Commissioner for Privacy and Data Protection

Submission to

Parliamentary Joint Committee on Intelligence and Security

on its

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

January 2015

Commissioner for Privacy and Data Protection

The Commissioner wishes to thank Ms Emily Minter, Senior Legal Advisor and Ms Adriana Latomanski, Policy Analyst, for their assistance in preparing this submission.

Commissioner for Privacy and Data Protection
GPO Box 24014
Level 6
121 Exhibition Street
Mebourne Victoria 3001
Australia
Phone: +61 3 8684 1660
Fax: +61 3 8684 1667
Email: enquiries@cpdp.vic.gov.au
Website: www.dataprotection.vic.gov.au

Commissioner for Privacy and Data Protection

EXECUTIVE SUMMARY

One of the most troubling features of the data retention scheme is that it creates undefined and uncontrolled security vulnerabilities.

Every Australian's communications data will be collected and stored for two years. This vast reservoir of highly sensitive, distributed data will not be adequately secured because the scheme does not properly address the security issues associated with the transmission and storage of the retained data.

The Bill substantially attenuates privacy rights but does not contain the safeguards that are necessary to ensure that its interference with fundamental rights is proportionate or necessary.

These shortcomings, combined with the Bill's failure to define fundamental concepts means that it is so vague and opaque as to make it impossible to clearly determine the risks it poses or to suggest appropriate mitigation measures. It also means that there is no meaningful way to determine how much it will cost taxpayers or to measure whether or not it produces public value commensurate with its cost.

ABOUT THE COMMISSIONER FOR PRIVACY AND DATA PROTECTION

The Commissioner for Privacy and Data Protection (CPDP) was established by the *Privacy and Data Protection Act 2014* (Vic)(PDPA). The CPDP was created in order to ensure an integrated, whole of Victorian government approach to information privacy and data security.

The CPDP is responsible for:

- overseeing the collection and handling of personal information in the Victorian public sector; and
- establishing, overseeing and monitoring a protective data security regime for the Victorian public sector.

Victoria is the only Australian jurisdiction to have established a legislatively backed regulatory framework that extends security obligations beyond personal information to all data held by the public sector, mandates the development of explicit protective data security standards and requires an independent statutory regulator to oversee and monitor them.

BACKGROUND

The Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (the Bill) seeks to amend the Telecommunications (Interception and Access) Act 1979 (TIA Act) to introduce a mandatory data retention scheme. In November 2014 both the Parliamentary Joint Committee on Human Rights (PJCHR) and the Senate Standing Committee for the Scrutiny of Bills commented on the

Bill.[1] The Senate Standing Committee for Legal and Constitutional Affairs is currently also conducting an inquiry. Its report is due on 12 February 2015.

This submission is made in response to an invitation by the Parliamentary Joint Committee on Intelligence and Security.

THE KEY FEATURES OF THE DATA RETENTION SCHEME

The Bill requires communications service providers to retain data about every Australian internet and telephone user for two years following the creation of the data. The Bill does not define the data that must be retained.[2]

The categories of information to be retained must relate to one of the following:

- the identity of the subscriber to a communications service
- the source of the communication
- the destination of the communication
- the date, time and duration of the communication
- the type of communication
- the location of the equipment used in the communication.[3]

The scheme is modelled on The European Union Data Retention Directive 2006/24/EC which was struck down by the Court of Justice of the European Union on 8 April 2014 for violating fundamental rights.[4] These are the same fundamental rights to which Australia is bound under international law.

The Attorney General released a draft dataset in October 2014.[5] This extrapolates on the six categories set out in the Bill and states that 'regulations will provide further details about what is to be collected and greater technical specificity about each of these categories'.[6]

Data that is said not to be included in the scheme includes individuals' web browsing history, the subject of an email or the content of an email. Given that there is significant uncertainty about the categories of data that will be covered by the scheme these exclusions are not adequately defined. If the retained data includes the source of a communication and the equipment used to communicate it as well as the destination of the communication, this would appear to include an individual's communication with a web site.

