2

The case for data retention

2.1 When this Committee last considered the issue of mandatory data retention as part of its *Inquiry into potential reforms of Australia's national security legislation*, the then Government had not prepared or released a detailed legislative proposal; the question was dealt with at the conceptual level. The absence of a detailed legislative proposal limited the capacity of the public to make meaningful comment on this issue, and limited the capacity of the Committee to consider and resolve the question of whether such a scheme was, at the most fundamental level, capable of being justified for national security and law enforcement purposes.

2.2 In 2012–13, there was a relatively clear divide between law enforcement and national security agencies in support of the proposal, and organisations and individual submitters in opposition to the proposal.

2.3 In this inquiry, however, the Committee and the public have had the benefit of being able to review draft legislation, a proposed data set, detailed supporting materials and submissions prepared by the Attorney-General's Department and other Government agencies. The Committee has, therefore, received detailed submissions arguing the need for data retention from a wide range of stakeholders.

2.4 Based on the submissions and evidence this Committee has received over the course of this inquiry, the dichotomy between Government and non-Government submissions has weakened. Many organisations and individuals remain opposed to the principle of data retention.[1] However,

---

1 See, for example: Mr Ben Johnston, *Submission 35*, p. 1; Mr Bernard Keane, *Submission 37*, p. 1; Mr Glenn Bradbury, *Submission 38*, p. 1; Blueprint for Free Speech, *Submission 54*, p. 3; Australian Privacy Foundation, *Submission 75*, p. 2; Dr Lesley Lynch, Secretary, New South Wales Council for Civil Liberties, on behalf of joint councils for civil liberties, *Committee Hansard*, Canberra, 30 January 2015, p. 79; Amnesty International, *Submission 95*, p. 1; Law Institute of Victoria, *Submission 117*, p. 1.

the concept of data retention, either as proposed by the Government in Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (the Bill) or in another form, has attracted support from a broad range of stakeholders. A selection of extracts from evidence provided by these stakeholders is contained below.

Box 2.1 – Selected extracts from submissions expressing in-principle support to data retention

It is Bravehearts' position that Australia should implement a data retention scheme as a critical tool for supporting the investigation of child sexual exploitation matters and other serious offences — Bravehearts, *Submission 33*.

[M]odernising our laws to reflect contemporary technical advances is obviously a sensible, justified and legitimate objective … We then, in short, support the passage of the bill … In particular, we strongly support the bill's proposal to confine the number of agencies that can access retained telecommunications data, and there are other aspects of the bill that we think are extremely useful — Professor Gillian Triggs, President, Australian Human Rights Commission, *Committee Hansard*, Canberra, 29 January 2015.

Metadata has become a vital part of the investigative process, and in almost all instances is a fundamental part of the case for acquiring a warrant with more and wider ranging powers — Alexander Lynch, *Submission 1*.

[W]e do see policy merits in a more standardised set of arrangements to give certainty for agencies, industry and citizens. So the policy intent of the overall framework we do think is an appropriate and worthwhile activity — Mr Matthew Lobb, General Manager, Industry Strategy and Public Policy, Vodafone Hutchison Australia, *Committee Hansard*, Canberra, 29 January 2015.

The Unit is largely supportive of the Bill, as a very important instrument in the fight against online child sexual abuse. The Australian Federal Police have identified the vital role metadata retention plays in the being able to identify and prosecute offenders engaged in online child sexual abuse. Further, the failure to pass this legislation will undoubtedly assist large numbers of offenders escape detection and prosecution each year, reducing the effectiveness of the Australian Federal Police in combating this crime type — Uniting Church Justice and International Mission Unit, *Submission 76*.

[T]he right to privacy is not absolute and requires an assessment to be made of whether the measures that may limit privacy are both necessary and proportionate to achieve that objective. Applying this in the context of the introduction of a data retention scheme, privacy interests must be balanced with the need to ensure that law enforcement and security agencies have access to the information necessary to perform their functions — Mr Timothy Pilgrim PSM, Australian Privacy Commissioner, *Committee Hansard*, Canberra, 29 January 2015

I think the previous inquiry exposed the extent to which data is potentially not being retained … we welcome efforts to standardise the data held and restrict access to a named group of agencies — Ms Narelle Clark, Deputy Chief Executive Officer, Australian Communications Consumer Action Network, Committee Hansard, Canberra, 29 January 2015.

2.5 Professor George Williams and Dr Keiran Hardy, submitting in their personal capacity as members of the Gilbert + Tobin Centre of Public Law at the Faculty of Law, University of New South Wales expressed in-principle support for data retention:

> 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. [2]

2.6 Mr John Stanton, CEO of Communications Alliance, the primary telecommunications industry body in Australia, gave evidence that the views of members of the telecommunications industry have also shifted since 2012:

> Last time we appeared before the committee back in 2012 we stated on behalf of the industry quite clearly that we did not believe a case had been made for the type of mandatory data retention regime that was at that time being proposed. Today it is fair to say there is something of a range of views among our membership as to whether such a case has now been made, and it depends in part on the final shape of the regime, around which many questions remain. [3]

2.7 However, the Committee does not wish to overstate the level and breadth of support for data retention. It remains a disputed proposal. For example, Blueprint for Free Speech stated that:

> Blueprint remains firmly against the introduction of a data retention regime in Australia. Cementing a place for a mass surveillance regime in Australia bucks international trend and does not reflect necessity or proportionality to the investigation and resolution of serious criminal activity.[4]

2.8 The Committee also received many submissions from individual community members which, by and large, expressed in-principle opposition to the proposed data retention regime. For example, Ms Priya Shaw stated that 'there is no version of this legislation I believe I can in good conscience support'.[5]

2.9 While it is impossible within the confines of this report for the Committee to cite from every individual submission, a representative selection of contributions from individual submitters is contained below.

Box 2.2 – Selected extracts from submissions made by individual community members

> Targeted communications surveillance, undertaken by LEAs via warrant, is a necessary and effective weapon in fighting serious crime including terrorism. However unwarranted blanket data

2 Professor George Williams AO and Dr Keiran Hardy, Gilbert + Tobin Centre of Public Law, Faculty of Law, University of New South Wales, *Submission 5*, p. 1.

3 Mr John Stanton, CEO, Communications Alliance, *Committee Hansard*, Canberra, 17 December 2014, p. 31.

4 Blueprint for Free Speech, *Submission 54*, p. 14.

5 Ms Priya Shaw, *Submission 47*, p. 1.

retention is fraught with dangers and represents a step change in powers that citizens would be required cede to government — Brian Ridgway, *Submission 54*.

I believe that our security organisations have failed to put a credible case as to why these changes, which impinge on the privacy of all Australians and thus give yet another win to the terrorists who aim to undermine our democracy, are necessary — Albert Lightfoot, *Submission 134*.

This bill will destroy the general public's basic right to privacy in an ill-advised bill resulting in the death of a fundamental democratic freedom — Iain Muir, *Submission 28*.

This metadata reveals far too much about citizens, who have a right to their privacy and who should not be treated like criminals — Fiona Maley, *Submission 49*.

Metadata now provides a more complete, constant and intrusive picture of an individual's lifestyle, habits and relationships than can be obtained by access to content alone — Alexander Lynch, *Submission 1*.

This bill tries to make the distinction that 'metadata' is of lesser importance to regular 'content'. I disagree, as it can be as important or even more important — Adam Cooksley, *Submission 43*.

… the Bill does not define what categories of data industry will be forced to retain. This is the single most critical aspect of the proposed regime, and the Government needs to reveal this information to enable effective and robust consideration of the proposal by the Australian community — Damien Donnelly, *Submission 30*.

Treating all Australians as potential suspects runs contradictory to not only our democracy but our Australian values — Alicia Cooper, *Submission 22*.

Australia's internet is already overly expensive and this policy will just end up costing every Australian citizen more money to use the internet. Whether it is paid for by the ISPs or by the Government, any internet user will have to foot the bill either through higher ISP fees, or through government taxes — Tom Courtney, *Submission 23*.

Not only will the proposed legislation compromise the privacy and freedoms of all Australians that use the internet, but and perhaps most importantly, similar laws around the world both in the United States and Europe have been proven not to work; why would they work here? — Cam Browning, *Submission 44*.

Many terrorists are already familiar with ways to circumvent these proposals meaning that majority of the people who will be affected will be law abiding citizens while the terrorists 'swim through the net' — Peter Freak, *Submission 26*.

The two year data retention duration specified in the legislation has never been justified. It is significantly longer than the retention duration in most other jurisdictions that have implemented similar schemes — Douglas Stetner, *Submission 32*.

This legislation should require a warrant for access to any data retained, as recommended by the Parliamentary Human Rights Committee. This maintains coherence with requirement for judicial oversight and maintains a balance where an external party must be satisfied as to the reason for the request — Barbara Reed, *Submission 154*.

The Australian public needs clear and transparent guarantees that their sensitive personal data information will be protected from hackers or foreign entities, especially in the light of the number of significant data breaches in recent times — Mason Hope, *Submission 18*.

What regulations will be enforced to make sure my private information and property are not stolen or leaked out onto the internet? Can the Australian Government guarantee that my information will be protected? Can ISPs do the same? Is it even possible to make such a guarantee? — Josh O'Callaghan, *Submission 29*.

With vast amounts of very revealing, very telling, very intimate data sitting in one place, these data centres will be a primary target of cybercriminals and hackers from all around the world — Daniel Scott, *Submission 61*.

Copyright holders will demand access to these stores of metadata likely pressing down on service providers via threats of litigation. These will be used in turn to self-police their intellectual property

— Iain Muir, *Submission 28*.

This bill is an attack on the personal freedoms of Australian citizens and particularly undermines the ability of journalists and whistle-blowers to expose corruption and misconduct in government agencies — Dr Peter Evans, *Submission 57*.

A similar metadata storage plan has already been considered and rejected by the European Union's Court of Justice — please give this plan the same consideration that it was given there — Bethany Skurrie, *Submission 63*.

