19 January 2015

Mr James Nelson
Inquiry Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600

Dear Mr Nelson

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

The Internet Society of Australia appreciates the opportunity to make a submission to the Parliamentary Joint Committee on Intelligence and Security in respect of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014.

The Society supports the Government's desire to ensure national security. However, based on an extensive review of the proposed legislation we have formed the view that it is deeply flawed and unlikely to achieve the Government's stated objectives.

We are the Australian chapter of the worldwide Internet Society. Our mission is to promote Internet developments for the benefit of the whole community, including business, educational, professional and private Internet users. Our directors and members hold significant roles in Internet-related organisations and enable the Society to provide high level policy and technical information to Internet user groups, governments and regulatory authorities.

Globally, the Internet Society coordinates Internet policy development and technical standards. This includes advising the United Nations and international Internet management organisations such as the Internet Corporation for Assigned Names and Numbers (ICANN) and the five Regional Registries. The Internet Society is responsible for the Internet Engineering Task Force.

On behalf of our board of directors and our members, and in furtherance of our submission, I would like to offer the technical and professional resources of the Internet Society in order to assist the Committee in its deliberations over this important legislation. Please contact me should the Committee wish to avail itself of the opportunity to meet with us to discuss the issues raised in our submission.

The Society will also be offering its technical and professional advice and assistance to the Government.

Yours sincerely

LAURIE PATTON
Chief Executive Officer

# Submission to the Joint Parliamentary Committee on Intelligence and Security inquiry into the *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*.

## Introduction

The Internet Society of Australia (the Society) believes that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (the Bill) is deeply flawed and will not achieve the Government's stated aims.

It does not reflect the complexity and diversity of today's communications. Moreover, it will not cover some of the Internet-based services most widely used by many Australians and will thus provide significant 'loop holes' capable of exploitation.

It will add significant costs to service providers – which will flow on to consumers – and will seriously hamper competition in the sector by raising barriers to entry for new, smaller entrants.

It will create disincentives for Australians to use Australian-based services, with clear impacts on the growth of our digital services economy.

The Bill also represents a challenge to privacy protections with the potentially for a loss of the confidence Australians have in their Internet use.

The Society's detailed concerns and recommendations are outlined below.

## Recommendations

*1.1.1 Clause 187A(2)(a) be amended to include a detailed and complete definition of the data to be retained, such that each characteristic is fully and accurately described, including for technical clarity.*

*1.1.2 Clause 187A(2) be amended such that the requirement that the definition of the data to be retained must directly relate to those characteristics should apply specifically to both the 'information' and 'documents containing information of that kind'.*

*1.2.1 Amend the Bill to require that access to data under Part 5-1A Data Retention only be granted on the ground of a reasonable suspicion that a 'serious offence' has been, is being or will be, committed.*

*1.3.1 Amend the Bill to remove the power of the Attorney-General to expand the Bill's existing list of 'enforcement agencies' and 'criminal law-enforcement agencies'. Alternatively, if recommendations are adopted to limit the grounds on which access is given, confine the declaration power of the Attorney-General to those bodies or agencies that are involved in the prevention and/or detection of a 'serious offence' as defined in the Telecommunications (Interception and Access) Act 1979.*

*2.0.1 The Government should meet with all relevant stakeholders to clarify the data that security and law enforcement agencies need to access for the prevention and/or investigation of criminal activity, and to develop and include appropriate terminology that can be incorporated into this legislation in order to make the legislation clear and unambiguous. This recommendation should be considered as a precursor to the recommendation on clarification of data to be retained, and for absolute clarity, 'relevant stakeholders' should be taken to include representatives of each of the following:*

- *Government*
- *Law enforcement and Security agencies*
- *Industry (both large and small providers, in addition to industry associations)*
- *Civil Society, including groups representing consumers, the Internet user community and privacy-focused groups*

*3.4.1 Amend Clause 187A(3) of the Bill to apply to all carriers, and carriage service providers that provide carriage services to the public.*

*4.2.1 Government assistance should be made available for ISPs who would otherwise not retain the required data and do not have the financial resources to develop systems that would retain the required data.*

## Detailed Discussion of The Society's Concerns

### *1. Impact on Privacy Protections*

The *Telecommunications (Interception and Access) Act 1979 (TIAA)* now strikes a balance between protections for Australians' privacy and the legitimate needs of law enforcement and security agencies to access data about communications used by Australians. These proposed amendments, however, give the Attorney-General power to expand the types of data collected, and the agencies that collect the data without the full Parliamentary scrutiny that should be mandated for any such expansion. Further, unlike other parts of the TIAA, the Bill does not limit the circumstances under which access will be permitted to the apprehension or investigation of criminal activity. The Bill therefore significantly shifts the balance away from the protection of Australians' privacy and towards an expanded ability of law enforcement and intelligence agencies to access personal information of Australians.