---

[1] See PJCHR *Fifteenth Report of the 44th Parliament,* November 2014 http://www.aph.gov.au/~/media/Committees/Senate/committee/humanrights_ctte/reports/2014/15_44/15th%20Report.pdf; Senate Standing Committee for the Scrutiny of Bills *Alert Digest No. 16 of 2014,* November 2014 http://www.aph.gov.au/~/media/Committees/Senate/committee/scrutiny/alerts/2014/pdf/d16.pdf

[2] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, 187A(1)

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

[4] See http://curia.europa.eu/juris/documents.jsf?num=C-293/12

[5] Australian Government *Data Retention Bill – Proposed data set* October 31 available at http://www.ag.gov.au/NationalSecurity/DataRetention/Documents/ProposeddatasetOctober2014.pdf

6 Australian Government *Data Retention Bill – Proposed data set* October 31 available at http://www.ag.gov.au/NationalSecurity/DataRetention/Documents/ProposeddatasetOctober2014.pdf

The Bill's Explanatory Memorandum justifies the dataset being amended by regulation on the basis that it will ensure that data retention obligations remain "sufficiently flexible to adapt to rapid and significant future changes in communications technology."[7]

The Bill also allows the Minister to declare additional agencies to be added to the list of 'criminal law-enforcement agencies' specified,[8] thereby enabling agencies beyond those listed in the Bill to access data under the legislation. Similarly, the Bill empowers the Minister to expand the meaning of 'enforcement agency'.[9]

The Bill's statement of compatibility disingenuously states that the "ministerial declaration scheme reinforces the right to privacy in that it ensures that enforcement agency access to telecommunications data is strictly circumscribed and subject to ministerial scrutiny".[10]

The categories of services for which data must be retained under the scheme can also be amended by Ministerial declaration.[11] This has resulted in confusion about the breadth of data that will need to be retained. For example, service providers have queried whether they will need to store data for services including tele-health, lifelogging, IP TV and other internet-connect devices.[12] As with the types of data, the categories may be amended at any time without warning or consultation.

The Explanatory Memorandum states that this is to "ensure the data retention regime is able to remain up-to-date with rapid changes to communications technologies, business practices, and law enforcement and national security threat environments."[13]

OUR ANALYTIC APPROACH

Privacy is a fundamental, but not an absolute, right. In certain circumstances it is appropriate that it yields to other countervailing rights in the public interest. National security, the investigation and prevention of serious crime and the protection of other fundamental rights – such as the right to life - constitute recognised exceptions to the right to privacy.

The most common analytic approach used to undertake the necessary balancing exercise between privacy and these other interests is to apply a legal test to determine whether the abrogation of privacy rights for law enforcement or national security purposes is **necessary and proportionate.**

The thirteen principles that should be taken into account in applying the necessary and proportionate test are:

- Legality

[7] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 Explanatory Memorandum, 36.
[8] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, 110A(3).
[9] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, 176A(3).
[10] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, Statement of Compatibility, 21.
[11] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, 187A(3)(b)(iii).
[12] The Age *Australian telcos in race against time to access metadata retention costs* 31 December 2014 http://www.theage.com.au/digital-life/consumer-security/australian-telcos-in-race-against-time-to-estimate-metadata-retention-costs-20141231-12fv57.html
[13] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 Explanatory Memorandum, 43.

- Legitimate aim
- Necessity
- Adequacy
- Proportionality
- Oversight by Competent Judicial Authorities
- Procedural Fairness
- User Notification
- Transparency
- Public Oversight
- Integrity of Communications and Systems
- Safeguards on International Cooperation
- Safeguards against Illegitimate Access and the Right to an Effective Remedy.

A detailed explanation of these principles is set out in Attachment 1.

Using this analytic framework, our submission is that the Bill, in its current form, fails the necessary and proportionate test on a number of grounds. Our submission also highlights other concerns about the Bill. In summary we argue that the Bill:

1. lacks legislative certainty
2. interferes with information privacy and other fundamental rights in a manner that is neither proportionate nor necessary
3. gives rise to security vulnerabilities that are undefined and uncontrolled
4. will not effectively achieve its public policy objectives
5. fails to establish adequate governance or oversight mechanisms:
6. will have significant and unjustified costs.

