more cost-effective and revealing than the comparatively expensive and more problematic communications content.

Unfortunately, legal safeguards on the access to, and use of, metadata have failed to keep pace with the sea change in the use and value of this data. Accordingly, it is no longer possible for the metadata-content distinction to be used as the basis for distinguishing between the privacy impacts of different forms of data. The implication of the highly privacy-intrusive nature of metadata is that, rather than focusing on expediting access to metadata, attention should be given to the adequacy of legal and technological safeguards on the large amounts of data currently collected.

We further note the attempts by the government and relevant agencies to re-assure the public that metadata is comparable only to the 'envelope' in a traditional postal communication. We submit that this is a completely false and misleading analogy. At the very least, metadata invariably includes details of both sender and recipient – in contrast, most posted letters contain only the intended recipient's address (and sometimes an individual's name) – no information about the sender is visible on the envelope unless the sender has specifically chosen to include a return address.

- *Claims that 'metadata' (or non-content telecommunications data) are less intrusive than communications content are misleading, as metadata reveals highly personal information about communications users. Especially when combined with contemporary data analytics, telecommunications data may reveal more about people than communications content. Therefore legal safeguards on the collection of, and access to, telecommunications data should be at least as strong as those that apply to communications content.*

[18] See the sources discussed in Michiko Kukutain 'Watched by the Web: Surveillance Is Reborn, review of 'Big Data,' by Viktor Mayer-Schönberger and Kenneth Cukier', *New York Times,* June 10, 2013, http://www.nytimes.com/2013/06/11/books/big-data-by-viktor-mayer-schonberger-and-kenneth-cukier.html.

[19] Note that discussion of this topic in the US is complicated for our purposes by a definition of 'personally identifiable information' (PII) which is narrower than Australia's "personal information," or the EU's broadly comparable definition of 'personal data'. This sometimes leads marketing and government sources in the US to misleadingly assert that various forms of communications and web-derived metadata are somehow 'not PII' and thus 'anonymous', whereas under Australian and EU law, and in practice, it is clear they can often easily be used to derive identity and, consequently, fall within the scope of the relevant data privacy laws.

Blanket Data Retention is Neither Essential Nor Effective

Supporters of blanket data retention claim that metadata is essential to the effective operation of security and law enforcement operations. For example, the Explanatory Memorandum to the Bill claims that:

> Access to historical data and analysis of inter-linkages with other data sources is vital to both reactive investigations into serious crime and the development of proactive intelligence on organised criminal activity and matters affecting national security.[20]

Independent analyses of the use of metadata, however, suggest that claims relating to the necessity and effectiveness of access to metadata are often over-stated.

In response to the Snowden revelations, the Privacy and Civil Liberties Oversight Board (PCOB), an independent agency established to advise the US executive on anti-terrorism laws, was asked to investigate the relevant NSA programs, including the program involving the mass collection of telecommunications metadata. In its report on this program, released in January 2014, the PCOB concluded that the program had shown 'minimal value' in preventing terrorism. In particular, the report stated that:

> Based on the information provided to the Board, including classified briefings and documentation, we have not identified a single instance involving a threat to the United States in which the program made a concrete difference in the outcome of a counterterrorism investigation. Moreover, we are aware of no instance in which the program directly contributed to the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack. And we believe that in only one instance over the past seven years has the program arguably contributed to the identification of an unknown terrorism suspect. Even in that case, the suspect was not involved in planning a terrorist attack and there is reason to believe that the FBI may have discovered him without the contribution of the NSA's program.[21]

Similarly, the evidence presented before the trial judge in *Klayman v Obama*[22] was insufficient to persuade the court of the efficacy of the NSA program. In particular, the court found that there was no single instance where the blanket collection of metadata either stopped an imminent terrorist threat or otherwise assisted in achieving a time-sensitive objective. On the basis of the evidence adduced by the government, Judge Leon concluded that there were 'serious doubts about the efficacy of the metadata collection program as a means of conducting time-sensitive investigations in cases involving imminent threats of terrorism.'

In the US, criticism of the NSA program led, in October 2013, to the introduction of a Bill, known as the *USA Freedom Act,* designed to end the mass collection of metadata. The Bill was introduced to the House by Representative Jim Sensenbrenner, a prominent Republican member of the House of Representatives, who was responsible for introducing the *USA PATRIOT Act.* In supporting the end of blanket data collection, the co-sponsors of the Bill, Representative Sensenbrenner and Democrat Senator Patrick Leahy, stated as follows:

> It is simply not accurate to say that the bulk collection of phone records has prevented dozens of terrorist plots. The most senior NSA officials have

[20] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, Explanatory Memorandum, Statement of Compatibility with Human Rights, [7].

[21] Privacy and Civil Liberties Oversight Board, *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court,* 23 January 2014, 11.

[22] 957 F Supp 2d 1 (DDC 2013).

> acknowledged as much in congressional testimony. We also know that the FISA court has admonished the government for making a series of substantial misrepresentations to the court regarding these programs. As a result, the intelligence community now faces a trust deficit with the American public that compromises its ability to do its job. It is not enough to just make minor tweaks around the edges. It is time for real, substantive reform.
>
> We are two veteran lawmakers who believe now is the time for that reform and for a meaningful discussion about protecting privacy and national security in the 21st century. We are not alone — we have heard from Americans across the country who rightfully question the need for these intrusive programs and we are joined by lawmakers in both chambers from across the political.[23]

In the European Union, a 2011 report by the Scientific Services of the German Parliament found that the then current data retention laws had no significant effects on crime rates in EU member states. In particular, the report noted that:

> In most states crime clearance rates have not changed significantly between 2005 and 2010. Only in Latvia did the crime clearance rate rise significantly in 2007. This is related to a new Criminal Procedure Law though and is not reported to be connected to the transposition of the EU Data Retention Directive.[24]

Referring to this report, European Digital Rights, in an evaluation report of the Data Retention Directive, concluded that 'taking all relevant factors into account, crime is investigated and prosecuted just as effectively with targeted investigation techniques that do not rely on blanket retention are used. Blanket and indiscriminate telecommunications data retention has no additional statistically significant impact on the investigation of crime.'[25] While a report prepared by the European Commission in March 2013[26] indicated that retention of traffic data was essential to investigating some crimes, it is also concluded that available statistical and quantititative analysis was unreliable, and therefore relied mainly on anecdotal evidence. In an independent report, first published in November 2013 and later republished in April 2014, Jones and Hayes referred to reports such as those of the European Commission, to conclude that:

> In respect to the "evidence" presented to justify the Directive, it is sufficient to note that the plural of anecdotes is not "data". And even to the extent that case studies can be seen to objectively demonstrate the Directive's effectiveness, it does not necessarily follow that they justify the Directive's scope, application, or absence of protection for due process and fundamental rights.[27]

The well-documented inflated claims about the efficacy of metadata by the US government, US security agencies, as well as others, should be instructive for Australian law-makers, especially as the Bill has been introduced at a time of heightened security alert, both in Australia and internationally. During periods of heightened national security concern, there is

---

[23] Senator Patrick Leahy and Rep. Jim Sensenbrenner, 'The Case for NSA Reform', 28 October 2013, http://www.politico.com/story/2013/10/leahy-sensenbrenner-nsa-reform-98953.html.

[24] Scientific Services of the German Parliament, Report WD 7 – 3000 – 036/11, http://www.vorratsdatenspeicherung.de/images/Sachstand_036-11.docx.

[25] European Digital Rights, *Shadow evaluation report on the Data Retention Directive (2006/24/EU),* 17 April 2011, 7

[26] European Commission, 'Evidence for necessity of data retention in the EU', March 2013, http://www.statewatch.org/news/2013/aug/eu-com-mand-ret-briefing.pdf.

[27] Chris Jones and Ben Hayes, Securing Europe through Counter-Terrorism: Impact, Legitimacy, Effectiveness (SECILE), *The EU Data Retention Directive: a case study in the legitimacy and effectiveness of EU counter-terrorism policy,* 8 April 2014, 33.

a potential danger of legislative over-reach, in the form of overly-broad surveillance laws. While access to telecommunications metadata may be useful for security and law enforcement agencies, it is important for any potential benefits to be properly balanced against potential privacy invasions, so that the laws are not disproportionate. This requires a prudent analysis of claims that blanket data preservation laws are essential, and the degree to which they may be effective as opposed to merely convenient; and claims to effectiveness should not simply be accepted at face value. As Jones and Hayes point out in their report, an important distinction must be drawn between debates about the effectiveness of data retention regimes and debates about their legitimacy. In any case, proposals for mandatory data retention should always be subject to a proper risk/benefit analysis.