2.10 The Committee has been requested to review the Government's proposal to establish a mandatory telecommunications data retention regime, including appropriate exemptions, safeguards and oversight mechanisms, and to provide advice to the Parliament on these important issues.

2.11 In this process, the Committee is mindful of the advice of the Australian Information Commissioner, Professor John McMillan, who has previously noted that the question of data retention raises a number of interrelated policy issues, and argued for the need to carefully distinguish between these issues when discussing data retention:

> [T]he term 'data retention' in fact camouflages a whole range of other issues. There is the question of data capture, data minimisation, data security, data storage and data use … My anecdotal observation of the debate is that all of those issues are sort of tossed around fairly indiscriminately, and all under the umbrella of 'data retention'. At the end of the day what we clearly need is to untangle those issues and work through them on a systematic and principled basis.[6]

2.12 This chapter addresses this issue through consideration of the following topics:

- the adequacy of the current regime,
- privacy and civil liberties concerns, and
- security of the retained data.

2.13 The Committee notes that the final two topics are closely related, as the potential for security breaches has significant ramifications for the proportionality and privacy risks associated with the proposed scheme.

2.14 Subsequent chapters of this report will address the substance of the proposed data retention regime, the implementation process, the cost of the proposed regime, arrangements for access to telecommunications data by government and non-government entities, and oversight and security arrangements.

6 Professor John McMillan, Australian Information Commissioner, *Committee Hansard*, Senate Legal and Constitutional Affairs References Committee, Canberra, 23 April 2014, p. 22.

Is the current regime adequate?

2.15 The following section provides an overview of the current regime for access to telecommunications data by national security and law enforcement agencies, including the types of data that are regularly accessed. The section concludes with a discussion of how the declining availability of telecommunications data, in conjunction with other challenges, is impacting on agencies operational capabilities and outcomes.

Overview of the current regime

2.16 At present, 'enforcement agencies' and the Australian Security Intelligence Organisation (ASIO) may access telecommunications data under an internal authorisation issued under Part 4-1 of the *Telecommunications (Interception and Access) Act 1979* (the TIA Act).

2.17 Telecommunications data is information about a communication or the parties to a communication, as distinct from the content or substance of that communication. Access to the actual content or substance of communication, such as a recording of a voice call, or the body or subject line of an email, is prohibited except under a warrant.[7]

2.18 During the course of the Committee's 2012–13 *Inquiry into potential reforms of Australia's national security legislation*, the Attorney-General's Department provided a document outlining the types of data it considered to be telecommunications data. In summary, telecommunications data includes:

- 'information that allows a communication to occur', such as the time, date and duration of the communication, the identifiers of the services and devices involved, and certain information about the location of the respective devices (such as which cell tower or access point the device was connected to), and
- 'information about the parties to the communication', such as their name, address and contact details, billing and transaction information, and general account information.[8]

2.19 An enforcement agency is defined to include the Australian Federal Police (AFP) or the police force of a State or Territory, as well as a limited number of crime commissions, integrity bodies, the Australian Customs

7 *Telecommunications (Interception and Access) Act 1979* (TIA Act), sections 7, 108 and 172.

8 See Appendix G of Parliamentary Joint Committee on Intelligence and Security (PJCIS), *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, Canberra, May 2013.

and Border Protections Service (Customs) and the CrimTrac Agency. However, the definition also contains an open-ended provision permitting 'any body whose functions include administering a law imposing a pecuniary penalty; or administering a law relating to the protection of the public revenue'.[9]

2.20 The power to authorise access to historic telecommunications data by an enforcement agency is limited to:

- the head of an agency,
- the deputy head of an agency, or
- a management-level officer or employee of the agency authorised, in writing, by the head of the agency.[10]

2.21 These authorised officers may only authorise access to historic telecommunications data where access to that particular data is 'reasonably necessary' for the enforcement of the criminal law or a law imposing a pecuniary penalty, or for the protection of the public revenue. Authorisations may only be made after considering whether any interference with the privacy of any person is justifiable, having regard to the likely relevance and usefulness of the data, and the reason why access is proposed to be authorised.[11]

2.22 In 2012–13, more than 80 Commonwealth, State and Territory enforcement agencies accessed historic telecommunications data under the TIA Act. In total, those agencies made 330 640 authorisations for access to historic telecommunications data,[12] resulting in a total of 546 500 disclosures.[13] The Queensland Police Service explained that, depending on how a service provider counts their disclosures, a single authorisation may result in a number of disclosures:

> [A]n authorisation requesting all information in relation to the connection of a mobile service requires a number of separate requests to be submitted to one telecommunications company as they will only provide information to specific request such as 'subscriber information', 'point of sale', 'copy of customer contract' and 'payment details'. It is this information together that would

9 TIA Act, section 5.

10 TIA Act, section 5AB.

11 TIA Act, Part 4-1.

12 Attorney-General, *Telecommunications (Interception and Access) Act 1979: Report for the year ending June 2013*, Commonwealth of Australia, 2013, pp. 47–51.

13 Australian Communications and Media Authority, *Communications Report 2012–13*, p. 54.

satisfy the documents/data being requested under the original authorisation.[14]

2.23 Previous evidence from the AFP indicates that approximately 85 per cent of data authorisations relate to subscriber information, such as name and address information, with only 15 per cent relating to 'traffic data', such as call charge records.[15] Victoria Police similarly provided evidence to this Committee that such subscriber checks 'make up the overwhelming majority of historical data requests made by Victoria Police'.[16] This evidence is consistent with the detailed operational briefings provided by a number of law enforcement and national security agencies to this Committee. However, the absence of more detailed, publicly-available information about the use of law enforcement agencies' use of powers under Chapter 4 of the TIA Act is an issue with the existing regime.[17] The Committee has made recommendations in support of enhanced collection of statistical information and annual reporting arrangements in Chapter 7 of this report.

2.24 For ASIO, authorisations for access to historic telecommunications data may only be made where the person making the authorisation is 'satisfied that the disclosure would be in connection with the performance by the Organisation of its functions'.[18] The Inspector-General of Intelligence and Security described the threshold set by the TIA Act as 'low', but also noted that ASIO must additionally comply with the Attorney-General's Guidelines, issued under section 8A of the *Australian Security Intelligence Organisation Act 1979* (ASIO Act),[19] which provide, among other things, that:

- the initiation and continuation of investigations shall be authorised only by the Director-General, or an officer at or above Executive Level 2 authorised by the Director-General for that purpose,[20]

14 Queensland Police Service, *Submission 19*, p. [3].

15 Australian Federal Police (AFP), *Submission 25*, Senate Legal and Constitutional Affairs References Committee, *Inquiry into the comprehensive revision of the Telecommunications (Interception and Access) Act 1979*, pp. 5–6.

16 Victoria Police, *Submission 8*, p. 2.

17 See, for example: PJCIS, *Report of the inquiry into potential reforms of Australia's national security legislation*, Canberra, May 2013, Recommendation 3; Attorney-General's Department, *Equipping Australia Against Emerging and Evolving Threats* (2012), p. 26; *Submission 26*, Senate Legal and Constitutional Affairs References Committee, *Inquiry into the comprehensive revision of the Telecommunications (Interception and Access) Act 1979*, p. 28.

18 TIA Act, Part 4-1.

19 Inspector-General of Intelligence and Security (IGIS), *Submission 131*, p. 3.

20 *Attorney-General's Guidelines in relation to the performance by the Australian Security Intelligence Organisation of its function of obtaining, correlating, evaluating and communicating intelligence relevant to security (including politically motivated violence)* (Attorney-General's Guidelines),

- any means used for obtaining information must be proportionate to the gravity of the threat posed and the probability of its occurrence,[21]
- inquiries and investigations into individuals and groups should be undertaken using as little intrusion into individual privacy as is possible, consistent with the performance of ASIO's functions, and with due regard for the cultural values, mores and sensitivities of individuals of particular cultural or racial backgrounds, consistent with the national interest,[22] and
- wherever possible, the least intrusive techniques of information collection should be used before more intrusive techniques.[23]

2.25 The number of data authorisations made by ASIO is not publicly reported on national security grounds. However, the former Director-General of Security, Mr David Irvine, recently provided evidence to the Senate Legal and Constitutional Affairs References Committee that the number of authorisations made by ASIO for access to telecommunications data each year is 'proportionate… with other individual agencies.'[24] This Committee is aware of the number of data authorisations made by ASIO, and can confirm the accuracy of Mr Irvine's statement.

Utility of telecommunications data for national security and law enforcement investigations

2.26 Mr David Vaile and Mr Paolo Remati, from the Cyberspace Law and Policy Community of the University of New South Wales Law Faculty, identified the value of telecommunications data to law enforcement and national security investigations:

> Many uses of telecommunications metadata, and content for that matter, for targeted law enforcement and criminal intelligence purposes are widely accepted and uncontroversial. Use of large volumes of metadata may also be justified in some cases. It is important to support such law enforcement and intelligence capabilities, since they have proven useful and there is a consensus that they can be appropriately regulated based on years of policy refinement.[25]

Guideline 8.1.

21 Attorney-General's Guidelines, Guideline 10.4(a).

22 Attorney-General's Guidelines, Guideline 10.4(b).

23 Attorney-General's Guidelines, Guideline 10.4(d).

24 Mr David Irvine AO, Director-General of Security, *Committee Hansard*, Senate Legal and Constitutional Affairs References Committee, Canberra, 21 July 2014, p. 10.

25 Mr David Vaile and Mr Paolo Remati, Cyberspace Law and Policy Community, University of New South Wales Law Faculty, *Submission 194*, p. 2.