1. LACK OF LEGISLATIVE CERTAINTY

Central to the Bill's difficulties is that it does not define the most important aspects of the data retention scheme. Service providers who operate a relevant service must keep data "of a kind prescribed by the regulations."[14] The Attorney-General is empowered to declare whether an authority or body is entitled to have access to retained data.[15] The type of services to which the scheme will apply includes a service for carrying communications operated by a carrier or an internet service provider "or of a kind prescribed by the regulations."[16]

The core provisions of the Bill are either missing or can be amended by the Executive without proper Parliamentary oversight or consent, secluded from public scrutiny. Dealing with significant matters in

[14] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, s 187A(1)(a).
[15] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, 110A(3).
[16] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, 187A(3).

primary legislation supports the democratic process by ensuring that matters are subject to public scrutiny and are debated thoroughly and transparently. It also ensures that matters are subject to political checks and balances, including consideration of compatibility with regulatory and other requirements. We support the Senate Standing Committee for the Scrutiny of Bills which has stated that:

> *[I]t seems appropriate for Parliament (not the executive) to take responsibility for ensuring that the scheme is adequately responsive to technological change in the telecommunications industry. Although the committee accepts that regulation-making powers are in some cases justified by the necessity to build in scope for flexible regulatory responses to changing circumstances, whether this scheme – which is highly intrusive of individual privacy – should be applied in a new technological context is a matter which will raise significant questions of policy. The committee generally expects that significant matters will be included in primary legislation – they are not appropriately delegated by the Parliament to the executive government.*[17]

CATEGORIES OF SERVICES FOR WHICH DATA MUST BE MAINTAINED

The categories of services for which data must be maintained should be specified in legislation for the same reasons that types of data should be – primarily to ensure certainty, transparency, to allow for due process and political scrutiny, and to allow for the creation of appropriate governance arrangements, including privacy and protective data security protections.

LAW ENFORCEMENT AGENCIES TO HAVE ACCESS TO THE DATA

We consider that the types of law enforcement agencies to have access to the data should be dealt with in primary, rather than by delegated legislation to ensure that parliamentary debate and public scrutiny occurs.

We recommend that the legislation provide a clearly defined list of agencies that are able to request access to data. Any modification to this list should be subject to legislative amendment only.

The Bill should be amended to include clearly defined objective thresholds for access to retained data by criminal law enforcement agencies. These thresholds should be set taking into account the public interest, including consideration of the principles of proportionality, necessity, effectiveness, and transparency. Access should only be available in relation to serious offences, for example, offences that attract significant periods of imprisonment. The PJCHR recommendation to limit disclosure authorisation for existing data to where it is necessary for the investigation of specified serious crimes, or categories of serious crimes is supported. As the Bill provides insufficient safeguards to protect against data that is being disclosed for an authorised purpose to be used for unrelated purposes, we also support the PJHCR recommendation that the Bill be amended to restrict access to retained data on defined objective grounds.

[17] Senate Standing Committee for the Scrutiny of Bills Alert Digest No. 16 of 2014, 3.

Commissioner for Privacy and Data Protection

2. INTERFERENCE WITH PRIVACY

There is no doubt that the data retention scheme is intrusive. The retained data will reveal patterns of communications that will enable those who have access to it to investigate and understand the private lives of all Australians, such as the habits of everyday life, places of residence, minute by minute movements, activities undertaken, social, professional and commercial arrangements, and relationships and social environments frequented.[18] It will cover personal and business communications, including those of Ministers, members of parliament and officials, senior officials such as the Director General of ASIO and the Commissioners of the federal and state police forces.[19]

By requiring retention of such sweeping categories of data, and by allowing potentially numerous agencies to have access, the scheme significantly interferes with the fundamental right to privacy in a manner that is not proportionate to the objectives of the Bill.

As noted earlier, the Bill is largely modelled on the now invalid European Union Data Retention Directive. In ruling on the Directive, the EU Court of Justice stated:

> *Although the retention of data required by the directive may be considered to be appropriate for attaining the objective pursued by it, the wide ranging and particularly serious interference of the directive with the fundamental rights at issue is not sufficiently circumscribed to ensure that that interference is actually limited to what is strictly necessary.*[20]

This analysis applies equally to the Bill. The public interest in maintaining an extremely flexible data retention scheme does not outweigh the public interest in ensuring:

- adequate privacy and security protections are maintained
- a certain and transparent scheme that is subject to public scrutiny.