Proper analysis of the potential benefits of data preservation laws must take into account the potential for users, with no more than average sophistication, to effectively circumvent such laws by using the many widely available techniques to mask metadata. For example, users may use techniques such as tunnelling, where an IP datagram is carried as a payload by another IP packet, thereby hiding the original IP address, or virtual private networks (VPNs), which use a variety of techniques to disguise an IP address.[28] Many of the techniques for masking data, including VPNs and the Tor network, were detailed in evidence to the PJCIS's inquiry into potential reforms of national security legislation.[29] As long ago as the middle of 2014, it was reported that the government's mandatory data retention proposals had resulted in a surge of interest by some Internet users in VPNs.[30] This suggests that mandatory data retention is likely to provide greater incentives for criminals and terrorists to conceal their communications, potentially complicating the work of security and law enforcement agencies and increasing the costs of legitimate surveillance. Accordingly, in so far as security and law enforcement agencies may find Internet metadata useful, this is most likely confined to data relating to unsophisticated or incautious Internet users, which may amount to a relatively narrow dataset. As explained in this submission, the risks entailed in collecting and retaining metadata relating to all Internet users outweigh these relatively modest potential benefits.

- *While access to telecommunications data can clearly be helpful to investigations conducted by law enforcement and security agencies, the evidence indicates that claims that mass collection and retention of metadata is essential are often over-stated. Independent analyses suggest that serious crime and terrorism may be just as effectively investigated by more targeted investigation techniques, which do not rely on mass data retention and which, accordingly, are less privacy-intrusive.*

- *The ready availability of techniques for masking metadata to users with no more than average sophistication suggests that blanket data retention regimes may be counter-productive, as they create an incentive for users to conceal their communications.*

[28] See Geoff Huston, 'Where is Metadata Anyway?', *CircleID,* 17 August 2014, http://www.circid.com/posts/print/20140817_where_is_metadata_anyway/.

[29] Parliamentary Joint Committee on Intelligence and Security, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation* (May 2013) 179-182.

[30] Chris Griffith, 'Australians flock to VPNs to avoid data retention, *The Australian,* 13 August 2014, http://www.theaustralian.com.au/technology/australians-flock-to-vpns-to-avoid-data-retention/story-e6frgakx-1227022957464?nk=2aa5a083f3e4d30361d9443a16e5c263.

Unacknowledged Risks of Blanket Data Retention

Mandatory blanket data retention regimes, such as that proposed in the Bill, pose significant risks, which do not seem to have been fully taken into account in assessing the proportionality of the proposals. In particular, the APF would like to highlight the following risks:

- **The Bill increases the danger of private sector misuses of personal data.**
  Businesses in the private sector exist to make a profit, through effective commercial exploitation of the assets they control. If service providers (such as carriers and ISPs) are required by law to hold more extensive information assets than they would otherwise hold (stored metadata), then they will seek to exploit these assets commercially, at least within the limits of what the law allows.

  As a result of what the provisions of this Bill do and (more importantly) do not require, the following consequences will arise for the personal data of Australians:

  (a) Content and web browsing history will be more extensively retained than would otherwise be the case;
  (b) More metadata (and associated content and/or browsing data) will be exploited commercially by service providers than would otherwise be the case;
  (c) More metadata (and associated content and/or browsing data) will be disclosed by service providers to other private sector users;
  (d) More metadata (and associated content and/or browsing data) will be retained longer than previously or would otherwise be the case, and longer than two years; and
  (e) Accordingly, the security risks inherent in the retention of personal data will increase significantly, because more (and more valuable) data will be retained for longer.[31]

  While the Bill creates the pre-conditions for the risks arising from mass collection of metadata that would otherwise not be created and/or retained, the APF considers that it makes no genuine attempt to prevent these dangers.

- **Content and browsing history will be stored as well as metadata.**

  As explained below, the Bill claims to exempt communications content and browsing history from the data retention regime. Regardless of these exemptions, however, there is nothing to prevent any service provider from keeping any such content or browsing history, and associating it with metadata. There are at least three reasons why a service provider may prefer (and therefore choose) to retain such associated content or browsing data:

  (a) It may be less costly to keep the content and/or browsing data than to determine which category of data it is and delete it.

  (b) There may be some temporary need to keep the content and/or browsing data, and it is then more costly to retrospectively delete it than it is to keep it.

  (c) If the associated metadata must be retained by law, then it may be more cost effective to economically exploit that retained metadata if associated content and/or browsing data is also retained and exploited.

[31] The Explanatory Memorandum to the Bill expressly acknowledges the privacy implications that arise from 'the increased volume of data which may be generated by the mandatory dataset arrangements': Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, Explanatory Memorandum, [46].

The result is that the requirements to store metadata are likely to increase the retention of associated content and browsing data, despite proposed s 187A(4) appearing to misleadingly give the contrary impression. Accordingly, the exclusion of browsing history from the proposed data set is disingenuous, to say the least. In this respect, this exclusion, and statements promoting the purported merits of the exclusion, seem reminiscent of statements made in debates about the failed 'Access Card' Bill that simply claimed that an Access card was not an ID card.[32]

The potential increased retention of data, including browsing history, poses unacknowledged risks associated with the use of such data by service providers, as well as third parties. Moreover, as further explained in this submission, the complete failure of the Bill to satisfactorily confine the telecommunications data that can be accessed under Chapter 4 of the TIA Act means that, once browsing history has been collected, it can be accessed by an enforcement agency without a warrant.

- **Insufficient control on the use of metadata by service providers and/or third parties.**
  There is nothing in the Bill that effectively prohibits service providers from using the retained metadata, together with associated content and browsing data. While there are some controls on the use of such data under the *Privacy Act 1988* (Cth) and Part 13 of the *Telecommunications Act 1997* (Cth), the APF considers these controls are far from adequate.

  Regarding the *Privacy Act,* the relevant Australian Privacy Principle (APP) is APP 6. Assuming that the data is 'personal information' for the purposes of the *Privacy Act,* and that the service provider is not entitled to the 'small business exemption', APP 6 essentially restricts the use of personal data to uses which are within the primary purpose of collection of the data (as notified in accordance with APP 5) or which the individual concerned would reasonably expect and are related to the primary purpose of collection (or 'directly related', for sensitive data). The primary purpose of collection of the metadata (and any associated data, such as browsing data) will always be for some purpose of the service provider, not the purpose of retaining the data due to a government requirement, so any expansion of the primary purpose of collection by a service provider, or of secondary purposes, allowed under APP 6 will apply to the additional data that has been retained. This also applies to the use of this data for direct marketing purposes (APP 7).

  Moreover, under APP 6, essentially the same rules apply to the disclosure of personal data to other businesses. The practical consequence is that a larger pool of data will be available for disclosure than would otherwise be the case.

  Part 13 of the *Telecommunications Act* regulates the confidentiality (use and disclosure) of information obtained by certain participants in the telecommunications industry during the supply of telecommunications services.[33] More specifically, it requires certain participants in the telecommunications industry – carriers, carriage service providers

[32] See, for example, Graham Greenleaf, ''Access All Areas': Function Creep Guaranteed in Australia's ID Card Bill (No. 1)' *Computer Law & Security Report*, (2008) Vol 24 No 1, 56-66 < http://law.bepress.com/unswwps/flrps/art64/>.

[33] The Explanatory Memorandum to the Bill states that 'service providers which are non-APP entities are subject to the data protection obligations contained in Part 13 of the Telecommunications Act': Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, Explanatory Memorandum, [48]. In so far as this implies that Part 13 does not apply to service providers that are APP entities it is inaccurate.

(CSPs), number database-operators, emergency call persons and their respective associates – not to disclose or use any information or document that relates to:

(a) the contents of communications that were carried, or are being carried, by a carrier or CSP;

(b) carriage services supplied or intended to be supplied by a carrier or CSP; or

(c) the affairs or personal particulars (including any unlisted telephone number or any address) of another person.[34]

In relation to the first category, it is important to note that Part 13 protects information or a document about a communication, but not the content or substance of a communication, which is protected under the TIA Act. Part 13 sets out a number of exceptions to the confidentiality rules. It also regulates the secondary use and disclosure of the relevant information by persons to whom the information is lawfully disclosed.[35] As an act or practice that is permitted under Part 13 is an act or practice that is 'authorised by or under law' for the purposes of the *Privacy Act*,[36] such uses or disclosures will not breach APP 6.

The APF submits that, largely as result of the exceptions to the confidentiality provisions, in the context of the greater amounts of data likely to be retained as a result of the Bill, the safeguards on the use and disclosure of data established under Part 13 are unsatisfactory. In particular, s 290 creates an exception to the use or disclosure of information with the implicit consent of the sender and recipient of a communication; and s 291 creates an exception for use or disclosure for the purpose of the business needs of a carrier or CSP. Furthermore, s 280 establishes an exception for use or disclosure to enforcement agencies pursuant to interception warrants; and where use or disclosure is required or authorised under law, including under Chapter 4 of the TIA Act. As this submission explains, the safeguards for accessing data under the TIA Act, and especially the warrantless access permitted under Chapter 4 of the TIA Act, are inadequate in that they fail to sufficiently protect the privacy of electronic communications.