2.27 However, several submitters asserted that telecommunications data is of no value to law enforcement and national security investigations. For example, Mr Peter Freak stated that:

> This kind of information not only is intrusive but does absolutely nothing to stop a potential terrorist attack. Despite this, it does however waste law enforcement resources that could be otherwise spent catching actual terrorists.[26]

2.28 The Attorney-General's Department submitted that:

> telecommunications data is critical to the investigation of almost any criminal activity, serious or otherwise, and almost any activity prejudicial to security that has been facilitated, enabled or carried out via communications technology. Electronic communications, by definition, do not leave a physical footprint, allowing individuals and groups to plan and carry out such activities without risk of detection via many 'traditional' investigative techniques. As such, the records kept by telecommunications companies about the services they have provided (telecommunications data) are often the only source of information available to agencies to identify and investigate individuals and groups using communications technologies for such purposes.[27]

2.29 The Committee also received detailed evidence from agencies about the role telecommunications data plays in their investigations. Agencies emphasised that telecommunications data is used extensively, and provides significant value, in serious and complex investigations.

2.30 Ms Kerri Hartland, then Acting Director-General of Security, confirmed that 'communications data has been critical to the disruption of terrorist attacks in Australia',[28] and provided the Committee with a detailed, unclassified summary of the use of telecommunications data in Operations Pendennis[29] and Neath.[30] ASIO's assessment was that, in both cases, had relevant telecommunications data not been available ASIO would have been blind to critical information, including the existence of covert communications between members of the terrorist groups, and the

26 Mr Peter Freak, *Submission 26*, p. 1.

27 Attorney-General's Department, *Submission 27*, p. 14.

28 Ms Kerri Hartland, Acting Director-General of Security, Australian Security Intelligence Organisation (ASIO), *Committee Hansard*, Canberra, 17 December 2014, p. 5.

29 ASIO, *Submission 12.1*, p. 33; Operation Pendennis involved the disruption of planned mass casualty attacks in Sydney and Melbourne in 2005-06 resulting in the arrest of 22 men, 18 of whom were convicted of terrorism offences.

30 ASIO, *Submission 12.1*, p. 34; Operation Neath involved the disruption of a planned attack on Holsworthy Barracks in Sydney in 2009, resulting in the arrest of 5 men, 3 of whom were convicted of terrorism offences.

full scope of the network of persons involved, with potentially 'disastrous' consequences.[31] ASIO provided the Committee with further, classified, evidence on the use of telecommunications data in these operations.

2.31 The Director-General of Security, Mr Duncan Lewis, also provided the Committee with a detailed explanation of how ASIO uses telecommunications data in the early stages of its investigations:

> When an individual comes to ASIO's attention, there are a range of methods that can be applied to establish whether that person's activities are relevant to security or not. Requesting historical communication data is often one of the most useful as well as one of the least intrusive methods of establishing those matters of fact. In many cases a simple subscriber check on a phone number is sufficient to determine that there is actually no investigation required and the matter can be put aside.[32]

2.32 Mr Lewis also highlighted the importance of reliable access to telecommunications data to counter-espionage investigations:

> Less known, of course, is the way in which historical communication data has been of assistance to us as we tackle the problems of counterespionage. We provided a submission to the committee which you have all seen, and I know one of my colleagues gave evidence in a closed session.[33]

2.33 The AFP explained in its submission that telecommunications data is a 'cornerstone of contemporary policing' and allows the AFP to:

- identify suspects and/or victims,
- exculpate uninvolved persons,
- resolve life threatening situations like child abduction or exploitation,
- identify associations between members of criminal organisations,
- provide insight into criminal syndicates and terrorist networks, and
- establish leads to target further investigative resources.[34]

2.34 The AFP advised that telecommunications data is accessed only on a 'case by case basis according to identified operational needs', and has provided fundamental information across the full suite of the AFP's investigative functions, including:

31 Ms Hartland, *Committee Hansard*, Canberra, 17 December 2014, p. 5.

32 Mr Duncan Lewis AO DSC CSC, Director-General of Security, ASIO, *Committee Hansard*, Canberra, 30 January 2015, p. 65.

33 Mr Lewis, *Committee Hansard*, Canberra, 30 January 2015, p. 64.

34 AFP, *Submission 7.1*, p. 3.

> counter terrorism, serious and organised crime, firearm and drug trafficking, child protection operations, cybercrime, crimes against humanity such as slavery, people smuggling and human trafficking, as well as community policing in the ACT and airports.[35]

2.35 At a public hearing, Commissioner Andrew Colvin provided further, detailed information about the AFP's use of telecommunications data in particular classes of investigations:

> Looking at AFP investigations commenced between July and September of this year, 2014, I can advise that telecommunications data has been used in 92 per cent of counterterrorism investigations, 100 per cent of cybercrime investigations, 87 per cent of child protection investigations and 79 per cent of serious organised crime investigations.[36]

2.36 Victoria Police highlighted to the Committee how changes in the broader communications environment are requiring agencies to rely on telecommunications data as an increasingly integral part of their investigations:

> In an age where there is an ever-increasing reliance across virtually all elements of our community on telecommunications in its various forms, coupled with increasingly sophisticated telecommunications technologies, law enforcement must be able to stay abreast of the tools of the trade or the modus operandi of the similarly empowered and sophisticated criminal element who are always amongst us.
>
> One of the touchstones of investigation that junior investigators are taught is the notion that every contact leaves its trace. In the past, this was intended to draw the investigator's attention to the possibilities of fibres, fingerprints and DNA evidence. In the present, this thinking is just as applicable to the opportunities provided to serious and organised crime investigators by metadata …
>
> An investigation can be considered to be a process underpinned by a series of logical and ordered steps, and the identification, analysis and interpretation of the traces that an offender has left behind in the course of his or her preparatory actions or actual offending will always be amongst the critical first steps that can ultimately determine the success or otherwise of an investigative

35 AFP, *Submission 7.1*, p. 3.

36 Commissioner Andrew Colvin, AFP, *Committee Hansard*, Canberra, 17 December 2014, p. 3.

> process, whether such traces are in the form of a fingerprint or a call charge record.[37]

2.37 The Australian Securities and Investments Commission (ASIC) highlighted the important role that telecommunications data plays in the initial stages of an investigation, and noted that the absence of such information can result in investigations failing before they truly even commence.[38]

2.38 Mr Michael Griffin, the recently-appointed Commonwealth Law Enforcement Integrity Commissioner, and a former Director of Military Prosecutions for the Australian Defence Force; Examiner of the Australian Crime Commission; and Principal Member, Senior Member and Member of the Administrative Appeals Tribunal, Migration Review Tribunal and Refugee Review Tribunal, and of the Veterans' Review Board, explained the role historic telecommunications data plays in anti-corruption investigations involving compromised law enforcement officials:

> I have had the benefit of being briefed on all of [the Australian Commission for Law Enforcement Integrity's] current operations as well as a number of past investigations. In my review of these cases, the thing that has struck me the most is the lengths to which corrupt officers will go to cover their tracks. Accordingly, telecommunications data is essential to finding corrupt conduct and can be crucial to its successful prosecution.
>
> …
>
> [T]he particular area of interest to us relates to people who are presently covering their tracks, and very recently covering their tracks. It is unlikely that the connections they have made will be present contemporaneously. Therefore, it is the historical record that is important to us, and looking at our history of investigations, we are of the view that the two-year period works for us. Although, as you will see from Operation Heritage-Marca, we have looked at historical data, where it has been available, that has gone back several years, indeed to 2006 in Operation Heritage-Marca.[39]

2.39 The AFP also drew the Committee's attention to the important role that telecommunications data plays in enabling and supporting the use of

---

37 Inspector Gavan Segrave, Intelligence and Covert Support Command, Victoria Police, *Committee Hansard*, Canberra, 30 January 2015, p. 44.

38 Australian Securities and Investments Commission (ASIC), *Submission 24*, p. 9.

39 Mr Michael Griffin AM, Integrity Commissioner, *Committee Hansard*, Canberra, 29 January 2015, pp. 34–35.

other investigative powers that Parliament has granted law enforcement and national security agencies:

> Intercepted or accessed content played a role in at least 328 convictions [by the AFP] over the past five years. In each of these cases telecommunications data was a crucial tool to ensure that those more intrusive capabilities were appropriately targeted and deployed.[40]

2.40 The New South Wales Police Force (NSW Police) also provided further evidence in support of the nexus between telecommunications data and telecommunications interception.[41]

What data is accessed?

2.41 Victoria Police emphasised to the Committee that the extensive use of telecommunications data at the early, intelligence stages of investigations should not be misinterpreted as agencies engaging in unjustified 'fishing expeditions':

> I think there is potential for some observers to misconstrue this idea of law enforcement using metadata in terms of intelligence. It needs to be tied back to an understanding of the investigative process … It is important for people to understand that in most instances metadata is used at the early stages of investigations when police are trying to get an understanding of a whole range of things in relation to the circumstances under investigation. I think this is what we mean when we talk about it being used in an intelligence sense, not that it is some broad fishing expedition because we have nothing better to do.[42]

2.42 South Australia Police explained to the Committee how the concepts of 'reasonable necessity' and 'relevance', which are core elements of the statutory test for authorised officers making a data authorisation under Chapter 4 of the TIA Act, are applied:

> The legislation talks about it being reasonably necessary and relevant. To me, if person A is murdered, who has had contact with that person in the previous 24 hours, 48 hours, seven days is quite relevant to that murder investigation, and that is what we are asking at that point in time. It is the same with a drug

40 AFP, *Submission 7.1*, p. 5.

41 Detective Superintendent Arthur Kopsias APM, Commander, Telecommunications Interception Branch, New South Wales Police Force, *Committee Hansard*, Canberra, 30 January 2015, p. 49.

