GILBERT + TOBIN CENTRE OF PUBLIC LAW

THE UNIVERSITY OF NEW SOUTH WALES

FACULTY OF LAW

GILBERT + TOBIN CENTRE
OF PUBLIC LAW

9 December 2014

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

Dear Secretary,

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

Thank you for the opportunity to make a submission to this inquiry. We do so in our capacity as members of the Gilbert + Tobin Centre of Public Law at the Faculty of Law, University of New South Wales. We are solely responsible for the views and content in this submission.

We recognise the importance of standardising the collection of data by communications service providers. Given that telecommunications data can play an important role in investigating serious criminal offences such as terrorism and child pornography, we accept that this data should be available to law enforcement agencies in appropriate circumstances. Having a clear and codified legislative scheme for the collection of telecommunications data is a worthy goal that will aid in the prevention of serious crime.

Our concerns then about the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth) (the Bill) are not in respect of its object, which we support, but in regard to how this has been implemented. In particular, the Bill in its current form is little more than a shell for such a scheme, with many important details left to be finalised in regulations. This can be seen not only in the types of data that will be retained under the scheme,[1] but also with regard to the agencies that will have access to this data.[2] This ad hoc approach is unsatisfactory given that mandatory data retention has significant implications for the right to privacy.[3] Telecommunications data can reveal significant private details about an individual, such as who they have communicated with and their

[1] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth), sch 1, Item 1, cl 187A.
[2] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth), sch 2, Item 3, cl 110A, Item 4, cl 176A.
[3] Parliamentary Joint Committee on Human Rights, Parliament of Australia, *Examination of Legislation in Accordance with the Human Rights (Parliamentary Scrutiny) Act 2011: Fifteenth Report of the 44th Parliament* (November 2014) 11-13.

SYDNEY 2052 AUSTRALIA
Telephone: +61 (2) 9385 9654
Facsimile: +61 (2) 9385 1175
www.gtcentre.unsw.edu.au

whereabouts at particular times. The core aspects of the regime should therefore be defined in the primary legislation and reconsidered by Parliament if change is later considered necessary.

We also believe that the government has failed to satisfactorily justify why data should be retained for a period of two years.[4] The government has reasoned that data less than six months old is the most frequently accessed, but data up to two years old can be necessary for investigations into terrorism and other complex criminal offences.[5] Given that this timeframe is central to the operation of the regime, we believe that a stronger case needs to be made as to why it is necessary. We note that the same concern has been raised by the Parliamentary Joint Committee on Human Rights.[6] In particular, a stronger justification for the two-year timeframe could help to reduce public perceptions that the Bill is designed to allow mass surveillance of the population.[7]

Below we address in greater detail our major concerns with the Bill.

1. Definition of Metadata

Currently, Chapter 4 of the TIA Act allows enforcement agencies to access telecommunications data held by service providers.[8] This may be done with respect to data already collected (retrospective data) where it is reasonably necessary for investigations into criminal offences, missing persons or laws that impose pecuniary penalties or protect the public revenue.[9] Alternatively, an enforcement agency may authorise the monitoring of this data in advance (prospective data) for a period of up to 45 days where doing so is reasonably necessary for the investigation of a serious criminal offence.[10] Different rules apply to the Australian Security Intelligence Organisation (ASIO), which may authorise the disclosure of retrospective or prospective data (for a period of up to 90 days) where doing so would be in connection with the performance of ASIO's functions.[11] Importantly, the TIA Act does not define the types of data that are to be retained for any of these purposes. It states only that the contents or substance of a communication cannot be disclosed under these provisions.[12]

The Bill would require service providers to retain telecommunications data for two years.[13] Under this mandatory data retention regime, service providers would be required to retain: (a) information of a kind prescribed in the regulations, or (b) documents containing information of that kind.[14] The kinds of information to be prescribed in the regulations 'must relate to' one or more in a range of specified categories, including: the subscriber, account or device relating to a relevant service; the source of a