- **Storage of metadata (and associated data) increases security risks of personal data.** As the CJEU pointed out in its ruling on the Data Retention Directive, any data retention regime must ensure adequate security and protection of the data retained by service providers. Any retention of personal data, whether by service providers, their agents, or those to whom they disclose the data, increases the risks to individuals resulting from security breaches. This was emphasised by Timothy Pilgrim, Australia's Privacy Commissioner who, in a public statement on the data retention proposals cautioned that '[t]he retention of large amounts of personal information for an extended period of time increases the risk of a data breach'.[37] All of the factors discussed above have the potential to increase the scope and duration of personal data retained by carriers and ISPs, and parties to whom it may be disclosed. Furthermore, the attraction to hackers, or to insider miscreants, is increased by the aggregation of the personal data involved. In

[34] *Telecommunications Act 1997* (Cth) ss 276-278.
[35] *Telecommunications Act 1997* (Cth) ss 296-303A.
[36] *Telecommunications Act 1997* (Cth) s 303B.
[37] Timothy Pilgrim, Australia's Privacy Commissioner, 'Australian Government's data retention proposal – statement', 8 August 2014, http://www.oaic.gov.au/news-and-events/statements/privacy-statements/australian-governments-data-retention-proposal/australian-government-s-data-retention-proposal.

effect, the Bill has the potential to create 'honeypots' of personal data where little previously existed, or which would not otherwise be created, thereby facilitating computer crime.

Businesses have no absolute liability for the results of these increased risks, only a potential obligation under APP 11.1 of the *Privacy Act* to take 'such steps as are reasonable in the circumstances to protect the information'. Given the weakness of the data security principle in APP 11, individuals concerned effectively bear the risk if their additional personal data that has been retained is hacked without negligence on the part of the service provider. In this way, the Bill has unintended consequences that effectively stack the cards against individuals and the protection of their privacy. These consequence reinforce the lack of proportionality of mandated blanket data retention; the risks to individuals are very serious and indiscriminate, and certainly much more than acknowledged by proponents of the Bill.

While the Explanatory Memorandum to the Bill points out that the government intends to introduce legislation implementing proposed Telecommunications Sector Security Reforms (TSSR) by means of a statutory obligation on carriers and CSPs to 'do their best' to prevent unauthorised access,[38] this legislation has yet to be introduced, and the effectiveness of any such regime remains, at best, uncertain. Moreover, given the likely increase in the volume of data expected to be retained by carriers and ISPs, the TSSR will impose greater costs on industry than would be the case in the absence of a blanket data retention law.

- **'Chilling effect' of perceived mass surveillance.**

  In its ruling on the Data Retention Directive, the CJEU was specifically concerned that the mass retention of data was 'likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance'.[39] A substantial literature exists on the potential for the awareness of being under constant surreptitious surveillance, with no capacity to determine what will trigger some suspicion, to have serious adverse effects on free speech, behaviour, mental processes and cultural expression. For example, a recent survey of 800 writers conducted by PEN, the main NGO for writers concluded that global surveillance by governments was severely inhibiting free expression and creative freedom, prompting many writers, including those in democratic societies, to engage in self-censorship.[40] As explained in this submission, while the mass retention of data may have adverse effects on those who should never come under suspicion, it is highly likely to cause others to adopt measures to avoid detection, thereby complicating the work of law enforcement and security agencies.

- **Mass collection and storage of metadata (and associated data) increases risk of scope creep as data is available for use in litigation.**

  Given the volume of data that will be retained by carriers and ISPs, there will be considerable pressure for such data to be accessed and used for purposes other than law enforcement and national security. In particular, there will be immense pressure for the data to be accessed and used in both civil and criminal legal proceedings by parties

[38] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, Explanatory Memorandum, [45].

[39] Court of Justice of the European Union, Judgment in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others,* Judgment of 8 April 2014, para. [37].

[40] 'New PEN Report Demonstrates Global Chilling Effect of Mass Surveillance', PEN America, January 5, 2015, http://www.pen.org/press-release/2015/01/05/new-pen-report-demonstrates-global-chilling-effect-mass-surveillance.

who are not authorised to access the data under the TIA Act. In terms of criminal law proceedings, prosecutors will have clear incentives to seek to access data on the basis of speculation alone; while defence lawyers will have incentives to request access to potentially exculpate their clients. And further, Courts may clearly order the disclosure of records wherever relevant across a broad range of cases. In terms of civil litigation, the data exists as a 'honey-pot' for a broad range of actors. Parties to disputes in family law, and in all manner of commercial disputes (involving, for example, trade secrets, intellectual property, and defamation) will likely seek disclosure of retained metadata. For instance, Communications Minister Turnbull and the AFP have announced that data records could be made available for copyright litigation purposes.[41] Claims that the data will not be used by agencies for purposes other than those permitted under the TIA Act are simply disingenuous, as the Bill does not impose any limitations on access to the data by means of other legal avenues, including conventional litigation processes.

This unintended consequence of the Bill, arising from the existence of data that would otherwise not be retained, not only has cost implications for carriers and ISPs, but highlights the possibility of the retained data being used for a host of purposes outside the objectives permitted under the TIA Act.

- *Blanket data retention regimes pose a range of risks, which do not seem to have been taken into account by proponents of the Bill. In particular, the Bill will result in the collection and retention of much more data about users than would otherwise be the case, with the attendant risks associated with such large data sets. These risks include: risks associated with unanticipated uses of the data by service providers; risks associated with disclosures to third parties; and risks associated with the difficulties of adequately ensuring the security of large data sets. The APF submits that the current legal controls on the use, disclosure and security of such data, including those established under the Privacy Act 1988 (Cth) and Part 13 of the Telecommunications Act 1997 (Cth), are inadequate.*

- *Further risks posed by the mass collection and retention of telecommunications data include risks arising from Australians feeling they may be subject to constant mass surveillance and the potential for scope creep, including the use of such data in litigation unrelated to crime prevention and national security.*

[41] Knott, Matthew, 'Malcolm Turnbull introduces legislation for metadata retention scheme', *The Sydney Morning Herald,* October 30 2014, http://www.smh.com.au/federal-politics/political-news/malcolm-turnbull-introduces-legislation-for-metadata-retention-scheme-20141030-11e101.html.

Problems with the Definition of the Data Set

Changes in technology and business practices have clearly changed the nature of the data collected and retained by carriers and ISPs, especially (but not exclusively) in relation to the use of mobile devices.[42] These changes have contributed to significant confusion and uncertainty about the meaning of the term 'metadata'. They have also made it difficult to satisfactorily define the nature of the data required to be retained by the Bill.

The Bill does not seek to define the relevant data set, leaving the precise definition to be prescribed by regulations. Instead of defining the data set, the Bill provides[43] that the data defined in the regulations must relate to one or more broad categories of data, namely:

- Characteristics of a subscriber of a relevant service;
- Characteristics of an account, telecommunications device or other relevant service, relating to a relevant service;
- The source of a communication;
- The destination of a communication;
- The date, time and duration of a communication, or of its connection to a carriage service;
- The type of a communication and relevant service used in connection with a communication; and
- The location of equipment or a line used in connection with a communication.

The data falling within these categories, and which therefore may be prescribed by regulations, are further described in a table in the Explanatory Memorandum to the Bill, although the 'table is not exhaustive'.[44] At the time of introducing the Bill, the government publicly released a draft data set, which was referred to the PJCIS for review and public consultation.[45] The Bill also specifies certain data that cannot be prescribed by the regulations, including the contents and substance of a communication and data that states an address to which a communication was sent on the internet by means of an internet access service.[46] The last exception is designed to exclude internet browsing data from the scope of the data retention regime.[47]

When introducing the Bill, the government established a joint government-industry Implementation Working Group (IWG) to consult on a range of matters, including definition of the data set. The IWG has released a report which recommends that the government consider amendments to the data set and to the explanatory material accompanying the data set.[48] The IWG report noted ongoing difficulties of defining the data set, especially as 'significant technological change is likely to occur within the Australian telecommunications industry, with potential for significant technological evolution even in the short term'.[49] In identifying problems with the original data set, the IWG recommendations highlighted some terminological confusion, difficulties in collecting some of the information, and the open-ended language used in some examples.

---

[42] Geoff Huston, 'Where is Metadata Anyway?', *CircleID,* 17 August 2014, http://www.circid.com/posts/print/20140817_where_is_metadata_anyway/.

[43] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, cl 187A(2).

[44] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, Explanatory Memorandum, cl 26.

[45] See *Report 1 of the Data Retention Implementation Working Group,* Attachment A.

[46] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, cl 187A(4).

[47] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, Explanatory Memorandum, cl 38.

[48] *Report 1 of the Data Retention Implementation Working Group.*

[49] *Report 1 of the Data Retention Implementation Working Group,* 5.

The APF considers that it is desirable to introduce a legislative definition of telecommunications data in the TIA. As explained in this submission, a definition of telecommunications data is needed to address the current unsatisfactory state of affairs in which the data that may be accessed under Chapter 4 of the Act remains undefined. The APF therefore does not oppose the introduction of a statutory definition, particularly if this effectively excludes internet browsing data. The APF, however, opposes the manner in which the data set is dealt with in the Bill, and especially the use of the unduly broad and vague legislative criteria set out in the Bill for specifying the data set.