In commenting on the concept of a mandatory data retention scheme, the Parliamentary Joint Committee on Human Rights (PJCHR) from the previous parliament explained that communications data 'can reveal quite personal information about an individual, even without the content of the data being made available' and noted that 'the proposed scheme clearly limits the right to privacy.[1] The Society shares the Committee's concern over the potential challenges to rights to privacy posed by any mandatory data retention scheme, and shares the Committee's conclusion that:

> *… the [mandatory data retention] scheme must be sufficiently circumscribed to ensure that limitations on the right to privacy are proportionate (that is, are only as extensive as is strictly necessary).*[2]

There are three areas in the Bill that are drafted very broadly and which should be redrafted to strike a more appropriate balance between privacy protections for citizen and the legitimate needs of law enforcement and security agencies to access data. These are:

- the definition of the data to be retained;
- the grounds upon which access to data will be granted; and,
- the agencies and organisations that will have access to the data.

#### 1.1. Definition of Data to be Retained

The Bill, as currently drafted, does not provide detailed definitions of the data to be retained. Instead, Clause 187A(2) lists the 'characteristics' to which such information must relate. It will be left to regulations under Clause 187A(1) to set out the information (or documents containing such information) to be retained.

---

[1] Parliamentary Joint Committee on Human Rights (PJCHR), *Examination of legislation in accordance with the Human Rights (Parliamentary Scrutiny) Act 2011: Fifteenth Report of 44th Parliament*, p. 13.

[2] *Ibid*.

While the regulations must relate to the listed 'characteristics', because the 'characteristics' are broadly drawn, there is scope for the regulations to allow for very wide definitions of data to be adopted. The Society believes, therefore, that excluding detailed definitions of the data to be retained from the legislation undermines the ability of the Parliament to perform proper scrutiny and oversight of this Bill's data retention requirements.

There is a real risk that in attempting to comply with the vague descriptions of information required to be retained service providers are likely to retain more data than is required to assist law enforcement investigating serious crime, thus depriving ordinary citizens of their legitimate rights to enjoy private communications without excessive details of their private lives being at risk of misuse or unauthorised disclosure

Also while it may be simply a drafting error, the current wording of these clauses is such that the requirement that regulations relate to the 'characteristics' applies to 'information' but not to 'documents containing such information'.

**Recommendations**

*1.1.1 Clause 187A(2)(a) be amended to include a detailed and complete definition of the data to be retained, such that each characteristic is fully and accurately described, including for technical clarity.*

*1.1.2 Clause 187A(2) be amended such that the requirement that definition of the data to be retained must directly relate to those characteristics should apply specifically to both the 'information' and 'documents containing information of that kind'.*

## 1.2 Grounds on Which Access is Given

The TIAA currently provides access to two types of information.

- communications intercepted while passing over a telecommunications network
- stored communications (e.g. email messages, SMS, text messages).

For both kinds of content data, the TIAA limits the grounds on which access will be granted to a 'serious offence', as defined under that Act.[3] Further, the TIAA generally requires that such grounds be established through the issuing of a warrant for access. The Bill contains no similar threshold that must be met before data can be accessed.

**Recommendations**

*1.2.1 Amend the Bill to require that access to data under Part 5-1A Data Retention only be granted on the ground of a reasonable suspicion that a 'serious offence' has been, is being or will be, committed.*

[3] *Telecommunications (Interception and Access) Act 1979.* Section 5D.