CONTENT VS METADATA

The content, or substance, of a communication is excluded from the scheme under the Bill.[21] This is in response to a misapprehension that by excluding 'content' from the operation of the scheme, individuals' privacy will remain safeguarded. This view misrepresents the importance of metadata as a valuable intelligence asset. It is widely recognised that metadata can reveal personal information about individuals. The EU Court of Justice has found that metadata "... taken as a whole, may provide very precise information on the private lives of the persons whose data are retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, activities carried out, social relationships and social environments frequented."[22]It may reveal with whom a person is in

[18] Court of Justice of the European Union Press Release No 54/14 *The Court of Justice declares the Data Retention Directive to be invalid* 8 April 2014.
[19] Unless, of course, the Communications Access Co-ordinator gives an exemption. See s 187K
[20] See Court of Justice of the European Union Press Release No 54/14 *The Court of Justice declares the Data Retention Directive to be invalid* 8 April 2014.
[21] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, 187A(4).
[22] Court of Justice of the European Union Press Release No 54/14 *The Court of Justice declares the Data Retention Directive to be invalid* 8 April 2014.

contact, how often and where. It will reveal other aspects of a person's life, including sensitive information such as their political opinions, sexual habits, religious beliefs and health information.[23]

iiNet has stated that "metadata reveals even more about an individual than the content itself."[24] More alarmingly, former director of the CIA and NSA General Michael Hayden publically stated "we kill people based on metadata." He has also stated that metadata without content is capable of telling the government "everything" about an individual.[25]

Finally, Caspar Bowden, a specialist in EU Data Protection and European and US surveillance law has argued:

> *[R]etention is like having a CCTV camera installed "inside your head" that is, that it invades the subjective interior space of our thoughts and intentions, because these can be inferred from Internet and other metadata. It is incompatible with human rights, in any democracy, to indiscriminately and continuously collect communications data or metadata on the entire population. The essence of the freedom conferred by the right to private life is that official infringements must be justified and exceptional.*[26]

We endorse these views: the mass surveillance framework that the Bill seeks to establish by means of the wide scale collection of metadata is an unjustified infringement of fundamental rights.

3. SECURITY RISKS

The data retention scheme will require communications service providers to retain vast quantities of information. Some will be highly sensitive. Some will be security classified, such as government communications. The Bill is largely silent on how this information will be secured. Such information, if compromised, has the potential to pose a very real threat to Australia's national security and the lives of individual Australians.

The Attorney-General's Department suggests that the retained data will be "subject to the same strict controls that apply today"[27]and that the Privacy Commissioner "will continue to assess industry's compliance with the Australian Privacy Principles as well as monitoring industry's non-disclosure obligations under the Telecommunications Act."[28]

The security regime overseen by the Australian Privacy Commissioner is not fit for purpose. The only security obligation created by the *Privacy Act 1988* is Australian Privacy Principle 11 (APP 11), which states that:

> *If an APP entity holds personal information, the entity must take such steps as are reasonable in*

[23] See, eg, Solove D, et al *Privacy, Information, and Technology* (2006) Aspen Publishers, 101
[24] iiNet *Submission to the Legal and Constitutional Affairs References Committee, Comprehensive Revision of the Telecommunications (Interception and Access) Act 1979,* July 2014, 3.
[25] Michael Hayden speaking at the Johns Hopkins Foreign Affairs Symposium, 1 April 2014 http://web1.johnshopkins.edu/fas/
[26] Privacy and Security Inquiry: Submission to the Intelligence and Security Committee of Parliament, Caspar Bowden, 7 February 2014 http://blog.privacystrategy.eu/public/published/Submission_ISC_7.2.2014_-_Caspar_Bowden.pdf
[27] See http://www.ag.gov.au/dataretention

the circumstances to protect the information:
(a) from misuse, interference and loss; and
(b) from unauthorised access, modification or disclosure.

Although efforts have been made by the Office of the Australian Information Commissioner (OAIC) to clarify the meaning of APP 11, it has conceded that the meaning of 'reasonable steps' depends on the circumstances.[29] Its guidelines on APP 11 are at such a high level of abstraction that they do not provide concrete security guidance. Putting aside the fact that APP 11 does not apply to 90% of the private sector because of the small business exception, how is the Privacy Commissioner to determine the 'steps as are reasonable' to provide security for the data retention scheme? How do communications providers determine what is reasonable in the circumstances? How will outsourcing be dealt with?