The APF considers that the way in which the data set is defined in the Bill is deeply problematic in the following respects:

- **The data set is not appropriately limited to that which is necessary and proportionate for law enforcement and national security.**

The Explanatory Memorandum to the Bill claims that:

> The types of data that may be prescribed are circumscribed to remain necessary and proportionate to the legitimate aim of ensuring that law enforcement and intelligence agencies have access to the critical data they require to safeguard national security and prevent or detect criminal activity.[50]

As explained above, however, in its ruling invalidating the Data Retention Directive, the CJEU held that the data set required to be retained was disproportionate not only in so far as it indiscriminately applied to data relating to all subscribers and users of electronic communications, but as it applied to all forms of traffic data 'without any differentiation'.[51] As detailed below, this submission opposes, as a matter of principle, the blanket collection and retention of telecommunications data, and recommends that consideration be given to the adoption of a more circumscribed and targeted data preservation regime. Accordingly, the APF submits that the most effective way of ensuring that the data set is necessary and proportionate to the aims of law enforcement and national security is to establish a data preservation regime, which incorporates adequate thresholds and procedural safeguards so as to ensure that the data are sufficiently relevant to specific investigations.

- **The statutory categories in the Bill are too broad and uncertain, leaving too much detail to the regulations.**

Data retention (or, indeed, data preservation) regimes entail a high level of interference with the privacy of subscribers and users. As such, it is important for essential components of such regimes, such as the definition of the data set, to be subject to adequate Parliamentary scrutiny. The APF therefore submits that it is inappropriate for the scope of the data set to be effectively left to be determined by regulations, as currently proposed by the Bill. While the APF acknowledges that ongoing changes in technologies and business practices, and the associated need for flexibility, means that there is a role for some details of the data set to be left to delegated legislation, the APF submits that there is considerable scope for the data set to be more precisely defined in legislation than is the case in the current Bill.

[50] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, Explanatory Memorandum, cl 25.

[51] Court of Justice of the European Union, Judgment in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others,* Judgment of 8 April 2014, para. [57].

- **Telecommunications data which can be accessed under the TIA Act should be defined.**

As explained below, Chapter 4 of the TIA Act, which allows for warrantless access to non-content telecommunications data, does not include a definition of the data that can be accessed. A major concern with the access regime established under Chapter 4 is that the key term, 'telecommunications data', remains undefined. A key example of the terminological confusion that arises from the failure to adequately define the data that can be accessed under the Chapter 4 regime is whether a uniform resource locator (URL) is properly classified as 'stored content' (and therefore subject to the Chapter 3 access regime, or non-content telecommunications data, and therefore able to be accessed without a warrant under Chapter 4. The differing views on this issue were explained in a blog post to the Parliamentary Library website in August 2014.[52] The problem is illustrated by Telstra's evidence to the 2012 PJCIS inquiry into potential reforms of national security legislation, which indicated that it disclosed URLs to agencies as non-content telecommunications data, but not where a URL identifies the content of the communication.

The APF submits that, just as there is a need for the scope of retained or preserved data to be defined in legislation, there is a need for the scope of data which may be lawfully accessed to be appropriately defined. This should appropriately limit the scope of data that falls within Chapter 4, as well as enhance certainty of carriers and CSPs required to respond to applications for access.

- **Problems with the 'browsing history' exclusion.**

In proposed s 187A(4(b), the Bill purports to exclude information about subscribers' web history from the data retention regime. The Explanatory Memorandum to the Bill states that this provision will ensure that 'service providers are not required to keep records of the uniform resource locators (URLs), internet protocol (IP) addresses, port numbers and other internet identifiers with which a person has communicated via an internet access service provided by the service provider'.[53]

There are a number of problems with the purported 'browsing history' exclusion. First, as the exclusion is limited to information that 'states an address', there may be questions about precisely which sorts of data qualify as an 'address'. Second, and importantly, the exclusion of browsing history data applies only to the data retention regime. As there is no definition of 'telecommunications data' in the Chapter 4 access regime, and therefore no similar exclusion, where browsing history data is voluntarily retained there is no obstacle to the data being accessed by agencies. Without a guarantee that browsing history will not be accessed, prominent claims that the proposed data retention regime is not privacy-intrusive because it does not mandate the retention of browsing history data are simply disingenuous.

Third, a particular problem arises from the use of current and emerging practices of Internet address sharing, including what is known as Carrier Grade Network Address Translation (CGN), which is associated with the exhaustion of the IPv4 address space. In short, the sharing of IP addresses, currently in mobile networks but increasingly in other networks, means that the only way to identify a user is to record the destination IP address as well as the source IP address. As Huston has explained, where CGN entails sharing of both IP addresses and port numbers, 'the only way to disambiguate individual connections in the

[52] Jaan Murphy, 'Access to and retention of internet 'metadata', *FlagPost,* 18 August 2014, C:\Users\David\Desktop\Access to and retention of internet 'metadata'.htm.

[53] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, Explanatory Memorandum, cl 38.

CGN log is to log both source and destination IP addresses'.[54] This raises a conflict between the kinds of information required to be retained under s 187A(2) – which includes characteristics of the subscriber, of an individual account and the source of a communication – and the purported exclusion of the destination address in s 187A(4)(b). The consequence of the way in which the Bill is currently drafted is that in order to comply with the obligations to identify the characteristics of subscribers and sources of communications, in relevant applications of CGN, carriers and ISPs will need, in practice, to retain destination IP addresses. In this respect, it is important to note that proposed s 187A(4)(b) does not prohibit service providers from voluntarily retaining destination IP addresses, but simply provides that they are not required to retain such addresses.

- *The APF submits that there are a number of problems with the way in which the proposed data set is dealt with in the Bill. In particular, the data set is not appropriately limited to that which is necessary and proportionate for law enforcement and national security and the statutory categories in the Bill are too broad and uncertain, leaving too much detail to the regulations.*
- *The APF recommends the introduction of a definition of 'telecommunications data' for the purposes of the access regime in Chapter 4 of the TIA Act. Such a definition is required to remove uncertainty about the data that can be accessed under that regime.*
- *The APF submits that there are serious problems with the way in which browsing history is dealt with in the Bill, including in proposed s 187A(4(b). In particular, as there is no prohibition on service providers collecting and retaining Internet browsing history, which may be accessed as telecommunications data under Chapter 4 of the TIA Act, claims that the exclusion of browsing history from the data set means that the Bill is not privacy-intrusive are disingenuous. Moreover, as some technologies currently deployed by service providers require the logging of destination IP addresses in order to determine the source of a communication, the collection and retention of some browsing history data may be required in order for service providers to comply with their data retention obligations. The APF therefore recommends that the 'browsing history' exclusion be revisited with a view to addressing these problems.*

Duration of Data Retention Obligation

Proposed s 187C of the Bill specifies that, in general, the relevant data is to be retained for a period of 2 years after it comes into existence. The APF is concerned that the proposed two year extension period may be excessive and disproportionate in relation to the objectives of the Bill, and that it may impose disproportionate costs on carriers and ISPs. In this respect, we draw attention to the submission made to this inquiry by the Communications Alliance and AMTA, which notes that the majority of requests made by agencies to access telecommunications data held by ISPs relate to data that is less than 6 months old. The APF therefore submits that the duration of any statutory obligation to retain or preserve data should be limited, in the first instance, to 6 months, with the possibility of this being reviewed should evidence establish that it is insufficient.

[54] Geoff Huston, 'Where is Metadata Anyway?', *CircleID,* 17 August 2014, http://www.circid.com/posts/print/20140817_where_is_metadata_anyway/.

- *The APF submits that the two year retention period is excessive in relation to the objectives of the Bill, and recommends that this be reduced to six months.*

Access to Telecommunications Data and Stored Communications

Any requirements for retaining or preserving data must be accompanied by adequate and appropriate procedural safeguards regulating access to such data. In its ruling invalidating the Data Retention Directive, the CJEU pointed to the absence of substantive and procedural safeguards on access to retained data and their subsequent use. In particular, the Court was concerned that access to retained data was not dependent on prior review by a court or independent administrative body, which would determine whether the access was necessary for the objective pursued.[55] The APF recognises that access to content and to metadata can be of great value to law enforcement and national security agencies in their investigations. Nevertheless, an absence of adequate legal safeguards on access to content and data opens the door to widespread surveillance conducted on the basis of convenience rather than necessity.

The access regimes under the TIA Act draw a fundamental distinction between access to content and access to telecommunications data. The TIA Act provides for access by means of a warrant, with a distinction between the regime applying to real-time interception warrants (such as phone calls), dealt with in Chapter 2 of the Act, and that applying to 'stored communications' (such as emails and text messages), which is set out in Chapter 3. Access to telecommunications data (as opposed to content) is dealt with in Chapter 4, which provides for such content to be accessed without a warrant. Schedule 2 of the Bill introduces amendments to Chapters 3 and 4 which limit the scope of agencies that can apply for stored communications warrants under Chapter 3 and that can access telecommunications data under Chapter 4 in order to ensure that 'data access arrangements are rigorously scrutinised'.[56] While the APF welcomes the limitations introduced by the Bill, we submit that they fall well short of the procedural safeguards required to adequately protect the privacy of communications content and telecommunications data.