### 1.3 Agencies able to Access Data

The Bill describes the list of agencies that can access data to an 'enforcement agency' or 'criminal law-enforcement agency'.[4] However, the Bill also provides that heads of agencies and authorities not listed in the legislation may request the Attorney-General to declare that the agency or authority is an enforcement agency' or 'criminal law-enforcement agency' for the purposes of the legislation.[5]

In making such declaration, the Attorney-General must have regard to whether the agency or authority administers a law 'imposing a pecuniary penalty' or one relating to the protection of public revenue'.[6] Almost all Commonwealth, State, Territory and Local authorities and agencies now have the power to impose pecuniary penalties or the power to protect public revenue and could therefore potentially seek to be named an 'enforcement agency' under the legislation. Indeed, a number of agencies have already indicated that they intend to pursue this course of action.

Defining such organisations in regulations instead of in the primary legislation means additions to the list will not receive the parliamentary scrutiny that should be afforded to the granting of these powers.

**Recommendations**

*1.3.1 Amend the Bill to remove the power of the Attorney-General to expand the Bill's existing list of 'enforcement agencies' and 'criminal law-enforcement agencies'. Alternatively, if recommendations are adopted to limit grounds on which access is given, confine the declaration power of the Attorney-General to those bodies or agencies that are involved in the prevention and/or detection of a 'serious offence' as defined in the TIAA.*

## *2. Lack of Clarity*

In many areas the language used in the Bill is unclear and does not reflect the technical complexity of today's communications.

The 'characteristics' of the data to be retained would be reasonably clear in the mobile and fixed-line telephony contexts. The 'source' would be the calling number of the device, the 'destination' would be the called device, and the date, time and duration of the call is information already retained by telephone service providers. (The Society does however have concerns about the inclusion of location information relating to mobile telephony and believes this information warrants safeguards additional to those for other 'call-related' data.)

However, in the context of Internet Protocol-based communications the meaning of those terms noted is not clear-cut. One of the 'characteristics' of the data to be retained is the 'destination' of a communication. Yet in Clause 187A(4)(b)(i) of the Bill, a service provider is explicitly not required to keep

[4] The Amendment, Schedule 2, Proposed Clauses 110A and 176A

[5] *Ibid*.

[6] *Ibid*, Proposed Clause 176A (3)

information on an 'address to which the communications was sent' on the Internet. 'Address' could mean the URL, the IP address, both, a MAC address[7] or other information – the communication's destination.

Furthermore, in the context of defining those covered by proposed requirements, the Bill refers to a person that owns or operates 'infrastructure' in Australia. It is unclear whether that refers to persons/companies that provide a service in Australia, or that own or operate equipment of some kind, or persons that own or operate 'network units' as defined in the *Telecommunications Act 1997*.

It is also unclear why one of the 'characteristics' of the data is a 'telecommunications device relating to a relevant service'. Service providers are not likely to have information on the nature of the device relating to the relevant service if the customer has chosen and sourced the device themselves (e.g. an ADSL modem for an Internet service).

Finally, the Bill seeks to define many communications from a single device as one 'communication'. Given that it is routine practice for many devices to remain on and connected for hours, days or even months at a time, this choice of wording is extremely problematic.

**Recommendations**

*2.0.1 The Government should meet with all relevant stakeholders to clarify the data that security and law enforcement agencies need to access for the prevention and/or investigation of criminal activity, and to develop and include appropriate terminology that can be incorporated into this legislation in order to make the legislation clear and unambiguous. This recommendation should be considered as a precursor to the recommendation on clarification of data to be retained, and for absolute clarity, 'relevant stakeholders' should be taken to include representatives of each of the following:*

- *Government*
- *Law enforcement and Security agencies*
- *Industry (both large and small providers, in addition to industry associations)*
- *Civil Society, including representatives of Internet users and privacy-focused groups*

# *3. Coverage*

## 3.1 Providers

[7] This refers to a 'Media Access Control' address, which is a unique identifier assigned to network interfaces for communications on the physical network segment. It is in no way specifically related to any products marketed by Apple Computer. For more information, please see: http://standards.ieee.org/faqs/regauth.html

Under Clause 187A(3) the data retention requirements apply only to services operated by a carrier, an Internet service provider (as defined in the Broadcasting Services Act 1992) or of a kind prescribed by regulations. This is highly problematic for three reasons.

Firstly, licensed carriers that are not also carriage service providers will not have any information about relevant services to retain. A carrier licence only allows ownership of transmission infrastructure. A licensed carrier is not required to also own and operate switching equipment that provides a service that might generate communications data.