42 Inspector Segrave, *Committee Hansard*, Canberra, 30 January 2015, p. 59.

> trafficker: whom that person has had contact with is relevant to that investigation.[43]

2.43 The Director-General of Security also drew the Committee's attention to how the limits and controls on ASIO's access to telecommunications data, which are contained in both the TIA Act and the *Attorney-General's Guidelines* made under section 8A of the *Australian Security Intelligence Organisation Act 1979*, are applied in practice:

> ASIO is careful to ensure that the level of intrusion into individual privacy remains proportionate to that threat and in accordance with the guidelines that were provided by the Attorney-General. It is not and will not be the case that ASIO automatically requests the maximum amount of data available. Should this bill become law, ASIO will continue to request access to historical communication data needed only for the purpose of carrying out our function, regardless of the length of time that data may be available for. We abide by the law.[44]

2.44 In response to a question from the Committee, a senior official of the Australian Commission for Law Enforcement Integrity (ACLEI) confirmed that access to historical telecommunications data would itself likely play a key role in any investigation by ACLEI of any alleged corrupt access to or misuse of telecommunications data by a law enforcement official.[45]

2.45 Telstra noted that there appear to be significant public misconceptions about the nature and extent of access to telecommunications data by Australian law enforcement and national security agencies:

> I think that there is often a lot of mystery around it. Very simply, it is often very simple metadata—the same sorts of information that you might be able to access from your bill: who you called; where you were when you made the call, by cell tower; a name and a billing address. I am sure people perceive that it is mysterious. It is actually, often—most times—very simple metadata.[46]

2.46 Telstra's statement is consistent with the Attorney-General's Department's submission to this inquiry,[47] and the AFP's submission to the Senate Legal and Constitutional Affairs References Committee's *Inquiry into the*

43 Assistant Commissioner Paul Dickson, Crime Service, South Australia Police, *Committee Hansard*, Canberra, 30 January 2015, p. 60.

44 Mr Lewis, *Committee Hansard*, Canberra, 30 January 2015, p. 65.

45 Mr Nick Sellars, Executive Director, Secretariat, Australian Commission for Law Enforcement Integrity, *Committee Hansard*, Canberra, 29 January 2015, p. 35.

46 Mrs Kate Hughes, Chief Risk Officer, Telstra, *Committee Hansard*, Canberra, 29 January 2015, p. 17.

47 Attorney-General's Department, *Submission 27*, p. 61.

Comprehensive Revision of the Telecommunications (Interception and Access) Act 1979.[48] This evidence indicates that approximately 85 per cent of data authorisations relate to subscriber information, such as name and address information, with only 15 per cent relating to 'traffic data', such as call charge records.

2.47 At a public hearing with the Committee, Victoria Police also highlighted that the number of data authorisations made each year by law enforcement agencies does not reflect the number of persons under investigation using those powers:

> **Inspector Segrave:** The numbers that have been put before you today, in terms of the applications, reflect the uptake of the broader community of the communications technologies that are available. Obviously, they have increased exponentially over time and the law enforcement figures just reflect that. The other point that I would make in relation to those numbers, certainly from a Victoria Police point of view—and I would be confident that that extends across other law enforcement agencies—is that it should not be interpreted that, if we have made 60 000 requests in a year, that is 60 000 individuals. A lot of the organised crime figures that are investigated and where these tools are utilised routinely drop phones and roll phones over, so there are multiple requests in relation to that. There may be multiple requests in relation to call charge records over periods of time, and so on. Another aspect that needs to be understood is that, if you were to drill down into those figures, the actual numbers, in terms of the individuals that are the subject of the applications, are much less than the bottom line figure—[49]

2.48 Victoria Police went on to confirm that there may be many hundreds of requests for telecommunications data for a single investigation that may only relate to 'half a dozen or a dozen individuals'.

> **Mr DREYFUS:** Can I reassure you, Inspector, on behalf of myself and my colleagues, that we have been given, in closed hearings, by the Australian Federal Police and ASIO, multiple examples of exactly what you are talking about. I am not disclosing anything here. For major investigations, there will be hundreds of requests for telecommunications data for a single investigation—
>
> **Inspector Segrave:** Indeed. That is the experience across—

48 AFP, *Submission 25*, Senate Legal and Constitutional Affairs References Committee, pp. 5–6.

49 Inspector Segrave, *Committee Hansard*, Canberra, 30 January 2015, p. 60.

> **Mr DREYFUS:** possibly only covering half a dozen or a dozen individuals, but nevertheless there are hundreds of requests. So, take it from me, and I think I can speak for my colleagues: we are not assuming—it is quite the reverse—that the 60,000 requests from your force or the 122,000 requests from New South Wales describe a number of persons. Far from it. [50]

A 'self-service' regime?

2.49 A number of submissions and witnesses argued that the existing controls in the TIA Act around access to telecommunications data are inadequate. For example, Professor George Williams argued that the current regime for access to telecommunications data is something of an accident of history, and that it should be reformed:

> my underlying concern is that I do not think the current system is appropriate, but I think it is somewhat accidental that we have got to this position where agencies can access vast amounts of data—tens of thousands, perhaps, over a number of years—without any form of clear political accountability. I think the scheme has grown up without actually being designed properly. And if we were starting fresh—let us say we did not have this data access that we have at the moment—I do not think there would be any doubt about the need to have some sort of authorisation process in play. It is just that we have this unfortunate ad hoc regime that I think we need to move beyond.[51]

2.50 The Law Council argued that the introduction of a mandatory data retention regime would increase the risks under an internal authorisation model for access to telecommunications data:

> under the proposed data retention regime, vastly more telecommunications data will be available – both in terms of volume and potentially the quality of the data retained – than is currently the case. This change heightens the risk of an encroachment on rights of privacy.[52]

2.51 The Committee accepts that the adequacy of safeguards around access to telecommunications data are relevant to the proportionality of the proposed data retention regime. Chapters 6 and 7 of this report address the controls and safeguards around telecommunications data in detail.

---

50 Inspector Segrave, *Committee Hansard*, Canberra, 30 January 2015, p. 60.

51 Professor Williams, *Committee Hansard*, Canberra, 30 January 2015, p. 11.

52 Law Council of Australia, *Submission 126*, p. 18.

The challenges facing national security and law enforcement investigations

2.52 The Government has indicated that it considers the implementation of a mandatory data retention regime to be an urgent priority to address challenges facing Australia's national security and law enforcement agencies.[53]

2.53 However, the Law Council of Australia argued that the Government has not demonstrated the urgency or pressing social need underpinning the Bill. The Law Council regarded the fact that 'certain features' of the Bill will not commence until six months after Royal Assent, and that the overall scheme will not be fully functional for a further 18 months after commencement, as indicating an absence of such an urgent need.[54]

2.54 In evidence, the Law Council went somewhat further, arguing that there is no evidence that the current regime was ineffective:

> [T]he examples [given] were examples where the metadata had been available under the existing voluntary regime. So that does not demonstrate the necessity of this new regime; it demonstrates that the existing regime is working.
>
> The difficulty is that submitters to this inquiry were asked to take on face value the statement that carriers are in fact reducing the amount of information that they retain such that the voluntary disclosure regime may become less effective over time. I do not think that that has been demonstrated in evidence or at least that I have seen in the submissions.[55]

2.55 Guardian Australia also noted the longstanding nature of the debate around mandatory data retention, including this Committee's consideration of the issue in 2012–13:

> Debate about interception, storage and use of Australians' communications for security and law enforcement purposes is longstanding, not a product of relatively recent concerns about a particular strain of terrorism.[56]

53 The Hon. Tony Abbott MP, Prime Minister, Transcript of Joint Press Conference with the Minister for Justice, the Hon. Michael Keenan MP and the Commissioner of the AFP, Mr Andrew Colvin APM OAM, 5 February 2015, Melbourne.

54 Law Council of Australia, *Submission 126*, pp. 6–7.

55 Mr Peter Leonard, Chairperson, Media and Communications Committee, Business Law Section, Law Council of Australia, *Committee Hansard*, Canberra, 30 January 2015, p. 31.

56 Guardian Australia, *Submission 132*, p. 3.

2.56 Mr Virgil Hesse cautioned the Committee against overreacting to recent events, such as the incidents in Sydney, Paris and Ottawa, when considering this proposal:

> Sadly recent events have left State and Federal Law Enforcement asking questions which in hindsight point to a breakdown across the Law Enforcement's and their ability to adequately monitor one individual who had intentions no one person could predict.
>
> I would ask the Committee to be very careful in reacting emotively with regard to this aberration when considering the third tranche of legislation, that being the Data Retention component.[57]

2.57 The Committee noted evidence that data retention would likely not have enabled agencies to prevent these incidents. NSW Police gave considered evidence on this point, emphasising that attempting to determine whether such information could have assisted in hindsight necessarily involves a hypothetical, counterfactual exercise:

> [A]s a hypothetical, with the nature of Sydney itself and where law enforcement would benefit from metadata in relation to, say, the Sydney incident, it most likely would not have prevented the Sydney incident. At the time, metadata could have been essential in trying to identify any other persons who may be engaged in a group or involved in that type of offence. Historical metadata could still benefit police down the track to see who that person has associated with in terms of a cell or, if they have been radicalised, where they come from.[58]

2.58 The Attorney-General's Department and a number of agencies noted that long-term changes in the telecommunications industry are impacting a number of key investigative capabilities. These changes are being exacerbated by an increasingly high-risk operational environment.

2.59 This section of the report will consider evidence received regarding:

- the declining ability of agencies to reliably access the content of communications,
- the declining ability of agencies to reliably access telecommunications data about communications, and
- the extent to which the current operational environment is exacerbating these challenges, increasing the urgency of the reform.