Chapter 3 of the TIA Act, which applies to 'stored communications', was introduced in 2006[57] in order to clarify the position relating to access to stored communications, which until then had been uncertain. The stored communications regime enables an 'enforcement agency' to apply for a stored communication warrant to investigate a 'serious contravention'. The definition of 'stored communications' in s 5 of the Act, when read together with the broad definition of 'communication', indicates that communications are not necessarily confined to content, but may include metadata relating to stored communications content. Whereas a warrant for the interception of a real-time communication can only be granted in relation to an investigation of a ';serious offence', a stored communications warrant can be granted in

[55] Court of Justice of the European Union, Judgment in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others,* Judgment of 8 April 2014, paras. [61]-[62].

[56] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, Explanatory Memorandum, cl 84.

[57] *Telecommunications Interception (Amendment) Act 2006* (Cth).

relation to investigating a 'serious contravention'. A 'serious contravention' is defined in s 5E of the Act to include a 'serious offence', which is defined by s 5D to be an offence punishable by imprisonment for a maximum period of 7 years, but to extend to offences punishable by imprisonment for a maximum period of 3 years. Applications for stored communications warrants must be made to 'issuing authorities', which include judges (such as members of the Federal Court of Australia, Family Court of Australia and State magistrates) and designated members of the AAT.

In its inquiry into the Bill that introduced the stored communications regime, the Senate Committee on Legal and Constitutional Affairs expressed concerns that the regime did not strike the right balance between the protection of privacy and public interest objectives, such as law enforcement. In this respect, the Committee's report stated that:

> The Bill would result in a wide number of government agencies being able to covertly obtain material for investigating a significant range of sometimes relatively minor offences.
>
> The Committee is of the view that the invasion of privacy resulting from covert interception of communications is significant and should therefore only be accessible to core law enforcement agencies.[58]

As explained below, the APF considers that although the amendments to Chapter 3 proposed in the Bill go some way to addressing the concerns identified by the Senate Committee, albeit belatedly, they fall short of the reforms needed to appropriately protect the privacy of stored communications.

While it seems that metadata associated with a stored communication may be accessed by means of a warrant, Chapter 4 of the TIA Act makes it clear that a warrant is not required to access such data. Access to telecommunications data (as opposed to content) is currently regulated by Chapter 4 of the TIA Act, which was introduced in 2007.[59] Chapter 4 provides for the voluntary disclosure of information or document, other than the contents or substance of a communication, despite the confidentiality obligations imposed on entities such as carriers and CSPs under Part 13 of the Telecommunications Act. By excluding the contents or substance of communications,[60] the disclosure regime is effectively confined to telecommunications data (or metadata). In effect, the regime permits an 'enforcement agency' to authorise a carrier or carriage service provider to disclose telecommunications data where it is reasonably necessary for the enforcement of the criminal law, a law imposing a criminal penalty, or the protection of the public revenue.[61] Separate provisions relate to access to telecommunications data for national security purposes.[62] In addition, a separate provision applies to authorisations of access to prospective, or near real-time, telecommunications data, which can only be made by a 'criminal law-enforcement agency'.[63] An 'enforcement agency' is defined extremely broadly to include all agencies entitled to intercept the contents of communications as well as bodies whose functions include administering a law imposing a pecuniary penalty or administering a law relating to the protection of the public revenue.[64]

The regime permitting warrantless disclosure of telecommunications data, while controversial, has been widely used. Between July 2012 and June 2013 there were 319,874

---

[58] Senate Committee on Legal and Constitutional Affairs, *Report on Inquiry into Provisions of the Telecommunications (Interception) Amendment Bill 2006,* 27 March 2006, paras 3.40-3.41.

[59] *Telecommunications (Interception and Access) Act 2007* (Cth).

[60] TIA Act, s 172.

[61] TIA Act, ss 178-179 (historical data).

[62] TIA Act, ss 174-176.

[63] TIA Act, s 180 (prospective, or near real-time data).

[64] TIA Act, s 5 (definition of 'enforcement agency').

authorisations by Australian governments for access to telecommunications information.[65] Those authorisations included Bankstown City Council, Ipswich City Council, Knox City Council, Wyndham City Council, the RSPCA in three states, Australia Post, the Clean Energy Regulator, Workcover NSW, WA Department of Fisheries, Australian Health Practitioner Regulation Agency, Tax Practitioners Board, Medicare, Department of Immigration & Citizenship, Harness Racing NSW and the national and state police forces. Quite clearly, the unfettered access permitted under the existing regime is overly broad, with much of the access relating to neither national security nor serious crime. Evidence presented to the current inquiry indicated that Victorian police have sought access telecommunications data 310,000 times in the past five years, while the Australian Federal Police have sought access 110,000 times in the same period.[66] In its 2013 report on potential reforms of national security legislation, the PJCIS recommended a review of the threshold for authorising access to telecommunications data, with a focus on reducing the number of agencies entitled to access and increasing the threshold of the gravity of conduct which may entitle access to telecommunications data.[67]

The Bill amends the regimes relating to access to stored communications and telecommunications data by:

- Introducing a new definition of 'criminal law-enforcement agency', for the purposes of the stored communications access regime in Chapter 3 of the TIA Act and the telecommunications data regime in Chapter 4 of the TIA Act, which is effectively confined to Australian police forces and anti-corruption agencies that have the ability to apply for interception warrants, as opposed to laws imposing pecuniary penalties and revenue laws, but which may be extended by a declaration by the Attorney-General;[68]
- Introducing a new definition of 'enforcement agency' for the purposes of historical telecommunications data pursuant to Chapter 4 of the TIA Act, which includes a 'criminal enforcement agency', but which may be extended to other authorities and bodies by a determination by the Attorney-General;[69]
- Introducing new oversight and accountability provisions, modelled on Part 6 of the *Surveillance Devices Act 2004* (Cth), which extend the role of the Commonwealth Ombudsman to assess compliance with an enforcement agency's obligations under Chapters 3 and 4 of the TIA Act;[70] and
- In particular, extending the role of the Ombudsman to auditing the use and access to data retained as a result of the data retention regime.[71]

The Explanatory Memorandum to the Bill claims that the amendments to the agencies entitled to access stored communications and telecommunications data 'promote the protection from unlawful and arbitrary interference with privacy by ensuring that access to data only occurs in confined circumstances as dictated by operational need and that the ability to become an agency who may access telecommunications data is closely circumscribed and subject to parliamentary disallowance.'[72]

---

[65] Attorney-General's Department, *Telecommunications (Interception and Access) Act 1979,* Annual Report 2012-13, 49.

[66] David Wroe and Nino Bucci, 'Privacy fears on 'spy' laws', *The Age,* 14 January 2015.

[67] Parliamentary Joint Committee on Intelligence and Security, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation* (May 2013), Recommendation 5, 26.

[68] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, Sched 2, cl 110A.

[69] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, Sched 2, cl 176A.

[70] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, Sched 3, cll 186B-186E.

[71] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, Sched 3.

[72] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, Explanatory Memorandum, Statement of Compatibility with Human Rights, cl 39.

The APF supports the very limited reforms made in the Bill, but disputes the claims made in the Explanatory Memorandum on the basis that the safeguards and accountability mechanisms in the Bill are inadequate, at least in the following respects:

- **Definition of 'criminal law-enforcement agency'.** The APF submits that too much discretion is given to the Attorney-General in declaring bodies or authorities to be a criminal law-enforcement agency. While the Bill provides that the Attorney-General must consider a range of factors, including whether the functions of the authority or body include investigating serious contraventions, this is not an effective limitation on the Attorney-General's discretion, and could potentially mean that the scope of the definition could be extended to bodies administering laws imposing pecuniary penalties or revenue laws. The APF considers that the ability to seek a stored communications warrant, or authorise access to historical telecommunications data, should be confined to authorities or bodies responsible for investigating serious criminal offences, serious allegations of public corruption, or serious threats to national security. Consequently, the APF recommends significantly limiting the Attorney-General's discretion, so that it is effectively confined to such bodies or authorities. Moreover, in exercising the determination-making power, the APF recommends that the Attorney-General be specifically required to take into account the effect of a determination on the right to privacy.