The Bill does not cover carriage service providers that are not Internet service providers. That would include the vast majority of services provided as private networks such as corporate Virtual Private Networks, business-grade networks linking office PABXs, data networks linking ATMs, or just resellers of telephony services that do not provide access to publicly available internet services. Indeed, public access networks such as municipal Wi-Fi networks, public libraries, airport and rail public networks will not log users' communications data as they are neither carriers nor ISPs. These are the very networks that one would expect to be used for their communications by those the Government seeks to target in this legislation.

Finally, because regulations can be used to expand those covered by the Bill its ultimate coverage is uncertain. This is particularly relevant for industry participants who are not covered by this Bill but could, in future, be subject to its requirements.

## 3.2 Immediate Circle

The Bill also will not apply to services that are provided within the provider's 'immediate circle'. Examples of an immediate circle include libraries and universities. It is also unclear whether this exemption would mean Internet cafes are also not subject to the Bill's requirements. It appears that anybody seeking to evade the provisions of the Bill could simply become a student somewhere and communicate within that educational institution without detection.

## 3.3 Over-The-Top Services

Australians increasingly use a broad range of Internet-based services (applications) for their communications (often referred to as over-the-top (OTT) services), such as webmail, social media, instant messenger and Voice over Internet Protocol (VoIP) services.

This expansion in choice of communications methods creates new challenges for law enforcement and intelligence agencies, especially given the increasing use of encryption for such services.

Putting aside the very significant technical challenges involved in retaining non-content data relating to the use of such services, the Bill appears to make a distinction between services operated from within Australia, which are to be included, and those operated from elsewhere, which are not. As such, data usage on the most popular application services used by Australians – such as those provided by Facebook, Google, Yahoo, Microsoft (including Skype) and others – may not be available for use by law enforcement and security agencies.

This prospect will result in significant 'gaps' in the data retained under the terms of this Amendment (including a very significant majority of emails sent and received by Australian consumers) and is therefore likely to undermine the efficacy of this legislation's stated purpose of providing the means to identify activities that represent a potential security risk.

### 3.4 Retention of Telephony Information

Clause 187A(4)(b)(ii) of the Bill exempts service providers from retaining information that 'was obtained by the service provider only as a result of providing the service'. The Society understands that the provision is intended to exclude web browsing history from retention requirements. However, it would operate to exempt the provider of a telephony service from retaining both the called number and duration of the call, since those pieces of data are only discovered by the provider as a result of the telephone service.

**Recommendations**

*3.4.1 Amend Clause 187A(3) of the Bill to apply to all carriers, and carriage service providers that provide carriage services to the public.*

## *4. Impact on the Industry, Competition and Deregulation*

The Bill's requirements for data retention represent a major impost on industry. The Bill will significantly expand data that service providers now retain. And for those service providers that do not now have systems in place to retain the data, retention requirements may well be an insurmountable barrier to entry, particularly for smaller providers.

### 4.1 Requirements to Expand Existing Retention Capability

The drafters of the legislation and accompanying explanatory material are being disingenuous in describing this data as data routinely collected and stored by service providers. Traditionally, the data accessed by agencies is billing data, information that routinely appeared on the customer's service invoice to enable the customer to verify that the correct legal entity was being billed and verify that the bill was correct. This is also data that the provider is required to keep for periods of years to substantiate financial reports and in case of a legal dispute.

This Bill significantly expands the forms and types of information and data that providers will be required to store, keep secure, manage and make available in accessible formats far beyond data kept anyway for billing purposes, with a concomitant increase in cost, complexity, and the risk of improper disclosure or information theft with potentially serious consequences to citizens and customers if their private communications data falls into the improper hands.

### 4.2 Requirement to Provide New Retention Capability

The Bill requires those service providers that do not currently retain required information to develop 'other means' of doing so. The Bill would require service providers whose service does not create the

required information 'to use other means' to create the required information or a document containing the information.[8]

For providers of mobile and fixed-line telephony services, this requirement will be relatively easily met, with the important exception of location data for mobile services. However, most, if not all Internet service providers (ISPs) base their billing model on transmission capacity used by the subscriber. Information on the time, duration, date and destination of capacity used is not usually retained. Indeed, some smaller ISPs could struggle to survive if they had to develop and maintain a costly data retention system that is not required for their business purposes.