---

57 Mr Virgil Hesse, *Submission 15*, p. 1.

58 Assistant Commissioner Lanyon, *Committee Hansard*, Canberra, 30 January 2015, pp. 61–62.

Declining ability to reliably access the content of communications

2.60 The Attorney-General's Department noted that the ability of law enforcement and national security agencies to access the *content* of communications is in long-term decline, as a result of ongoing technological change. The Department claimed that this decline is degrading the ability of agencies to investigate serious threats, such as organised crime and terrorist cells. As a result, agencies are 'increasingly reliant on alternative investigative techniques, including access to telecommunications data'.[59]

2.61 NSW Police provided a valuable explanation of this challenge:

> It is a pretty broad topic but it is also very close to my heart as I have been the [telecommunications interception (TI)] commander for 15 years. I have been doing interceptions for 15 years. I have managed thousands and thousands of intercepts. But, in the last four or five years, the phrase 'going dark' has come about in terms of the strong encryption out there, lots of over-the-top providers providing apps, the online process. The advent of the internet, if I could explain it to you, has actually degraded our interception capability to the point where we are receiving a lot less than we used to receive.
>
> When I went to the [Telecommunications Interception Branch], I used to apply for the warrants. I used to go before Federal Court judges; in those days, we did not have AAT members. I used to go down with a request for the warrant, the same warrant that is served today, and present it before the member, present our case with the affidavit, come back with a warrant and serve it on the carrier. In those days, we had the luxury of one carrier. We would get all communications related to Mal Lanyon, say—everything. It was not a problem. It was easy. Any words spoken were what was said over the phone. The audio was easy to work out. But with the advent of the internet, although it is the same warrant today to the same member, there are about 600 or 700 potential ISPs and carriage service providers out there; and, when we serve the warrant, I am not getting the content, the communications, I used to get, to the point where we have to do other things—I cannot disclose those things in this forum—to complement the TI process.
>
> So we are exploring alternative methods of operational deployment and other forms of electronic surveillance services to fill in the gaps. There is a gap there. Encryption has become

59 Attorney-General's Department, *Submission 27*, p. 13.

> mainstream now, with the Snowden impact; we have over-the-top applications and the smartphones out there: all those things are impacting on us. I am not saying they are bad for the global community. I think there are some good things in there, but for us it is hard just to keep abreast.[60]

2.62 The Attorney-General's Department also noted that the relative value of telecommunications data to investigations is increasing as communications technology plays an increasing role in activities prejudicial to security, including cyber-espionage, and serious criminal activity.[61]

Declining ability to reliably access telecommunications data

2.63 The Attorney-General's Department noted that the ability of agencies to access telecommunications data is in long-term decline, reducing the value of data both as a primary investigative tool, and impairing the ability of agencies to mitigate the loss of capability they are experiencing as a result of the ongoing loss of access to the content of communications. The Committee identified this issue as a key challenge to national security investigations in its 2013 Report.[62]

2.64 The Department confirmed that this trend 'has continued unabated since the Committee's report, with further, significant reductions in the period for which certain service providers retain critical telecommunications data'.[63]

2.65 In its submission, the Attorney-General's Department drew a distinction between the increasing volume of telecommunications data being retained across the telecommunications industry, and retention practices in relation to particular categories of telecommunications data that are of any significant utility for national security and law enforcement purposes:

> It is important to distinguish between industry retaining telecommunications data in general, and retaining the types of telecommunications data that are critical to law enforcement and national security investigations. While it is true that, across the telecommunications industry, more telecommunications data is generated and retained than at any previous point in history,

60 Detective Superintendent Kopsias, *Committee Hansard*, Canberra, 30 January 2015, p. 56.

61 Attorney-General's Department, *Submission 27*, pp. 11–12.

62 PJCIS, *Report of the inquiry into potential reforms of Australia's national security legislation*, Canberra, May 2013, p. 190.

63 Attorney-General's Department, *Submission 27*, p. 13.

> much of this data is of limited, if any, investigative value and would not be subject to data retention obligations.[64]

2.66 The evidence received by the Committee over the course of this inquiry outlined two distinct challenges:

- a general decline in the availability of telecommunications data, and
- the inconsistent availability of telecommunications data for similar services provided by different providers, and between different services provided by the same provider.

Declining availability of telecommunications data

2.67 The AFP explained the challenge facing law enforcement agencies as a result of declining retention practices for critical categories of telecommunications data:

> Telecommunications data is a critical component of investigations and has been successfully used to support numerous investigations into serious criminality from many, many years. Industry already captures much of this data, but, as more services become available, providers are keeping fewer records for shorter periods of time.[65]

2.68 In his second reading speech to the House of Representatives following the introduction of the Bill, the Minister for Communications, the Hon Malcolm Turnbull MP, provided an example of the decline in retention practices and their potential to impact on national security investigations:

> Last year, a major Australian ISP reduced the period for which it keeps IP address allocation records from many years to three months. In the 12 months prior to that decision, the Australian Security Intelligence Organisation (ASIO) obtained these records in relation to at least 10 national security investigations, including counter-terrorism and cybersecurity investigations. If those investigations took place today, vital intelligence and evidence simply may not exist.[66]

2.69 In its submission, the Attorney-General's Department provided two specific examples where, since this Committee's 2013 report, major Australian service providers have substantially reduced their holdings of IP address allocation records and other critical data types. The Department advised that the impact of one of these changes is that, '[a]s a

64 Attorney-General's Department, *Submission 27*, p. 13.

65 Commissioner Andrew Colvin, *Committee Hansard*, Canberra, 17 December 2014, p. 3.

66 The Hon Malcom Turnbull MP, Minister for Communications, *House of Representatives Hansard*, 30 October 2014, p. 12561.

direct result of this action, agencies are unable to reliably identify suspects or execute interception warrants on this carrier's network.'[67]

2.70 Mr Chris Berg, Senior Fellow at the Institute of Public Affairs, summarised the challenge facing agencies in the following terms:

> The existing telecommunications data access regime takes advantage of a practice that telephone providers utilise for business purposes – the recording of data about the time, length, and parties to an individual telephone call. This information is retained in order to accurately bill customers, as telephone services are billed typically on a per-call basis or some variation of that system. From this data large amounts of information can be gleaned, but it is important to note that the data exists independently of its law enforcement uses. The data has been created by telecommunications providers for specific business purposes.
>
> In the internet era, this sort of data is both less important and less accessible. Communication that was once done by phone might be done over email, or in a chat room. Telephone calls which were logged on a per-call basis might be conducted over purely internet telephonic services like Skype. Rather than selling customers per-call access, now telecommunications is sold in large blocks of data. The only information needed for billing purposes with internet access might be download volumes. Even then that might not be necessary, either in the case of unlimited download plans or simply because excess downloads are 'shaped' – that is, offered freely at a reduced speed – rather than charged back to the customer.[68]

2.71 In its submission, ASIO provided a similar assessment of the underlying drivers of the decline in retention practices.[69]

2.72 Agencies provided a large number of case studies addressing situations where the non-retention of telecommunications data hampered law enforcement and national security investigations. For example, NSW Police explained to the Committee how changing industry retention practices are impacting on its investigations:

> There were only about 1 100 requests [for IP data in 2013–14], of which conservatively 80 per cent failed to yield a subscriber from

67 Attorney-General's Department, *Submission 27*, p. 16.

68 Mr Chris Berg, Senior Fellow, Institute of Public Affairs, *Submission 94*, p. 4.

69 ASIO, *Submission 12.1*, p. 20.

> the other end because, without the legislation, carriers are not required to keep the proposed data sets.
>
> Similarly, on metadata call charge records, investigators get very skilled at knowing which carriers they can get data from and which they cannot. They know very well, so the level of requests that go to carrier A, knowing that they only hold that data for four to six seeks, is obviously reduced. There is no point putting a request in if we know the carrier does not hold the data for that long.[70]

2.73 Similarly, South Australia Police explained how the inability to access 14-month old telecommunications data in a murder investigation hampered efforts to investigate a newly-identified suspect:

> A stalled murder investigation was reviewed about 14 months after the victim's death. Fresh information received during the review identified a suspect who was a known drug dealer. The victim, a regular drug user, had been in contact with the suspect and investigators suspect the victim may have been killed over a drug debt. Historical telecommunications data was sought for the suspect's mobile service for around the time of the murder but it was no longer available. The unavailability of the telecommunications data has been detrimental to the investigation and the case remains unsolved.[71]

2.74 The major service providers each provided the Committee with assurances that they do not currently intend to further reduce their retention practices.[72] For example, in response to a question as to whether there was any imminent proposal to reduce the data that it keeps, Telstra, responded:

> We have no proposals to substantially reduce our data holdings at this point in time. What we have at the moment is sufficient to meet our regulatory obligations and to manage our network and provide services to customers.[73]

2.75 However, these assurances must be viewed in light of the providers' further evidence that services providers are likely to release *new* services,

---

70 Assistant Commissioner Lanyon, *Committee Hansard*, Canberra, 30 January 2015, p. 49.

71 South Australia Police, *Submission 9*, p. 3.

72 Mr James Shaw, Director, Government Relations, Telstra, *Committee Hansard*, Canberra, 29 January 2015, pp. 18–19; Mr Matthew Lobb, General Manager, Industry Strategy and Public Policy, Vodafone Hutchison Australia (Vodafone), *Committee Hansard*, Canberra, 29 January 2015, p. 64; Mr David Epstein, Vice-President, Corporate and Regulatory Affairs, Singtel-Optus (Optus), *Committee Hansard*, Canberra, 30 January 2015, p. 21.

73 Mr Shaw, *Committee Hansard*, Canberra, 29 January 2015, pp. 18–19.

update the underlying architecture of their existing networks and services, and transition subscribers and communications onto IP-based platforms in the future. This may further reduce the availability of telecommunications data for national security and law enforcement purposes. For example, Telstra also explained that:

> As we change our business, as we introduce new products, or we might phase out an old system and introduce a new system—a new building platform or something, for instance—we would design that in order to meet business needs and whatever regulatory obligations there are. If that meant that we kept less data because we did not need to keep it, then that would be an artefact of that particular process.[74]

2.76 Similarly, Vodafone explained that, while it does not currently intend to reduce its retention practices in relation to its traditional telephony network, it expects that increasingly large volumes of communications will occur via newer, IP-based technologies. For these technologies, less telecommunications data is kept, and such data is kept for significantly shorter periods of time.[75]

2.77 Optus also observed that it is the migration of customers and services to newer platforms, which have shorter retention periods, that is driving down the overall period for which relevant telecommunications data is retained:

> I think the main influence on change and the overall character of the dataset, if you were to look at it in the very broad, is that increasingly communications are moving to mobile services and increasingly—even with what we would regard as voice communications between ourselves—they are in effect data, and that has an influence on how data is kept.[76]

Inconsistent availability of telecommunications data

2.78 The Committee received evidence from law enforcement agencies and ASIO that the *inconsistent* retention of data between providers, and between services offered by the same provider, poses a considerable challenge. That is distinct from the declining retention of critical telecommunications data across the industry.[77]

2.79 For example, Commissioner Colvin explained that:

74 Mr Shaw, *Committee Hansard*, Canberra, 29 January 2015, p. 14.

75 Mr Lobb, *Committee Hansard*, Canberra, 29 January 2015, p. 66.

76 Mr David Epstein, Vice-President, Corporate and Regulatory Affairs, Optus-Singtel (Optus), *Committee Hansard*, Canberra, 30 January 2015, p. 21.