- **Definition of 'enforcement agency'.** Under the access regime proposed in the Bill, only a 'criminal law-enforcement agency' will have standing to apply for stored communications warrants (and authorise access to prospective telecommunications data), whereas an 'enforcement agency' will be entitled to authorised access to historical telecommunications data. The definition of an 'enforcement agency' is broader than the definition of a 'criminal law-enforcement agency' in that the Attorney-General has an additional power to declare an authority or body that is not a law-enforcement agency, to be an enforcement agency.[73] In making such a declaration, the Bill provides that the Attorney-General must consider a range a factors, specifically including whether the functions of the authority or body include administering a law imposing a pecuniary penalty or a law relating to the protection of the public revenue.[74] The Explanatory Memorandum to the Bill justifies the potentially broader scope of authorities or bodies entitled to access telecommunications data on the basis of the 'higher level of intrusion into privacy occasioned by access to stored communications and prospective telecommunications data'.[75] As this submission has explained, however, access to telecommunications data (or metadata) now poses equivalent risks to privacy, and in some instances manifestly greater risks, than access to communications content. Consequently, the APF recommends that there should be no distinction between authorities and bodies entitled to apply for a stored communications warrant and those entitled to access telecommunications data, such that the ability to access such data should be confined to authorities or bodies responsible for investigating serious criminal offences, serious allegations of public corruption, or serious threats to national security.

- **Thresholds for access to stored communications and telecommunications data.** The Bill does not alter the thresholds for access to stored communications or telecommunications data under the TIA Act. Given the extent to which access to telecommunications data may interfere with the right to privacy just as much as access to communications content, the APF considers there is a strong case for introducing a

[73] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, Sched 2, cl 176A(3).
[74] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, Sched 2, cl 176A(4)(a).
[75] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, Explanatory Memorandum, cl 91.

uniformly high threshold for access to both communications content and telecommunications data. In this respect, the APF notes that, in its inquiry into the 2006 Amendments, the Senate Committee on Legal and Constitutional Affairs was as concerned with the relatively minor offences which could justify access to stored communications as with the range of agencies entitled to access. The APF therefore submits that there is no justification whatsoever for a lower threshold – which requires only that an investigation relate to a 'serious contravention' – to apply to access to stored communications than the threshold that applies to real-time interceptions – which requires that an investigation relate to a 'serious offence'. In this respect, the APF reiterates the following comments made in its submission to the Senate Committee on Legal and Constitutional Affairs in its inquiry into the 2006 Amendments:

> The principle that invasion of privacy through covert interception should only be allowed in relation to genuinely serious offences is clearly established in the existing regime. In our view, no convincing case has been mounted for why a lower threshold should apply to stored communications, which can contain information just as private, sensitive and even intimate. In the absence of any such case, it is difficult to have a rational discussion about where the threshold should be set, but we strongly urge the Committee to recommend higher thresholds than those proposed.[76]

Accordingly, the higher threshold should apply to access to both real-time communications and stored content, and require that such access relate to investigations of serious criminal offences (ie. offences punishable by imprisonment for at least 7 years, as opposed to the current 3 year applying to stored communications), serious allegations of public corruption, or serious threats to national security. Given the extremely serious privacy implications of access to telecommunications data, the APF further submits that access to such data should be subject to the same thresholds as apply to communications content.

- **Warrantless access to telecommunications data.** Under Chapter 4 of the TIA Act, an enforcement agency may authorise a carrier or CSP to disclose historical telecommunications data where access is reasonably necessary to enforce a criminal law, enforce a law imposing a pecuniary penalty or protect the public revenue. The disclosure of prospective data, on the other hand, may only be authorised by a criminal enforcement agency when it is considered reasonably necessary for the investigation of an offence with a maximum term of 3 years' imprisonment. As explained immediately above, the APF considers that the current thresholds for access are too low, and that there is a strong case for higher thresholds for access to both stored content and telecommunications data. The disclosure of telecommunications data may only be approved by an authorised officer of the relevant enforcement agency. The APF considers that, given the highly privacy intrusive nature of much telecommunications data, the current Chapter 4 access regime incorporates insufficient procedural safeguards for access to telecommunications data, as access does not depend upon a decision of an independent body competent to determine whether the interference with privacy is proportionate to the relevant law enforcement or security objectives. At a minimum, and as supported by the CJEU ruling on the Data Retention Directive, the APF submits that adequate procedural safeguards must be placed on applications for access to non-content telecommunications data. As pointed out in the APF's submission to the Senate Standing Committee on Constitutional and Legal Affairs' inquiry into a comprehensive revision of the TIA Act: 'Metadata and content should be treated similarly, and in particular, the traditional legal process for authorising breaches of an individual's rights, namely the intercession of an independent judge assessing the specific case made in an application for a warrant should be applied to metadata

[76] Australian Privacy Foundation, *Submission to the Senate Legal & Constitutional Committee's Inquiry into the Telecommunications (Interception) Amendment Bill 2006*, March 2006, at http://www.privacy.org.au/Papers/index.html.

surveillance. If this surveillance is on a huge scale, with no consideration taken of association with individual offences or threats, the requirement for a warrant may offer a useful discipline'.[77] In most cases, and without being prescriptive in this submission, this should involve a process analogous to that applying to the issue of warrants for access to real-time interceptions and stored communications.

- **Oversight and accountability mechanisms.**
  As the TIA Act currently stands, there is no independent oversight of the regime that applies to access to telecommunications data under Chapter 4, and oversight of the stored communications regime in Chapter 3 is limited to the Commonwealth Ombudsman's role in monitoring compliance with an agency's record keeping and record destruction obligations. Schedule 3 of the Bill would enhance oversight and accountability of the relevant access regimes by extending the Ombudsman's role to monitoring agency compliance in exercising their powers with Chapters 3 and 4, and incorporating an auditing function.

  The APF welcomes the enhanced oversight and accountability mechanisms contained in the Bill, but is concerned that, given the highly intrusive nature of the data retention proposals, they are insufficient. In particular, the APF points out that any oversight by the Ombudsman occurs after communications content or telecommunications data has been accessed, and therefore after privacy harms have been incurred. To address this shortcoming, the APF recommends that consideration be given to introducing greater oversight at the time of application for access to content or data. In particular, the APF considers that there is a case for the introduction of a Commonwealth Public Interest Monitor (PIM), which would be notified of applications for access, and be empowered to appear and make submissions on applications for warrants and access. In this respect, the APF notes that the TIA Act already provides for such roles for the Queensland PIM and the Victorian PIM in relation to applications for warrants, by Queensland and Victorian agencies, for access to real-time communications.[78] The APF considers that introducing a Commonwealth PIM, with a role in relation to applications under Chapters 3 and 4, as well as Chapter 2 applications, would introduce a much-needed degree of transparency to the processes for granting access to both content and data.

[77] Australian Privacy Foundation, *Submission to the Senate Legal & Constitutional Committee's Inquiry into a Comprehensive Revision of Telecommunications (Interception and Access) Act 1979,* 13 March 2014, at http://www.privacy.org.au/Papers/index.html.

[78] See, for example, TIA Act, ss 44A, 45,

- *The APF submits that too much discretion is given to the Attorney-General to declare bodies or authorities to be a 'criminal law-enforcement agency' for the purposes of the stored communications regime in Chapter 3 of the TIA Act. The APF recommends that the ability to seek a stored communications warrant, or authorise access to historical telecommunications data, should be confined to authorities or bodies responsible for investigating serious criminal offences, serious allegations of public corruption, or serious threats to national security. The APF further recommends that, in exercising the determination-making power, the Attorney-General be specifically required to take into account the effect of a determination on the right to privacy.*

- *The APF submits that, given the highly privacy-intrusive nature of metadata, the definition of an 'enforcement agency' for the purposes of access to historical telecommunications data is too broad. The APF therefore recommends that access to telecommunications data for the purposes of Chapter 4 of the TIA Act should be confined to authorities or bodies responsible for investigating serious criminal offences, serious allegations of public corruption, or serious threats to national security.*

- *The APF submits that the thresholds for access to stored communications and telecommunications data under the TIA Act are too low. The APF recommends that the threshold for access to stored communications should be brought into line with the threshold for interceptions of real-time communications such that access must relate to investigations of offences punishable by imprisonment for at least 7 years. The APF further recommends that the same thresholds should apply to access to telecommunications data under Chapter 4 of the TIA Act.*

- *The APF submits that, given the highly privacy-intrusive nature of metadata, the procedural safeguards for access to telecommunications data under Chapter 4 of the TIA At are inadequate. The APF therefore recommends that procedural safeguards be introduced to regulate access to non-content telecommunications data, which involve a decision of an independent body required to balance the objectives of access against the intrusion on the right to privacy. The safeguards should involve a process analogous to applications for a warrant for access to real-time communications and stored communications.*

- *The APF welcomes the enhancement to the oversight and accountability mechanisms for access to stored communications and telecommunications data, including the enhanced role of the Commonwealth Ombudsman, contained in Schedule 3 of the Bill. Especially given the highly privacy-intrusive nature of both stored communications and metadata, the APF recommends that consideration be given to establishing a Commonwealth Public Interest Monitor (PIM), who would be empowered to appear and make submissions on applications for warrants and access.*

Necessary and Proportionate Measures: The Merits of a Limited Data Preservation Regime

As this submission has explained, courts and human rights bodies have unanimously found that blanket data retention regimes, such as those proposed in the Bill, are neither necessary nor proportionate to the legitimate objectives served by law enforcement and national security agencies. Blanket regimes are disproportionate because they indiscriminately mandate the retention of data relating to entire populations, irrespective of the nature of the data or of whether or not there is a reasonable suspicion of a serious threat posed by those to whom the data relates. The mass retention of data, much of which is 'personal information', represents an interference with privacy that cannot be justified on the basis that there is a possibility, however remote, that it may possibly be useful. Nevertheless, the APF acknowledges that, in certain circumscribed circumstances, access to telecommunications data is helpful to law enforcement and security agencies. The APF also acknowledges that, given changes in technologies and business practices, there is a case for carriers and ISPs, in clearly circumscribed circumstances, to be required to retain certain data that would otherwise not be retained. The legitimate objectives of law enforcement and national security can, however, be met by measures that are far less intrusive than those contained in the Bill.