The Bill does not prevent retained data from being transmitted to, and stored in, offshore cloud computing services that are under the control of foreign corporations and foreign governments. It does not exclude retained data being stored in cloud computing services that are physically located within Australia but which are owned by foreign entities that may be subject to extraterritorial legal obligations that subject the retained data to the laws of foreign countries.

The sheer amount of data to be retained in the hands of commercial entities means that the security risks applicable to the retained data in the hands of third parties are magnitudes greater than are currently applicable. The Privacy Commissioner does not have direct jurisdiction over the contracted service providers (CSPs) to which telecommunications service providers may share data – any obligations on CSPs with respect to the data they may handle as a result of the scheme will be by way of private contract with the primary service provider.

In the meantime, cyber security threats are escalating. The serious threat to Australia's national security posed by cyber attack has been widely acknowledged.

The *ASIO Report to Parliament 2013-2014* states:

> *In 2013–14, the range, scale and sophistication of state actors engaged in hostile cyber espionage activity against the Australian Government and private sector systems continued to increase. The potential access to large aggregations of valuable information, the plausible deniability it offers to state actors and the often difficult-to-detect nature of the activity ensure cyber espionage remains— and will continue to be—a widely used and increasingly sophisticated espionage vector.*[30]

The EU Court of Justice also noted the threat to security posed by the EU Data Retention Directive. It found that "the directive does not provide for sufficient safeguards to ensure effective protection of the data against the risk of abuse and against any unlawful access and use of the data."[31]

Adding to security concerns is the fact that it is commercial service providers (not government agencies)

---

[29] See http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/chapter-11-app-11-security-of-personal-information
[30] *ASIO Report to Parliament 2013-2014,* 6 http://www.asio.gov.au/img/files/2013-14-Report_to_Parliament.pdf
31 Court of Justice of the European Union Press Release No 54/14 *The Court of Justice declares the Data Retention Directive to be invalid* 8 April 2014.

that will be required to retain the data. These companies will be responsible for ensuring that security controls are in place to ensure the confidentiality, integrity and availability of the retained data. Commercial entities are not required to adhere to the same level of data security standards as government agencies, and have considerable inconsistencies in their approach to protective data security. Breaches to the security of large, well resourced private sector organisations are commonplace but many remain unknown because of commercial secrecy and the fact that Australia does not have a data security breach framework in place.

The most sophisticated businesses are not immune to cyber vandalism. A recent US-based study found that the organisations they canvassed were on average victims of 1.6 successful cyber attacks every week.[32] Given the 'honey-pot' of data to be retained by service providers under the scheme it is not unreasonable to assume they will be the targets of more than their share of attacks.

Australian government agencies are required to adhere to protective data security standards under the Protective Security Policy Framework. Similar schemes exist for commercial businesses that have access to government data, for example the Australian Defence Industry Security Program and, in the United States, the National Industrial Security Program. These schemes require, at the outset, agencies and businesses to conduct a thorough risk assessment of the threats and vulnerabilities associated with their information retention and handling regimes.

The types of issues that require consideration in the Bill include obligations on service providers to have in place:

- internal security management frameworks, including proper policies and procedures
- strategies to identify and mitigate risks
- recruitment and access controls, and monitoring and training of staff
- security incident management systems
- reporting requirements in relation to security of data
- procedures in relation to other bodies that may access the data, such as contracted service providers
- procedures to ensure that security measures are clearly integrated into, and implemented through all stages of the information lifecycle
- procedures to ensure the physical security of the data in relation to its storage, transfer and disposal.