77 For example, South Australia Police, *Submission 9*, p. 1.

> When the AFP are dealing with serious threats to national security and other serious crime, we cannot afford to rely on luck to see if the provider that the criminal has chosen to use has retained that data. I also do not think the public would consider that an acceptable outcome for serious criminal investigations.[78]

2.80 The AFP further explained that sophisticated criminals actively exploit the inconsistent retention practices between providers:

> We want standardisation. Also, we do not want the crooks to shop. We do not want them to go to the providers who they know keep the data—and it will not take long to work out who keeps the data and who does not keep the data. We do not want them to sit there and say, 'That's the best network to go if you are a criminal, because we know that they are not going to keep the IP addresses if it is dynamic. They are not going to keep it for any length of time. They might keep it for three months, because that is what their business model says, but beyond that that is fine. Why we do not go to one of the big ones at the moment is because they keep it for—for however long they keep it—a long period of time'. We do not want that to happen. We want a consistent model, so that we have a level playing field and the people we are trying to combat against also have a level playing field.[79]

2.81 The AFP confirmed that the risk of sophisticated criminals actively seeking out providers with more limited retention practices is not hypothetical, and is 'absolutely' occurring at present.[80]

2.82 Mr Chris Dawson, Chief Executive Officer of the Australian Crime Commission (ACC), explained the importance of reliable and consistent access to historic telecommunications data, noting that the ACC investigates 'complex communications webs which are often only able to be discovered through retrospective analysis of criminality which span at times many years.'[81]

2.83 ASIO provided a summary of its assessment of current industry retention practices, demonstrating their wide variability.[82] A copy of this table is included in the detailed discussion on retention periods in Chapter 4 of this report (Table 4.2).

---

78 Commissioner Andrew Colvin, *Committee Hansard*, Canberra, 17 December 2014, p. 3.

79 Deputy Commissioner Michael Phelan APM, Australian Federal Police, *Committee Hansard*, Canberra, 17 December 2014, p. 15.

80 Deputy Commissioner Phelan, *Committee Hansard*, Canberra, 17 December 2014, p. 15.

81 Mr Chris Dawson, Chief Executive Officer, Australian Crime Commission, *Committee Hansard*, Canberra, 17 December 2014, p. 6.

82 Australian Security Intelligence Organisation, *Submission 12.2*, p. 5.

2.84 Optus noted the current inconsistencies and the potential for these disparities to increase over time:

> [T]his regime is bringing everyone to a common set of standards. At the moment, probably the vast bulk of communications pass through the three major carriers in some form or another by means that are captured relatively well for the purpose of a regime like this one that we are discussing, but increasingly there is the potential for that to fragment. Indeed, people are always on the lookout for something. You will have seen media reports, for example, [about] drug syndicates and bikie gangs. There was a reason for that. Whether they can feel entirely confident of what they are up to is another thing, but they have clearly tried it on because they are of the belief that they can evade the protections that apply or the enforcement regime that applies in Australia through mainstream services.[83]

2.85 Optus went on to confirm that the concerns regarding the inconsistent retention of telecommunications data sought by law enforcement agencies did not just relate to the major carriers:

> I think it is a combination of a smaller part of the market, fragmentation in the market, technological alternatives and a broader change to what I would call crudely a data based regime for communications, rather than necessarily a traditional PSTN type voice regime.[84]

2.86 The level of inconsistency was most clearly highlighted by the evidence from Telstra, which confirmed that agencies' ability to access telecommunications data could vary significantly depending on which day of the year the request relates to:

> Some of the data that is being sought on a quiet day might be kept for a couple of weeks but on New Year's Eve is on the network for only a few hours.[85]

Higher risk operational environment

2.87 The Attorney-General's Department explained that the 'increasingly high-risk operational environment',[86] particularly the increased threat of domestic terrorism, has exacerbated the capability gaps experienced by agencies:

---

83 Mr Epstein, *Committee Hansard*, Canberra, 30 January 2015, pp. 21–22.

84 Mr Epstein, *Committee Hansard*, Canberra, 30 January 2015, p. 22.

85 Mr Shaw, *Committee Hansard*, Canberra, 29 January 2015, p. 14.

86 Attorney-General's Department, *Submission 27*, p. 12.

> [I]n an increased threat environment characterised by a higher operational tempo, there is a narrower margin for error in law enforcement and national security investigations. This narrower margin is particularly evident in relation to 'lone wolf' threats: such persons have limited, if any, contact with other known extremists, giving authorities fewer opportunities to detect their activities and intentions. As such, any missed opportunity to identify and prevent these attacks represents a significant risk.[87]

2.88 The Department noted that, where telecommunications data is not retained, it can result in missed opportunities:

> In the best case, agencies may be able to progress investigations by using more resource-intensive methods (limiting their capacity to investigate other matters) or more intrusive investigative techniques.
>
> In the worst case, a crime or threat to security will not be adequately investigated.[88]

2.89 ASIO's submission described the scale of the challenge it is facing to identify, investigate and prevent terrorist attacks in Australia at present:

> Presently, there are over 300 counter-terrorism investigations, of which a third are high threat priority cases. High threat cases are ones in which ASIO holds credible information requiring time critical action to resolve or monitor. The dominant theme across these cases is the conflicts in Syria and Iraq.[89]

2.90 The Attorney-General's Department also noted the increasing risk posed by cyber-espionage, and the importance of telecommunications data to combat that risk:

> Instances of espionage and foreign interference within Australia have continued to increase, both in terms of the number of occurrences and the range of operatives. In particular, the scale and sophistication of cyber-espionage conducted against Australian Government and private sector systems has increased significantly …
>
> … [A]ccess to telecommunications data and the lawful interception of… communications are often both crucial aspects of counter-espionage investigations.[90]

---

87 Attorney-General's Department, *Submission 27*, p. 15.

88 Attorney-General's Department, *Submission 27*, p. 15.

89 ASIO, *Submission 12.1*, p. 15.

90 Attorney-General's Department, *Submission 27*, pp. 11–12.

2.91 The Commissioner of ASIC highlighted the need for reliable access to telecommunications data to combat the increasing global threat of insider trading:

> It is not like terrorism, and I do not make a case that it is exactly the same as terrorism. That would be churlish and, frankly, stupid. But insider trading is an especially pernicious activity. If insider trading is permitted to continue, retail investors and institutional investors will lose confidence in the Australian market. Australia is a net importer of capital—a very major net importer of capital—and if foreign investors in particular, let alone Australian investors, lose confidence in our market, we lose this whole engine and multiplier effect that we have through our capital markets for efficient capital raising. … I am not equating this to a terrorist act, but I am equating this somewhat to other crimes which cause physical harm to people. It is very difficult for a person who has lost their life savings to recover, particularly if your are at that part of your life… where you do not have a lot of time to recover a deadweight loss.[91]

2.92 The Director-General of Security also addressed the question of whether the two-year implementation timeframe following the Bill receiving Royal Assent runs counter to the argument that the passage of the Bill is required to address these urgent operation pressures:

> We had a discussion internally about this. From the time of Royal Assent, there is no … backsliding in terms of the data that is being held by the telecommunication companies at that point.[92]

2.93 Additionally, the Attorney-General's Department's explained that one of the core objectives of the implementation planning arrangements proposed to be established by the Bill is to:[93]

> ensure that service providers achieve substantial compliance with their data retention obligations early in the implementation phase by encouraging interim data retention solutions, for example, by increasing storage capacity for existing databases to approach the two year retention period, or by prioritising the implementation of full data retention capability for some services or kinds of data.

2.94 The implementation arrangements for the proposed data retention scheme are discussed later in the report.

---

91 Mr Greg Tanzer, Commissioner, ASIC, *Committee Hansard*, Canberra, 29 January 2015, pp. 4–5.

92 Mr Lewis, *Committee Hansard*, Canberra, 30 January 2015, p. 69.

93 Attorney-General's Department, *Submission 27*, p. 34.

Reconciling data retention with privacy and civil liberties concerns

2.95 In May 2013, the previous Committee cautioned that:

> A mandatory data retention regime raises fundamental privacy issues, and is arguably a significant extension of the power of the state over the citizen. No such regime should be enacted unless those privacy and civil liberties concerns are sufficiently addressed.[94]

2.96 The Bill's Statement of Compatibility with Human Rights identifies that the proposed data retention regime would engage the right to protection against arbitrary or unlawful interferences with privacy, set out in Article 17 of the *International Covenant on Civil and Political Rights* (ICCPR) (referred to hereafter as the 'right to privacy'),[95] as well as the right to freedom of expression, set out in Article 19 of the ICCPR. The Australian Human Rights Commission supported this assessment.[96]

2.97 The Attorney-General's Department recently gave evidence to the Senate Legal and Constitutional Affairs References Committee summarising the effect of Australia's obligations under Article 17:

> Article 17 of the International Covenant on Civil and Political Rights sets out the right of persons to be protected against arbitrary or unlawful interference with their privacy. In order to avoid being arbitrary, any interference with privacy must be necessary to achieve the legitimate purpose and proportionate to that purpose.[97]

2.98 The Australian Privacy Commissioner, Mr Timothy Pilgrim PSM, drew the Committee's attention to the test put forward by the Office of the United Nations High Commissioner for Human Rights:

> The limitation must be necessary for reaching a legitimate aim, as well as in proportion to the aim and the least intrusive option available. Moreover, the limitation placed on a right (an interference with privacy, for example, for the purposes of

94 PJCIS, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, Canberra, May 2013, p. 190.

95 Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 [Data Retention Bill], *Explanatory Memorandum*, p. 10.