An important terminological distinction can be drawn between data retention regimes, which customarily incorporate blanket data retention, and data preservation regimes, under which applications can be made to preserve data that is related to specific investigations.[79] In a report on comparative approaches to data preservation prepared for the European Commission in November 2012, the Centre for Strategy and Evaluations Services defined data preservation as the expedited storage of particular data in 'situations where a person or organisation (which may be a communications service provider or any physical or legal person who has the possession or control of the specified computer data) is required by a state authority to preserve specified data from loss or modification for a specific period of time'.[80]

The stored communications regime in Part 3 of the TIA Act includes, in Part 3-1A, which was introduced in 2013, a data preservation regime. Under this regime, an issuing agency can give a preservation notice to a carrier requiring the preservation of all stored communications that relate to the person or telecommunications service specified in the notice.[81] There are two types of preservation notices: domestic preservation notices, which cover stored communications that relate to breaches of certain Australian laws; and foreign preservation notices, which cover stored communications that relate to contraventions of certain foreign laws (and which may only be given by the Australian Federal Police). In relation to domestic preservation notices, historic notices cover stored communications held by a carrier on a particular day, while ongoing notices cover stored communications held by a carrier in a 30 day period. Failure to comply with a preservation notice is a breach of the carrier's national interest obligations under s 313 of the *Telecommunications Act.*[82] Preservation notices do

[79] See Chris Jones and Ben Hayes, Securing Europe through Counter-Terrorism: Impact, Legitimacy, Effectiveness (SECILE), *The EU Data Retention Directive: a case study in the legitimacy and effectiveness of EU counter-terrorism policy,* 8 April 2014, 20-21.

[80] Centre for Strategy & Evaluations Services, 'Evidence of Potential Impacts of Options for Revising the Data Retention Directive: Current approaches to data preservation in the EU and in third countries', November 2012, 4, http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/data-retention/docs/drd_task_2_report_final_en.pdf

[81] See, for example, TIA Act s 107H (domestic preservation notices).

[82] *Telecommunications Act 1997* (Cth) s 313(7)(ca).

not require a warrant, and it is therefore relatively easy for issuing agencies to secure the continued existence of data of potential interest, with subsequent access to that data taking place if required using the relevant access regimes. In general terms, the APF supports a targeted data preservation regime as an essential mechanism for balancing the protection of privacy and the needs of law enforcement and security agencies. That said, the APF refers the committee to its 2011 submission to the inquiry of the Joint Select Committee on Cyber-Safety into the Cybercrime Legislation Amendment Bill 2011, which identified ways in which the preservation notice regime is seriously privacy-intrusive, including the over-broad scope of 'stored communications' falling within the regime and the need to limit the agencies capable of issuing preservation notices.[83]

As this submission has explained, the definition of 'stored communications' in s 5 of the TIA Act, when read together with the definition of 'communication' (which includes 'any part of a conversation or message'), may potentially be broad enough to include non-content telecommunications data. If that is the case, then issuing agencies already have the power to give preservation notices in relation to at least some non-content telecommunications data provided that the conditions for issuing the notice, including that the agency considers there are reasonable grounds for suspecting that stored communications might assist in the investigation of a 'serious contravention'.[84] As the APF pointed out in its 2011 submission to the Cyber-Safety Committee, there may be a case for distinguishing between data preservation notices relating to content and notices relating to non-content telecommunications data, which the preservation notice regime currently fails to satisfactorily do.

The APF submits that, in proposing a mandatory blanket data retention regime, the government has given insufficient consideration to the potential benefits of a targeted data preservation regime, in which relevant agencies may selectively require the preservation of telecommunications data, provided always that satisfactory procedural safeguards are met. Moreover, the APF considers that insufficient attention has been given to the potential for existing legal mechanisms to be used to require the preservation of relevant data, including (but not confined to) the preservation notice regime established under Chapter 3 of the TIA Act. In this respect, mention should also be made of long-established provisions, such as s 39 of the *Crimes Act 1914* (Cth), which make it an offence to destroy material where it is known it may be 'required in evidence in a judicial proceeding'. In any case, no consideration appears to have been given to the merits of adapting and extending a regime such as the Chapter 3 preservation notice regime, to appropriately apply to the preservation of non-content telecommunications data. This is especially startling given the likelihood that comparable jurisdictions, including EU member states such as Germany, as well as Canada, seem likely to introduce a targeted data preservation regime, in preference to an indiscriminate blanket regime. Without proper consideration of alternatives to blanket data retention, which may well be as effective as a blanket regime, it is simply impossible to claim that the case for a regime such as that proposed in the Bill has been made.

Accordingly, the APF recommends that:

- **The mandatory blanket data retention regime embodied in the Bill should be abandoned, on the basis that it is neither necessary nor proportionate, and its effectiveness is questionable, at least in the light of the high level of interference with privacy entailed by such a regime; and**
- **Consideration be given to the introduction of a more targeted and circumscribed data preservation regime, which may include a modified version of the preservation notice regime established under Chapter 3 of the TIA Act.**

[83] Australian Privacy Foundation, *Submission to Joint Select Committee on Cyber-Safety's Inquiry into the Cybercrime Legislation Amendment Bill 2011,* 26 July 2011, at http://www.privacy.org.au/Papers/index.html.
[84] TIA Act, s 107J(1)(c).

While, in principle, the APF supports a targeted data preservation regime, it is important that adequate attention be given to the formulation of appropriate limits on such a regime. Such limits should include thresholds for preservation notices, in order to ensure that agencies can only issue such notices where there is a reasonable suspicion of serious crime, terrorist activity or public corruption. Without such safeguards, a case-by-case preservation regime runs the same risks as a blanket data retention regime of becoming a form of undifferentiated mass surveillance. Moreover, while targeted data preservation regimes give the appearance of being less intrusive, it is always important to bear in mind the distinction between what carriers and ISPs may be required to do, and the data they may, as a matter of practice, decide to retain. In particular, if carriers and ISPs are issued with a high volume of data preservation notices, then they may have an economic incentive to engage in mass data retention. In this respect, there is a danger of a data preservation regime becoming a de facto form of blanket data retention. While adequate safeguards on the issuing of data preservation notices, and especially on the threshold for issuing such notices, may prevent this from occurring, this possibility serves to further focus attention on the need for adequate procedural safeguards on the access to preserved telecommunications data.

- *The APF submits that, in proposing a mandatory blanket data retention regime, the government has given insufficient consideration to the potential benefits of a targeted data preservation regime, in which relevant agencies may selectively require the preservation of telecommunications data, provided that satisfactory procedural safeguards are met. The APF therefore recommends that:*
  - ***(a) The mandatory blanket data retention regime embodied in the Bill be abandoned, on the basis that it is neither necessary nor proportionate, and its effectiveness is questionable, at least in the light of the very high level of interference with privacy entailed by such a regime; and***
  - ***(b) Consideration be given to the introduction of a more targeted and circumscribed data preservation regime, which may include a modified version of the preservation notice regime established under Chapter 3 of the TIA Act.***

ATTACHMENT

The European Experience with Data Retention

January 2015

The European Union (EU) and its constituent Member States have for some time had data retention laws.[85] Indeed, the Australian Government has looked to the European experience as a model for its own proposals, and Attorney-General Brandis has also remarked that data retention 'is very much the way in which western nations are going'.[86] However, from a privacy perspective, the European data retention regime has proved highly problematic – to the point of its invalidation – and so can hardly function as a good example for Australia to follow. Furthermore, the Data Retention Directive's invalidation poses serious questions over the viability of such laws in the EU in any future incarnations, as will be seen in more detail below.

The Data Retention Directive

The Data Retention Directive applied to the data generated by users of electronic communications services and networks, and required the operators of these services and networks to retain some types of traffic and location data on all users for a period between six months and two years.

The kind of data that should be kept included telephone numbers, account holders' and recipients' names and addresses, IP addresses, and location data, but not information about the content of the communications. Traffic data related to web browsing was also excluded. For Internet communications, the Directive only covered data relating to Internet access, email and telephony (i.e. Voice over IP services such as Skype).

The purpose of these rules was to ensure that this information is available for "the investigation, detection and prosecution of serious crime", and indeed the Directive seemed to be enacted in response to major terrorist attacks in European cities in the preceding years.