[4] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth), sch 1, Item 1, cl 187C.
[5] Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth), 19.
[6] See Parliamentary Joint Committee on Human Rights, above n 3, 15.
[7] See, eg, 'Metadata bill crosses privacy line: Greens', *SBS News (Online)*, 30 October 2014 <http://www.sbs.com.au/news/article/2014/10/30/metadata-bill-crosses-privacy-line-greens>. Katharine Murphy, 'Data Retention: Liberal Backbencher Calls for Metadata Warrant Requirement', *The Guardian* (Sydney), 12 August 2014.
[8] *Telecommunications (Interception and Access) Act 1979* (Cth), ch 4, div 4.
[9] *Telecommunications (Interception and Access) Act 1979* (Cth), ss 178, 178A, 179.
[10] Or one that is punishable by at least three years' imprisonment: *Telecommunications (Interception and Access) Act 1979* (Cth), s 180(4).
[11] *Telecommunications (Interception and Access) Act 1979* (Cth), ss 175-176. In the case of retrospective data, authorisations may be made by the Director-General of Security, Deputy Director-General of Security, or an authorised ASIO employee or affiliate. In the case of prospective data, authorisations may be made by the Director-General of Security, Deputy Director-General of Security, or an ASIO employee or affiliate employed at Senior Executive Service (SES) Level 2.
[12] *Telecommunications (Interception and Access) Act 1979* (Cth), s 172.
[13] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth), sch 1, Item 1, cl 187C.
[14] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth), sch 1, Item 1, cl 187A(1).

communication; the destination of a communication; the date, time and duration of a communication; and the location of equipment used in connection with a communication.[15] These categories of information are commonly referred to as 'metadata', and do not extend to the contents or substance of a communication.[16]

By listing these categories of information, the Bill provides guidance on the types of data that will be retained. However, it fails to include a formal definition of metadata in the TIA Act. Until the relevant regulations are made, the data to be collected under the regime will remain unspecified. Data specified in the regulations might 'relate to' one of the above categories in a tenuous way, thereby revealing more significant private information than the categories currently suggest. For example, information might be said to 'relate to' the subscriber of a relevant service if it reveals the location of the person's children and other family members.

Given the significant privacy implications in allowing enforcement agencies to access telecommunications data – such as information about the source, destination and location of communications between individuals – we believe that a formal definition of metadata should be included in the Bill. This could be achieved by requiring that service providers retain 'metadata'. Metadata could then be defined in the primary legislation according to those categories listed above. This would put it beyond doubt that only those types of information will be retained and accessed under the regime.

2. Criminal Law Enforcement Agencies and Enforcement Agencies

Under the TIA Act, 'enforcement agencies' are currently able to access both stored communications (such as the content of emails or SMS messages) and data about communications (metadata).[17] The former requires a warrant for access,[18] whereas the latter does not. 'Enforcement agency' is defined as including: the Australian Federal Police (AFP); State Police forces; investigative bodies such as the Australian Crime Commission (ACC) and the Independent Commission Against Corruption (ICAC); the CrimTrac Agency; and any body administering a law that imposes a pecuniary penalty or protects the public revenue.[19]

The Bill would amend the TIA Act so that only a 'criminal law enforcement agency' may apply for a warrant to access stored communications.[20] This will be defined as including the AFP, State Police forces, and other investigative bodies such as the ACC and ICAC.[21] On its face, the definition excludes authorities that are responsible for imposing pecuniary penalties or protecting the public revenue.[22] The government has claimed that this amendment 'substantially reduces' the number of agencies that are able to apply for stored communications warrants,[23] and this is a commendable goal given the significant personal information that can be revealed by the contents or substance of communications.

[15] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth), sch 1, Item 1, cl 187A(2).
[16] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth), sch 1, Item 1, cl 187A(4)(a).
[17] *Telecommunications (Interception and Access) Act 1979* (Cth), chs 3, 4.
[18] *Telecommunications (Interception and Access) Act 1979* (Cth), ss 110, 116.
[19] *Telecommunications (Interception and Access) Act 1979* (Cth), s 5.
[20] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth), sch 2, Item 3, cl 110A.
[21] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth), sch 2, Item 3, cl 110A(1).
[22] As permitted by the current definition of 'enforcement agency': *Telecommunications (Interception and Access) Act 1979* (Cth), s 5.
[23] Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth), 21.