96 Australian Human Rights Commission, *Submission 42*, p. 4.

97 Ms Katherine Jones, Deputy Secretary, National Security and Criminal Justice Group, Attorney-General's Department, *Committee Hansard*, Senate Legal and Constitutional Affairs References Committee, Canberra, 2 February 2015, p. 44.

> protecting national security or the right to life of others) must be shown to have some chance of achieving that goal.[98]

2.99 The Law Council of Australia also endorsed this test.[99]

2.100 Mr Vaile and Mr Remati of the University of New South Wales discussed how the Committee should approach the question of whether the scheme is necessary and proportionate:

> Proportionality requires identification and weighting of benefits and costs or risks for the proposal, and for its realistic alternatives. We need to avoid considering benefits or costs in isolation, or overlooking whether an effective alternative with better proportionality exists.
>
> …
>
> 'Necessity' and 'effectiveness' are key factors on the benefits side. Consideration of the effectiveness of alternatives is also a necessary part of consideration of necessity.[100]

2.101 As the Australian Human Rights Commission also noted, the mere fact that a law interferes with privacy or freedom of expression does not make that interference disproportionate, nor does it make that law unjustified. In the Commission's view:

> Human Rights Law provides significant scope for [law enforcement and national security] agencies to have expansive powers, even where they impinge on individual rights and freedoms. Such limitations must, however, be clearly expressed, unambiguous in their terms, and legitimate and proportionate to potential harms.[101]

2.102 Following on from the 2013 report of this Committee, which emphasised the need to address privacy and civil liberties concerns raised by mandatory data retention, the following sections consider the evidence received by the Committee about the necessity, efficacy and proportionality of a data retention scheme as a response to the current risk environment.

---

98 Office of the Australian Information Commissioner, *Submission 92*, p. 4, quoting Office of the United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, UN Doc A/HRC/27/37 (30 June 2014), p. 23.

99 Dr Natasha Molt, Senior Policy Lawyer, Criminal Law, Law Council of Australia, *Committee Hansard*, Canberra, 30 January 2015, p. 32.

100 Mr Vaile and Mr Remati, *Submission 194*, p. 3.

101 Australian Human Rights Commission, *Submission 42*, p. 3.

Can data retention meet the test as being necessary for a legitimate aim?

2.103 The Explanatory Memorandum identifies that the legitimate aim, or aims, of a data retention scheme are:

> the protection of national security, public safety, addressing crime, and protecting the rights and freedoms … by requiring the retention of a basic set of communications data required to support relevant investigations.[102]

2.104 The Parliamentary Joint Committee on Human Rights has reported on the Bill, and concluded that, in relation to the question of necessity:

> the committee considers that the statement of compatibility has generally established why particular categories of data are considered necessary for law enforcement agencies.[103]

2.105 However, the Committee received a number of submissions questioning the necessity of mandatory telecommunications data retention.

2.106 The Law Council of Australia argued that:

> [T]he case for mandatory data retention has not been made out because:
>
> - the ability of access to telecommunications data is not limited to national security or serious crime;
> - there is little evidence from comparable jurisdictions that had previously had mandatory data retention schemes to suggest that such schemes actually assist in reducing the crime rate, for example in Germany, research indicates that a mandatory data retention scheme led to an increase in the number of convictions by only 0.006%;
> - there is a lack of Australian statistical quantitative and qualitative data to indicate:
>   - ⇒ the necessity of telecommunications data in securing convictions; or
>   - ⇒ the cases where requests for telecommunications data could not be met because data had not been retained and its effect on an investigation.[104]

2.107 In evidence, the Law Council acknowledged that the evidence provided by agencies 'definitely have the benefit of showing why agencies such as the AFP consider the value of telecommunications data', but argued that

---

102 Data Retention Bill, *Explanatory Memorandum*, p. 10.

103 Parliamentary Joint Committee on Human Rights, *Fifteenth Report to the 44th Parliament*, p. 12.

104 Law Council of Australia, *Submission 126*, p. 7.

'there seems to be a lack of statistical data that indicates the value of such data'.[105]

2.108 A number of submissions cited the report alluded to by the Law Council, which was prepared by the Legal Services of the German Parliament.[106] Extracts of this report have been translated by the German privacy rights group, AK Vorrat.[107] The report is stated to have addressed Germany's data retention regime, which was in force between 1 January 2008 and 2 March 2010, and concluded that data retention had increased 'crime clearance rates' by 0.006%.

2.109 In a joint submission, the councils for civil liberties across Australia accepted that 'telecommunications data is an important investigative tool that and law enforcement and security agencies should have appropriate access to it'.[108] However, the councils noted that they:

> share the scepticism of many experts, parliamentarians, legal and civil society groups that the mass collection and retention of telecommunications data of non-suspect citizens for retrospective access will significantly increase Australia's (or any nation's) safety from terrorism and serious crime.[109]

2.110 The councils further drew the Committee's attention to the United States' Privacy and Civil Liberties Oversight Board's January 2014 *Report on the Telephone Records Program*. That program involved the collection by the United States Government of large volumes of call-charge records (the time, date, duration and phone numbers) from some US phone companies.[110] The Board's headline conclusion, which was referenced by the councils, was that 'we are aware of no instance in which the program directly contributed to the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack.'[111] However, the Board also concluded that the program:

- identified one unknown terrorism suspect, although there was reason to believe that the Federal Bureau of Investigation (FBI) 'may have

105 Dr Natasha Molt, Senior Policy Lawyer, Criminal Law, Law Council of Australia, *Committee Hansard*, Canberra, 30 January 2015, p. 30.

106 See, for example: Law Institute of Victoria, *Submission 117*, p. 8; Mr Vaile and Mr Remati, *Submission 194*, p. 4.

107 Available at: <http://www.vorratsdatenspeicherung.de/content/view/534/55/lang,en/> viewed 26 February 2015.

108 Councils for civil liberties across Australia, *Submission 129*, p. 8.

109 Councils for civil liberties across Australia, *Submission 129*, p. 9.

110 Privacy and Civil Liberties Oversight Board, *Report on the Telephone Records Program*, p. 8.

111 Privacy and Civil Liberties Oversight Board, *Report on the Telephone Records Program*, p. 11.

discovered him without the contribution of the National Security Agency's program',

- provided additional leads regarding the contacts of terrorism suspects, and
- demonstrated that foreign terrorist plots did *not* have a US nexus, allowing the US intelligence community to avoid false leads and to channel its limited resources more effectively.[112]

2.111 The Board also indicated that the Telephone Records Program provided little additional value to the FBI's more 'traditional', targeted powers, noting that:

- US service providers are already subject to long-standing data retention obligations under Federal Communications Commission Regulations that cover the telecommunications data collected under the program, ensuring that those records are relatively consistently available to the FBI,[113] and
- the FBI (and other US law enforcement agencies) have the power to access those records under an 'administrative subpoena', similar to data authorisations made under the TIA Act, making it possible to 'streamline this process and eliminate delays' in accessing the telecommunications data retained by service providers.[114]

2.112 The Department drew the Committee's attention to the European Commission's *Evaluation Report on the Data Retention Directive (Directive 2006/24/EC)*, which concluded that:

- 'The European Union should support and regulate data retention as a security measure',
- 'The evidence… is limited in some respects, but nevertheless attests to the important role of retained data for criminal investigation', and
- 'These data provide valuable leads and evidence in the prevention and prosecution of crime and ensuring criminal justice. Their use has resulted in convictions for criminal offences which, without data retention, might never have been solved. It has also resulted in acquittals of innocent persons'.[115]

112 Privacy and Civil Liberties Oversight Board, *Report on the Telephone Records Program*, p. 11.

113 Privacy and Civil Liberties Oversight Board, *Report on the Telephone Records Program*, p. 141.

114 Privacy and Civil Liberties Oversight Board, *Report on the Telephone Records Program*, pp. 140–141.

115 European Commission, *Report from the Commission to the Council and the European Parliament: Evaluation Report on the Data Retention Directive (Directive 2006/24/EC)*, p. 31.

2.113 The Commission also criticised the use of 'crime clearance rates' as an appropriate methodology to evaluate the effectiveness of data retention (internal citations omitted):

> [C]rime statistics – including the number of crimes and the number of crimes which are solved ('clearances') - are determined by multiple socio-economic factors, and success in tackling crime cannot be attributed to a specific security measure, such as data retention. Police use different methods for measuring crime clearance rates and, moreover, it may be argued that an undue focus on such statistics can be counterproductive to the effectiveness of law enforcement. In any case, it would not be possible to identify meaningful statistical trends only a few years after the [Data Retention Directive] entered into force.[116]

2.114 While claiming data retention to be a necessary tool, representatives of South Australia Police and Victoria Police highlighted the complexities of assessing its direct impact on investigative outcomes:

> **Assistant Commissioner Dickson:** It is a very difficult question to answer. In jury matters, it is difficult to know why a jury found a person guilty, as an example. Was it because of the metadata provided? Was it because of certain admissions made? Or was it because of the DNA evidence? It is very difficult to say that metadata was the reason that that person was convicted. Most convictions at the end of the day are because of a whole raft of different things and bits of evidence.
>
> **Inspector Segrave:** I will make another point there, if I may. The metadata, quite often, is a step in the process to the investigator to get to the evidentiary footing. Without the metadata, that evidentiary footing may never be achieved. But it is not actually represented or recognised in the brief of evidence that is put before a court. So it can be very hard to drill down into the brief and into the prosecution to have an understanding of the underlying role that metadata actually places. But I think law enforcement consistently says that, with our understanding of the investigative process and the application of metadata within that process routinely, it is critical to us.[117]

2.115 In response to later questioning, NSW Police further emphasised the difficulty in producing meaningful quantitative analysis for the utility of access to retained data:

---

116 European Commission (2013), *Evidence for necessity of data retention in the EU*, p. 8.

117 *Committee Hansard*, Canberra, 30 January 2015, p. 49.