These additional costs will also adversely affect the ability of local providers to compete in markets that are internationally exposed, particularly cloud hosting and email services. This Bill therefore has the potential to directly harm the international competitiveness of Australian service providers.

We recognise that the Bill makes provision for service providers to develop Implementation Plans, allowing them to develop systems for data retention over time.[9] Further, the Communications Access Co-ordinator may grant specific service providers exemptions from some or all of the requirements of the Amendment.[10] However, data retention requirements under the Bill will be ongoing with potentially significant financial implications for smaller service providers. Without Government assistance, it is highly probable that smaller service providers will either exit the market, or not enter the market in the first place, thereby putting upward pressure on internet connectivity and related costs as well as hindering innovation.

**Recommendations**

*4.2.1 Government assistance should be made available for ISPs who would otherwise not retain the required data and do not have the financial resources to develop systems that would retain the required data.*

## *5. Inquiry into use of Section 313 of Telecommunications Act*

The House of Representatives Standing Committee on Infrastructure and Communications is currently conducting an '*Inquiry into the use of subsection 313(3) of the Telecommunications Act 1997 by government agencies to disrupt the operation of illegal online services.*' Because that subsection allows Government agencies to request information from service providers, the outcomes of that inquiry will affect service provider provision of information and therefore needs to be considered as part of this inquiry. As such, the timetable for this inquiry should be extended beyond the reporting date of the Section 313 inquiry to enable the findings from that inquiry to be considered.

[8] *Ibid*, Proposed Clause 187A(6)

[9] Ibid, Proposed Clauses 187D to 187J.

[10] Ibid, Proposed Clause 187J.

## *6. Consultation and Regulation Processes*

The consultation processes used to determine the precise technical definition of the data to be retained are as yet undefined, and to date have excluded many important stakeholder groups. The Society therefore urges the government to include a broader range of stakeholders in its consultations in future.

The Internet Society is a unique organisation in that it represents the interests of all Internet users and which has expertise across both the regulatory and technical landscapes. The Society is therefore able to provide an holistic perspective of the potential impact of laws affecting the Internet and telecommunications services more broadly. One of our primary aims is to assist legislators, drafters and non-technical stakeholders in understanding the implications of changes to the operations of the Internet, including legislation that directly or indirectly affects Internet users.

As such, the Society is keen to be included in all future consultations relating to this legislation and urges the Government to also include other relevant civil society organisations in such consultations.

## *7. Conclusion*

The sections above summarise the major concern the Society has with this Bill. We believe that, as currently drafted, it will fail to achieve its intended aims and yet it will create significant and unnecessary obligations for Internet service providers, 'application' service providers and Internet users. Obligations that will have serious negative consequences for the continued development and use of communications services in Australia and the development of our digital services economy

As we have indicated above, there are simply too many opportunities for technically qualified organisations and individuals to work around the requirements of the legislation as it is currently framed. There is ample evidence that those the Government seeks to target already have highly skilled capabilities and the knowledge and equipment to avoid detection. Their communications are not likely to be overly constrained or necessarily detected by these new requirements.

Finally, the Society would like to draw to the Parliament's and to the Government's attention the ubiquitous nature of the globally based Internet. Australia is limited in how we can affect the use – both legitimate and illegitimate – of the World Wide Web.

The Society supports the Government's desire to ensure national security. However we believe that data retention is a matter where it is impractical for one country to legislate in isolation. We therefore urge the Government to work with us and other relevant stakeholders to develop a more workable data retention regime - one that takes into account both technical realities and the experiences of other countries and jurisdictions.

## *8. About the Internet Society*

The Internet Society of Australia (also known as ISOC-AU) is the Australian chapter of the worldwide Internet Society and is a not-for-profit organisation founded in 1996. Our mission is to promote Internet developments for the benefit of the whole community, including business, educational, professional and

private Internet users. Our directors and members hold significant roles in Internet-related organisations and enable the Society to provide high level policy and technical information to Internet user groups, governments and regulatory authorities.

Globally, the Internet Society coordinates Internet policy development and technical standards. This includes advising the United Nations and international Internet management organisations such as the Internet Corporation for Assigned Names and Numbers (ICANN) and the five Regional Registries. The Internet Society is responsible for the Internet Engineering Task Force. See: www.internet.org.au