On this last point we note the Bill does not provide for the irreversible destruction of the data at the end of the retention period. This was also one of the failings of the EU Data Retention Directive noted by the EU Court of Justice.[33]

4. INEFFECTIVE PUBLIC POLICY INITIATIVE

The Explanatory Memorandum suggests the scheme is proposed primarily as a means to increase the

[32] http://www.theage.com.au/it-pro/security-it/counting-the-real-cost-of-cyber-attacks-20141216-128ehk.html
[33] Court of Justice of the European Union Press Release No 54/14 *The Court of Justice declares the Data Retention Directive to be invalid* 8 April 2014.

ability of the TIA Act to assist in "investigating, prosecuting and preventing serious criminal offences (including murder, sexual assault, kidnapping, drug trafficking, money laundering and fraud) and activities that threaten national security".[34]

We question the necessity of such wide-scale surveillance to detect a relatively confined cohort of terrorists and criminals given law enforcement agencies already have the power to undertake targeted requests for data retention, for example by using an ongoing preservation notice under the TIA Act.

Concerns of this nature were raised by the then Shadow Communications Minister in response to the previous government's 2012 data retention proposal:

> *Why do we imagine that the criminals of the greatest concern to our security agencies will not be able to use any of numerous available means to anonymise their communications or indeed choose new services that are not captured by legislated data retention rules?*[35]

This view has been supported by industry representatives who have pointed out that the people who are of interest to law enforcement agencies will most likely be the people who have the motivation, skill, resources and patience to avoid the data retention scheme.[36]

Further, there has been research that suggests that the application of advanced data analytics or other forms of data mining is not well suited to identifying and preventing terrorism or organised crime.[37] The National Research Council noted, as one of its conclusions to its report *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment*:

> *The utility of pattern-based data mining is found primarily if not exclusively in its role in helping humans make better decisions about how to deploy scarce investigative resources, and action (such as arrest, search, denial of rights) should never be taken solely on the basis of a data mining result. Automated terrorist identification through data mining (or any other known methodology) is neither feasible as an objective nor desirable as a goal of technology development efforts.* [38]

The perpetrators of recent terrorist attacks in France, Sydney and at the Boston marathon were individuals who were well known to security and law enforcement agencies. Each of the countries affected has data retention laws. Experience suggests that security and law enforcement agencies do not need ever increasing amounts of raw data: what *is* needed is more effective analysis and interpretation of the available data and more nuanced and sophisticated approaches to identifying and mitigating risk.

In addition, an unintended consequence of the Bill will be its 'chilling effect'. It will encourage those who seek to evade it to undertake their activities offline. The PJCHR noted that the proposed data retention

---

[34] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 Explanatory Memorandum, 36.
[35] Malcolm Turnbull (2012) *Free at Last! Or freedom lost? Liberty in the Digital Age: 2012 Alfred Deakin Lecture.*
[36] See, eg, Jon Lawrence, Executive Officer, Electronic Frontiers Australia, comments to the Legal and Constitutional Affairs References Committee, Comprehensive revision of the Telecommunications (Interception and Access) Act 1979, 29 July 2014.
[37] Jeff Jonas and Jim Harper, 'Effective Counterterrorism and the Limited Role of Predictive Data Mining', *Policy Analysis* No. 584, December 11 2006, available at http://www.cato.org/pubs/pas/pa584.pdf
[38] United States National Research Council, Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals, *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment*, 78, available at http://www.nap.edu/catalog/12452.html

scheme could lead people to 'self-censor' the views they would normally express via telecommunications services.[39]It will also encourage those who pose a serious risk to the community's safety and security to develop and deploy increasingly sophisticated techniques to evade detection.

5. LACK OF APPROPRIATE OVERSIGHT, ACCOUNTABILITY AND TRANSPARENCY

While existing and proposed amendments to the TIA Act allow for oversight of the data retention scheme by the Commonwealth Ombudsman, this only applies to the use and handling of the data by law enforcement agencies, not the service providers required to retain the data. The Bill does not describe the security standards the Ombudsman will oversee.

Some service providers will be subject to the obligations set out in existing privacy law, and the oversight of the Australian Privacy Commissioner but others may not be covered. For the reasons set out earlier, the security requirements established under the *Privacy Act 1988* are not appropriate.

Further, the majority of investigations conducted by the Commissioner are initiated by a complaint. While the Commissioner also has own-motion investigation powers, these are used sparingly. For example, six matters were assessed for investigation in 2013-14.[40] This level of oversight is not adequate to cover the scale of the data retention scheme.

6. COST

The cost of implementing the data retention scheme cannot be accurately assessed. Some industry estimates have suggested costs may range between $100 million and $500 million[41].