However, as the Bill would allow the Attorney-General to declare other authorities and bodies as criminal law enforcement agencies, [24] uncertainty will remain over who will be able to apply for stored communications warrants. In making such a declaration, the Attorney-General must consider a range of factors, including whether the authority is involved in 'investigating serious contraventions'.[25] This wording suggests that only organisations involved in investigating serious breaches of the criminal law will be declared under the provision. However, it is not a limiting factor. The Attorney-General could declare *any* authority or body as a criminal law enforcement agency, so long as he or she considers the specified range of factors in doing so. In particular, the Attorney-General may consider 'any other matter' that he or she considers relevant.[26] It is therefore possible that agencies involved in enforcing fines and protecting the public revenue – including the Australian Taxation Office, local councils, or bodies responsible for enforcing copyright infringements – could be reinstated with the power to apply for warrants to access stored communications.

To achieve greater clarity in the definition of 'criminal law enforcement agency', and to appropriately limit access to stored communications in line with the government's intended purposes, we believe that the matter listed in the proposed s 110(4)(a) should limit the Attorney-General's declaration-making power. That is, the Attorney-General should only be able to declare an authority or body as a criminal law enforcement agency if he or she is satisfied that the agency is involved in 'investigating serious contraventions'.[27]

A similar problem exists with regard to the agencies that will have access to metadata. As in the current legislation, the Bill would allow metadata to be accessed by 'enforcement agencies'.[28] The Bill would define enforcement agencies as including (a) criminal law enforcement agencies, and (b) any other authority or body declared by the Minister to be an enforcement agency.[29] In declaring an authority or body as an enforcement agency, the Attorney-General must consider a range of factors, including whether the agency enforces the criminal law, imposes pecuniary penalties or protects the public revenue.[30] Again, these are not limiting factors, so it is possible that any authority or body could be declared as an enforcement agency provided that the Attorney-General considers those factors in making a declaration. Other than the criminal law enforcement agencies specified in the Bill (such as the AFP and State Police forces),[31] it is not clear which organisations will have access to metadata under the new regime. This will only become clear once the relevant declarations are made.

It is unsatisfactory that this central aspect of the regime – who can access metadata – will remain undefined until the Attorney-General makes declarations to that effect. This is especially concerning given that the government has made representations that metadata will only be accessed for the purpose of investigating serious criminal offences. For example, the Attorney-General has claimed that the metadata regime will apply 'only to the most serious crime, to terrorism to international and

[24] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth), sch 2, Item 3, cl 110A(3).
[25] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth), sch 2, Item 3, cl 110A(4)(a).
[26] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth), sch 2, Item 3, cl 110A(4)(f).
[27] As in Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth), sch 2, Item 3, s 110A(4)(a).
[28] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth), sch 2, Item 4, cl 176A.
[29] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth), sch 2, Item 4, cl 176A(1).
[30] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth), sch 2, Item 4, cl 176A(4)(a).
[31] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth), sch 2, Item 3, cl 110A(1).

transnational crime, to paedophilia'.[32] He has also claimed that agencies will not be able to access metadata for the purpose of investigating copyright infringements and online piracy.[33] These statements are incorrect and misleading. The Attorney-General will have the power to declare any authority or body as an enforcement agency, including those that enforce fines, investigate minor criminal offences, or adjudicate civil wrongs. This could include local councils, gambling authorities, universities, private security firms, toll road operators, family law dispute resolution services and organisations responsible for enforcing copyright infringement.

If declared as enforcement agencies, these and any other organisations would be able to authorise the disclosure of metadata and access significant identifying details about individuals' lives. It may be that the current government does not intend to declare the organisations listed above as enforcement agencies, but there is nothing in the legislation to prevent future governments from doing so.

As such, we believe that the Bill should define 'enforcement agency' with greater specificity+. If it is not practicable to list all relevant authorities that will have access to metadata, the legislation should at least specify the types of authorities that will have access (such as local councils, and authorities responsible for taxation). These categories should be appropriately considered by Parliament as part of the primary legislation. In addition, the power to declare authorities or bodies as enforcement agencies should be limited to those organisations that enforce the criminal law, impose pecuniary penalties or protect the public revenue.

3. Lack of a warrant process

When the Attorney-General declares an agency as an enforcement agency,[34] that agency will be able to access metadata retained by service providers without a warrant. The agency would do so by requesting and authorising a service provider to disclose that information. Such authorisations could be made in relation to retrospective data where doing so would be reasonably necessary for the enforcement of the criminal law, a law imposing a pecuniary penalty, or a law protecting the public revenue.[35] In relation to prospective data, such authorisations could be made where reasonably necessary for the investigation of a serious criminal offence.[36] ASIO would be able to access retrospective or prospective metadata where the disclosure of that information would be in connection with the performance of the agency's functions.[37] This differs from the process relating to stored communications, which can only be accessed by criminal law enforcement agencies through a warrant process.[38]

We are concerned by the prospect that enforcement agencies will effectively be able to access metadata on a 'self-serve' basis. Given that metadata can reveal a significant amount of identifying information about an individual, we believe that greater procedural protections for accessing metadata should apply. This is especially important given that it is not yet clear which authorities or bodies will have access to metadata. It would also help to mitigate concerns amongst the general public about the possible scope of the new regime.