Challenges in Member States' national courts

Nevertheless, there were concerns that the DRD was too intrusive of the privacy and other fundamental rights of law-abiding Europeans. Indeed data retention rules – transpositions of the Directive into national laws - in EU Member States have been subjected to challenge in national courts even before the Court of Justice of the European Union's (CJEU's) decision from last year invalidating the Directive.[87]

In 2008, the **Bulgarian** Supreme Administrative Court annulled part of the domestic law transposing the DRD due to a lack of privacy guarantees and insufficient limitations regarding access to the data being retained, in breach of the Bulgarian Constitution.[88] The Bulgarian

[85] Namely: Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

[86] As reported in: http://www.zdnet.com/article/data-retention-is-the-way-western-nations-are-going-brandis/

[87] See: Eleni Kosta, 'The Way to Luxemburg: National Court Decisions on the Compatibility of the Data Retention Directive with the Rights to Privacy and Data Protection' (2013) 10:3 SCRIPTed 339 http://script-ed.org/?p=1163

[88] http://history.edri.org/edri-gram/number6.24/bulgarian-administrative-case-data-retention

legislature amended the transposing legislation in accordance with the Court's decision and criticism.

The following year, the **Romanian** Constitutional Court found the Romanian legislation implementing the DRD to be unconstitutional, infringing various provisions including the right to privacy, the secrecy of correspondence and freedom of expression. The Court also found that the Romanian government's attempt to justify mass mandatory data retention due to undefined 'threats to national security' was unlawful. In 2011 a new law to implement the DRD in Romania was proposed and adopted the following year, despite strong criticism. However no further challenge has been brought against that law.

In 2010, the **German** Constitutional Court considered its domestic transposition of the DRD, and found that it violated the secrecy of telecommunications as being a disproportionate interference with this principle and also had insufficient procedural safeguards. After this decision, no further legislation was introduced to implement the DRD in Germany.

In 2011, the **Cypriot** Supreme Court also considered the transposition of the DRD into the national law of Cyprus and found that the transposition violated the rights to privacy and secrecy of correspondence contained in the Cypriot Constitution due to a lack of procedural safeguards around police access to the retained data.

The Constitutional Court of the **Czech Republic** also ruled on the Czech transposition laws in 2011, and found some of the provisions to be unconstitutional. Again, the Constitutional Court was concerned about a lack of procedural safeguards, the proportionality and necessity of data retention regarding the fight against serious crime and terrorism, and the array of actors which could access the data. As a result of this decision, the implementing legislation was revised in order to take account of the Constitutional Court's criticisms, although this revision was also contested in further proceedings.

2014 CJEU decision

It is against this backdrop that privacy campaigners in Austria and NGO Digital Rights Ireland brought proceedings at the EU level against the DRD. They argued that the rules were disproportionate and unnecessary to achieve the aim of ensuring data was available for the purposes of fighting serious crime, and also argued that the rules were incompatible with the rights to privacy, data protection and free expression contained in the EU's Charter of Fundamental Rights.

On 8 April 2014 the CJEU gave its decision, that the DRD was invalid.[89] The CJEU found that, although the retention of data "genuinely satisfies an objective of general interest" (the fight against crime), the Directive's contents went beyond what was strictly necessary to achieve this goal and in doing so infringed the fundamental rights to respect for private life and to the protection of personal data. The Court was particularly concerned about the "interference with the fundamental rights of practically the entire European population", with the vast majority of those people not being "even indirectly in a situation which is liable to give rise to criminal prosecutions".

The CJEU also condemned the lack of procedural safeguards, in particular the absence of sufficient limitations to the access of this data by national authorities and their subsequent

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

use. For instance, there was no restriction on the access and use of the data to the purpose of fighting serious crime. Also of concern to the CJEU was the weakness of security measures around the data, and the fact there was no requirement to retain this data within the EU.

Aftermath

Different EU Member States have had different responses to the CJEU's decision:

- Some, such as **Finland, Luxembourg and Spain** have placed their national data retention laws under review;
- Some, such as **Austria, Slovakia and Slovenia**, have disapplied or not enforced them in whole or in part;
- Some, such as **Denmark and Sweden**, have maintained their existing data retention laws are in conformity with the CJEU's decision;
- And some - **notably the UK, and also Romania** - have proposed and enacted new laws ostensibly to address the CJEU's concerns with the Directive.

The UK's actions in the aftermath of the DRD decision in enacting – in a controversially rushed fashion - the *Data Retention and Investigatory Powers Act 2014* (UK) (DRIP Act) have been commented on by Australian politicians and the media, and seemingly taken as a sign that data retention laws are very much alive in 'similar' jurisdictions to Australia. However, the UK, for the time being, is an EU member and must comply with the CJEU's decision on data retention and other matters. The reintroduction of data retention in the UK through the DRIP Act has been done in a way which still implements blanket surveillance and does not address the CJEU's concerns about the DRD. Furthermore, it seems that not only has the DRIP Act not addressed the CJEU's decision in *Digital Rights Ireland*, but actually has increased the UK government's surveillance powers.

The DRIP Act is currently under challenge, in the form of a judicial review application in the High Court brought by NGO Liberty on behalf of two Members of the British Parliament, David Davis and Tom Watson that the DRIP Act does not sufficiently protecting individuals' privacy rights. Complaints have also been made to the European Commission that the UK, through the DRIP Act, is breaching EU law.[90]

Since the UK's conduct in passing the DRIP Act may well be found to be incompatible with the CJEU's decision and a breach of EU law, the British actions can hardly be taken by Australia as a strong example of the legitimacy of blanket data retention schemes.

Moreover, the UK is not alone in its data retention laws being under challenge: similar laws in **Belgium, Bulgaria, Ireland, the Netherlands, Poland, and Slovakia** are currently being contested. A recent Legal Opinion from the European Parliament Legal Service on the consequences of the *Digital Rights Ireland* judgment affirmed that the decision does not directly invalidate national data retention laws of EU Member States, but the decision does entail that if Member States continue to have legislation on the topic of data retention, it must comply with the EU's Charter of Fundamental Rights and conform to the CJEU's decision: in practice, though, 'Member States run an even higher risk than before of having their legislation annulled by the national courts, in a similar way to what has already happened in a number of Member States'.[91]

[90] https://www.accessnow.org/blog/2014/08/06/drip-the-commission-acknowledges-access-complaint
[91] https://s3.amazonaws.com/access.3cdn.net/27bd1765fade54d896_l2m6i61fe.pdf

Australian Privacy Foundation
Background Information

The Australian Privacy Foundation (APF) is the primary national association dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues that pose a threat to the freedom and privacy of Australians. The Foundation has led the fight to defend the right of individuals to control their personal information and to be free of excessive intrusions.

The APF's primary activity is analysis of the privacy impact of systems and proposals for new systems. It makes frequent submissions to parliamentary committees and government agencies. It publishes information on privacy laws and privacy issues. It provides continual background briefings to the media on privacy-related matters.

Where possible, the APF cooperates with and supports privacy oversight agencies, but it is entirely independent of the agencies that administer privacy legislation, and regrettably often finds it necessary to be critical of their performance.

When necessary, the APF conducts campaigns for or against specific proposals. It works with civil liberties councils, consumer organisations, professional associations and other community groups as appropriate to the circumstances. The Privacy Foundation is also an active participant in Privacy International, the world-wide privacy protection network.

The APF is open to membership by individuals and organisations who support the APF's Objects. Funding that is provided by members and donors is used to run the Foundation and to support its activities including research, campaigns and awards events.

The APF does not claim any right to formally represent the public as a whole, nor to formally represent any particular population segment, and it accordingly makes no public declarations about its membership-base. The APF's contributions to policy are based on the expertise of the members of its Board, Subcommittees and Reference Groups, and its impact reflects the quality of the evidence, analysis and arguments that its contributions contain.

The APF's Board, Subcommittees and Reference Groups comprise professionals who bring to their work deep experience in privacy, information technology and the law.

The Board is supported by Patrons, The Hon Michael Kirby and Elizabeth Evatt, and an Advisory Panel of eminent citizens, including former judges, former Ministers of the Crown, and a former Prime Minister.

The following pages provide access to information about the APF:
- Policies http://www.privacy.org.au/Papers/
- Resources http://www.privacy.org.au/Resources/
- Media http://www.privacy.org.au/Media/
- Current Board Members http://www.privacy.org.au/About/Contacts.html
- Patron and Advisory Panel http://www.privacy.org.au/About/AdvisoryPanel.html

The following pages provide outlines of several campaigns the APF has conducted:
- The Australia Card (1985-87) http://www.privacy.org.au/About/Formation.html
- Credit Reporting (1988-90) http://www.privacy.org.au/Campaigns/CreditRpting/
- The Access Card (2006-07) http://www.privacy.org.au/Campaigns/ID_cards/HSAC.html
- The Media (2007-) http://www.privacy.org.au/Campaigns/Media/