We note a cost estimate is currently being conducted by the Attorney-General's Department but, given that key features of the Bill are not defined and the fact that security measures have not been adequately dealt with, it is unlikely that costs will be anything other than guesswork for the foreseeable future.

Service providers have raised concerns about footing the bill for the scheme, warning that the costs will be passed on to consumers[42]. In 2014 the Minister for Communications stated that the government would pay a "substantial share of the costs of the scheme."[43] This means that taxpayers will fund their own surveillance.

---

[39] See PJCHR *Fifteenth Report of the 44th Parliament,* November 2014.
[40] Office of the Australian Information Commissioner *Annual Report 2013-14,* 92.
[41] See eg John Stanton, CEO, Communications Alliance Ltd, comments to the Legal and Constitutional Affairs References Committee, Comprehensive revision of the Telecommunications (Interception and Access) Act 1979, 29 July 2014.
[42] Internet service provider iiNet has previously estimated customers could pay $100 extra a year unless taxpayers fund the scheme
[43] SMH, *Telcos relieved at limited scope and cost of data retention law* 30 October 2014 http://www.smh.com.au/federal-politics/political-news/telcos-relieved-at-limited-scope-and-cost-of-data-retention-law-20141030-11ehbb.html

Commissioner for Privacy and Data Protection

ATTACHMENT ONE - THE 13 PRINCIPLES FOR THE NECESSARY AND PROPORTIONATE TEST[44]

LEGALITY

Any limitation to human rights must be prescribed by law. The State must not adopt or implement a measure that interferes with these rights in the absence of an existing publicly available legislative act, which meets a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee its application. Given the rate of technological changes, laws that limit human rights should be subject to periodic review by means of a participatory legislative or regulatory process.

LEGITIMATE AIM

Laws should only permit Communications Surveillance by specified State authorities to achieve a legitimate aim that corresponds to a predominantly important legal interest that is necessary in a democratic society. Any measure must not be applied in a manner that discriminates on the basis of race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

NECESSITY

Surveillance laws, regulations, activities, powers, or authorities must be limited to those which are strictly and demonstrably necessary to achieve a legitimate aim. Communications Surveillance must only be conducted when it is the only means of achieving a legitimate aim, or, when there are multiple means, it is the means least likely to infringe upon human rights. The onus of establishing this justification is always on the State.

ADEQUACY

Any instance of Communications Surveillance authorised by law must be appropriate to fulfil the specific Legitimate Aim identified.

PROPORTIONALITY

Communications surveillance should be regarded as a highly intrusive act that interferes with human rights threatening the foundations of a democratic society. Decisions about Communications Surveillance must consider the sensitivity of the information accessed and the severity of the infringement on human rights and other competing interests.

This requires a State, at a minimum, to establish the following to a Competent Judicial Authority, prior to conducting Communications Surveillance for the purposes of enforcing law, protecting national security, or gathering intelligence:

- there is a high degree of probability that a serious crime or specific threat to a Legitimate Aim has been or will be carried out
- there is a high degree of probability that evidence of relevant and material to such a serious

[44] International Principles on the Application of Human Rights to Communications Surveillance, https://necessaryandproportionate.org

crime or specific threat to a Legitimate Aim would be obtained by accessing the Protected Information sought
- other less invasive techniques have been exhausted or would be futile, such that the techniques used is the least invasive option
- information accessed will be confined to that which is relevant and material to the serious crime or specific threat to a Legitimate Aim alleged
- any excess information collected will not be retained, but instead will be promptly destroyed or returned
- information will be accessed only by the specified authority and used only for the purpose and duration for which authorisation was given
- that the surveillance activities requested and techniques proposed do not undermine the essence of the right to privacy or of fundamental freedoms.

COMPETENT JUDICIAL AUTHORITY

Determinations related to Communications Surveillance must be made by a competent judicial authority that is impartial and independent. The authority must be:

- separate and independent from the authorities conducting Communications Surveillance
- conversant in issues related to and competent to make judicial decisions about the legality of Communications Surveillance, the technologies used and human rights
- have adequate resources in exercising the functions assigned to them.