This could be achieved through a warrant process along the lines of that allowing access to stored communications.[39] An authorised officer of an enforcement agency could be required to apply to an

[32] ABC Television, 'National Security: Finding a Balance', *Q&A*, 3 November 2014 (George Brandis) <http://www.abc.net.au/tv/qanda/txt/s4096883 htm>.
[33] Ibid. See also Matthew Knott, 'Game of Thrones Downloaders Need Not Fear Data Retention Plans, Says Malcolm Turnbull', *Sydney Morning Herald*, 31 October 2014.
[34] Under Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth), sch 2, Item 4, cl 176A(3).
[35] *Telecommunications (Interception and Access) Act 1979* (Cth), ss 178, 178A, 179.
[36] *Telecommunications (Interception and Access) Act 1979* (Cth), s 180.
[37] *Telecommunications (Interception and Access) Act 1979* (Cth), ss 175-176.
[38] *Telecommunications (Interception and Access) Act 1979* (Cth), ss 110, 116.
[39] *Telecommunications (Interception and Access) Act 1979* (Cth), ss 110, 116.

'issuing authority' (an appointed judge, magistrate or tribunal member) for a warrant allowing access to metadata. The warrant could be issued if access to the information by an enforcement agency would be 'likely to assist' with the enforcement of a criminal law, a law imposing a pecuniary penalty, or a law protecting the public revenue.[40] This model was supported by the Parliamentary Joint Committee on Human Rights,[41] and the higher procedural burden would be consistent with the capacity for metadata to reveal significant private details about an individual. Metadata is not trivial information, and enforcement agencies should not be free to access that information wherever doing so is reasonably necessary to enforce minor infringements, such as parking or library fines.

We accept that a warrant process along these lines could pose a significant administrative burden to law enforcement and intelligence agencies investigating serious criminal offences and threats to national security. As such, a preferable alternative might be to implement a ministerial warrant process. This could be incorporated into existing ministerial warrant processes where available to ensure maximum efficiency without compromising procedural safeguards. For example, the Director-General of Security currently has the power to request an identified person warrant from the Attorney-General.[42] These warrants allow ASIO to conduct various forms of surveillance against a single person who is reasonably suspected of involvement in activities prejudicial to security.[43] Access to metadata could be included as another surveillance option which can be applied for through this single warrant process.

A ministerial warrant process would allow law enforcement and intelligence agencies to access metadata in a timely fashion whilst ensuring that there is enhanced political accountability for the regime. As it stands, the Bill would allow criminal law enforcement agencies and enforcement agencies to access metadata on their own terms, without any direct chain of responsibility extending to the Ministers responsible for its implementation.

*****

Improvements in these three areas would fill important gaps in the Bill, which currently sets out a framework for a data retention regime but fails to specify its core elements. The data to be retained by service providers remains ill-defined, and new enforcement agencies can be added on an ad hoc basis through additional regulations. In this undeveloped form the regime is open to enormous creep in scope and could expand significantly over time, including through regulations made by future governments. The improvements suggested above would help to limit the scope of the regime to the current government's intended purposes. They would also ensure that mandatory data retention impacts on privacy to the minimum extent necessary.

Yours sincerely,

Dr Keiran Hardy
Research Fellow, Gilbert + Tobin Centre of Public Law, University of New South Wales

Professor George Williams AO
Anthony Mason Professor and Foundation Director, Gilbert + Tobin Centre of Public Law, University of New South Wales

[40] As in *Telecommunications (Interception and Access) Act 1979* (Cth), ss 116(1)(d).
[41] Parliamentary Joint Committee on Human Rights, above n 3, 18.
[42] *Australian Security Intelligence Organisation Act 1979* (Cth), s 27C.
[43] *Australian Security Intelligence Organisation Act 1979* (Cth), s 27C(2).