DUE PROCESS

Due process requires that states respect and guarantee individuals' human rights by ensuring that lawful procedures that govern any interference with human rights are properly enumerated in law, consistently practiced, and available to the general public. Specifically, in the determination on his or her human rights, everyone is entitled to a fair and public hearing within a reasonable time by an independent, competent and impartial tribunal established by law except in cases of emergency when there is imminent risk of danger to human life. In such instances, retroactive authorisation must be sought within a reasonably practicable time period. Mere risk of flight or destruction of evidence shall never be considered as sufficient to justify retroactive authorisation.

USER NOTIFICATION

Those whose communications are being surveilled should be notified of a decision authorising Communications Surveillance with enough time and information to enable them to challenge the decision or seek other remedies and should have access to the materials presented in support of the application for authorisation. Delay in notification is only justified in the following circumstance:

- notification would seriously jeopardize the purpose for which the Communications Surveillance is authorised, or there is an imminent risk of danger to human life
- authorisation to delay notification is granted by a Competent Judicial Authority
- the User affected is notified as soon as the risk is lifted as determined by a Competent Judicial Authority.

The obligation to give notice rests with the State, but communications service providers should be free to notify individuals of the Communications Surveillance, voluntarily or upon request.

TRANSPARENCY

States should be transparent about the use and scope of communications surveillance laws, regulations, activities, powers, or authorities. They should publish, at a minimum, aggregate information on the specific number of requests approved and rejected, a disaggregation of the requests by service provider and by investigation authority, type, and purpose, and the specific number of individuals affected by each. States should provide individuals with sufficient information to enable them to fully comprehend the scope, nature, and application of the laws permitting communications surveillance. States should not interfere with service providers in their efforts to publish the procedures they apply when assessing and complying with state requests for communications surveillance, adhere to those procedures, and publish records of state requests for communications surveillance.

PUBLIC OVERSIGHT

States should establish independent oversight mechanisms to ensure transparency and accountability of communications surveillance. Oversight mechanisms should have the authority:

- to access all potentially relevant information about state actions, including, where appropriate, access to secret or classified information
- to assess whether the state is making legitimate use of its lawful capabilities
- to evaluate whether the state has been comprehensively and accurately publishing information about the use and scope of communications surveillance techniques and powers in accordance with its transparency obligations
- to publish periodic reports and other information relevant to communications surveillance
- to make public determinations as to the lawfulness of those actions, including the extent to which they comply with these principles.

Independent oversight mechanisms should be established in addition to any oversight already provided through another branch of government.

INTEGRITY OF COMMUNICATIONS AND SYSTEMS

In order to ensure the integrity, security and privacy of communications systems, and in recognition of the fact that compromising security for state purposes almost always compromises security more generally, states should not compel service providers or hardware or software vendors to build surveillance or monitoring capability into their systems, or to collect or retain particular information purely for state communications surveillance purposes. *A priori* data retention or collection should never be required of service providers. Individuals have the right to express themselves anonymously; states should therefore refrain from compelling the identification of users.

Commissioner for Privacy and Data Protection

SAFEGUARDS FOR INTERNATIONAL COOPERATION

In response to changes in the flows of information, and in communications technologies and services, states may need to seek assistance from foreign-service providers and states. Accordingly, the mutual legal assistance treaties and other agreements entered into by states should ensure that, where the laws of more than one state could apply to communications surveillance, the available standard with the higher level of protection for individuals is applied. Where states seek assistance for law enforcement purposes, the principle of dual criminality should be applied. States may not use mutual legal assistance processes and foreign requests for protected information to circumvent domestic legal restrictions on communications surveillance. Mutual legal assistance processes and other agreements should be clearly documented, publicly available, and subject to guarantees of procedural fairness.

SAFEGUARDS AGAINST ILLEGITIMATE ACCESS AND RIGHT TO EFFECTIVE REMEDY

States should enact legislation criminalising illegal communications surveillance by public or private actors. The law should provide sufficient and significant civil and criminal penalties, protections for whistle blowers, and avenues for redress by those affected. Laws should stipulate that any information obtained in a manner that is inconsistent with these principles is inadmissible as evidence or otherwise not considered in any proceeding, as is any evidence derivative of such information. States should also enact laws providing that, after material obtained through communications surveillance has been used for the purpose for which information was given, the material must not be retained, but instead be destroyed or returned to those affected.