> I do not think there would be a police force in Australia that would keep that sort of data and, as Mr Dickson alluded to before, one of the issues is that it is rarely a single source of data that is responsible. For example, metadata might identify a source for us and might contribute to the way we go with the first steps of an investigation but there would be a number of other contributors. So to say that it was simply purely as a result for metadata would be a very problematic statistic to keep and I do not know of a police force which keeps that sort of information.[118]

2.116 The Committee received a range of evidence and case studies highlighting the impact that the absence of telecommunications data can have on investigative outcomes. This evidence supplements evidence previously received by this Committee in the course of its 2012–13 inquiry, and other publicly-available information on this issue, including evidence received by the Senate Legal and Constitutional Affairs References Committee.

2.117 The Attorney-General's Department drew the Committee's attention to analysis conducted by the German Federal Police of the utility of retained data to their investigations, which demonstrated that:

> [O]f the investigations in which telecommunications data was accessed, that telecommunications data provided the *only* investigative lead in 45.4% of cases. Telecommunications data made an 'important' contribution in 92.7% of the remaining cases.[119]

2.118 In its submission, the AFP provided an unclassified summary of the impact that current, inconsistent data retention practices had on the outcomes achieved by Operation Drakensberg, a major online child exploitation investigation that commenced in November 2013 following a referral from UK authorities. The referral contained 333 IP addresses suspected of accessing child exploitation material hosted on a UK-based website in 2011, as well as a further 219 IP addresses that had not actually performed any transactions. The non-retention of IP address allocation records by Australian service providers meant that the AFP were unable to even commence investigations into more than 45 per cent of the IP addresses identified as being highest-risk—those that had likely accessed the child exploitation material. Of the remaining cases, where service providers had retained IP address allocation records for up to two years,

118 Assistant Commissioner Lanyon, *Committee Hansard*, Canberra, 30 January 2015, p. 61.

119 Bundeskriminalamt, *Statistical analysis of data collection in the BkA*, p. 13, quoted in Attorney-General's Department, *Submission 27*, p. 14.

the AFP were able to positively identify 139 suspects, a success rate of almost 80 per cent.[120]

2.119 In its supplementary submission, the AFP advised the Committee that it received 5 617 reports of online child sexual exploitation relating to Australian IP addresses in 2014, a 54 per cent increase from the previous year. As at 9:00am on 27 January 2015, the AFP had received 709 reports this year. If that rate continues, the AFP would receive approximately 9 585 reports this year, an increase of almost 71 per cent.[121] The AFP drew to the Committee's attention the findings of a 2013 study by the United Kingdom's Child Exploitation and Online Protection Centre, that 'up to 85 per cent of online child sexual exploitation offenders have, or at some point, will contact offend against a child'.[122]

2.120 The AFP also noted the potential for reports from its international counterparts to be delayed, which would require the AFP to access more historic telecommunications data, as was the case in Operations Drakensberg:

> The time taken in respect of the referral of an online child sexual exploitation matter by an international partner of the AFP, and the investigation by the AFP, is dependent on the complexities of the matter, evidence available, technology used, volume of data and the results available from internet service providers.[123]

2.121 The Uniting Church in Australia's Justice and International Mission Unit of the Synod of Victoria and Tasmania (hereafter referred to as the Uniting Church Justice and International Mission Unit) drew the Committee's attention to the recommendations of the Asia-Pacific Financial Coalition Against Child Pornography that 'both for Internet Service Providers and file sharing companies, data retention and preservation are critical functions in the fight against child pornography'.[124]

2.122 The Unit also observed that:

> The Bill does not provide law enforcement agencies with any additional powers, nor does it give them any capacity to access metadata beyond what they already have. However, they cannot

120 AFP, *Submission 7.1*, p. 11.

121 AFP, *Submission 7.2*, p. 2.

122 AFP, *Submission 7.2*, p. 1.

123 AFP, *Submission 7.2*, p. 2.

124 Asia-Pacific Financial Coalition Against Child Pornography, *Confronting New Challenges in the Fight Against Child Pornography: Best Practices to Help File Hosting and File Sharing Companies Fight the Distribution of Child Sexual Exploitation Content*, September 2013, p. 4, quoted in Uniting Church Justice and International Mission Unit, *Submission 76*, p. 5.

> access the information if the company that has it has wiped it before the police are able to request it.[125]

2.123 It was also argued that data retention is necessary to assist in the protection and promotion of human rights.

2.124 For example, the Attorney-General's Department, in evidence to the Senate Legal and Constitutional Affairs References Committee, summarised the Australian Government's obligations under international human rights law to take positive steps to protect and promote fundamental human rights. The Department noted that this obligation is achieved in part through the maintenance of effective law enforcement and national security capabilities:

> International law to which Australia is a party recognises that Australians have a right to security of person, which requires the government to protect a person's physical safety and right to life. That means we must have an effective criminal justice system and the capacity to undertake preventative operational measures to protect people from the worst behaviour of others. The Australian Government also has an obligation to provide the right to an effective remedy for victims of crime. That means agencies need the investigative tools that will enable offenders to be brought to justice.
>
> The government believes that effective access to telecommunications data is critical to the government meeting those responsibilities. In investigating past crimes and deterring and preventing future crimes, Australia's agencies have come to rely heavily on telecommunications data. This should not be surprising, given how heavily the broader Australian population and the criminal element without our broader population have come to rely on communications technology … It is particularly necessary during the early stages of investigating crimes, where telecommunications data availability can often determine whether or not an investigation can succeed and the human rights of the victim can be protected.[126]

2.125 The Uniting Church Justice and International Mission Unit's submission contained a detailed review of Australia's human rights obligations in relation to online child exploitation. In particular, the Unit drew the

125 Uniting Church Justice and International Mission Unit, *Submission 76*, p. 9.

126 Ms Jones, *Committee Hansard*, Senate Legal and Constitutional Affairs References Committee, Canberra, 2 February 2015, p. 43.

Committee's attention to the United Nations Human Rights Council's Resolution A/HRC/8/L.17 of 12 June 2008, calling on governments:

> 2(g) To establish mechanisms, where appropriate, in cooperation with the international community, to combat the use of the Internet to facilitate trafficking in persons and crimes related to sexual or other forms of exploitation and to strengthen international cooperation to investigate and prosecute trafficking facilitated by the use of the Internet.[127]

2.126 The Unit then noted Australia's obligations under Articles 7, 8 and 17 of the ICCPR, Articles 16 and 34-36 of the *Convention on the Rights of the Child*, and Article 9 of the *Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography* to protect children from the cruel, degrading and inhuman treatment, sexual servitude, and violations of their privacy, honour and reputation associated with child exploitation, and argued that:

> The demonstrated likelihood that without data retention (as proposed in the Bill) hundreds, if not thousands, of offenders engaged in online child sexual abuse offences will escape detection and prosecution over time, should outweigh any concerns about the impact of data retention on the right to privacy.
>
> …
>
> It needs to be stressed that for the vast majority of Australians, law enforcement will never access the data retained under the requirements of the *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, so the Unit rejects the arguments that retaining data is a violation of the privacy rights of all Australians.[128]

2.127 Bravehearts argued that data retention represents a particular opportunity to improve conviction rates in relation to child sex offenders:

> [W]e know that trying to find evidence to prosecute sex offenders is very difficult. This is why we have such a low conviction rate, because it is such a difficult crime to prosecute. And this is an opportunity where there is actually evidence; the police can get evidence. And we would hate to see that squandered, because it is critical in terms of child protection that this metadata is retained

127 Uniting Church Justice and International Mission Unit, *Submission 76*, p. 10.

128 Uniting Church Justice and International Mission Unit, *Submission 76*, pp. 11–12.

> and that police have access to it in order that they can identify children who are at risk.[129]

2.128 Professor George Williams of the Gilbert + Tobin Centre of Public Law acknowledged the need for agencies to be able to intrude on individuals' privacy by accessing telecommunications data, but emphasised the need for appropriate safeguards to ensure that such access occurs only as part of a legitimate investigation.[130]

Can data retention meet the test as being effective for a legitimate aim?

2.129 As noted above, for a measure to be considered 'necessary' for a legitimate aim, it must be shown to have some chance of achieving that goal. That is, even where a measure is properly directed at a legitimate aim, it may not be regarded as 'necessary' if it produces second-order consequences that undermine its likely efficacy.

2.130 Mr Chris Berg, Senior Fellow at the Institute for Public Affairs argued that the existence of relatively easy-to-use counter-surveillance tools, such as Virtual Private Networks (VPNs), would undermine the value of data retention for law enforcement and national security purposes:

> The law enforcement value of data retention will be seriously eroded by the large scale VPN use. Any mildly sophisticated user is capable of setting up a VPN on their computer or mobile phone. Given that data retention is intended for 'serious crime' in the words of the prime minister, it is likely that any serious criminals will deploy VPNs or other data retention countermeasures to prevent law enforcement action. The Institute of Public Affairs has previously identified VPNs as a critical barrier to government internet policy in the domain of copyright infringement. Security and law enforcement agencies – like copyright holders – have to understand how technological adaptation will limit the efficacy of desired new powers.[131]

2.131 Communications Alliance, Mr Ben Johnston, and Mr Bernard Keane also highlighted this issue.[132]

---

129 Mrs Hetty Johnston AM, Chief Executive Officer, Bravehearts, *Committee Hansard*, Canberra, 30 January 2015, p. 1.

130 Professor Williams, *Committee Hansard*, Canberra, 30 January 2015, p. 9.

131 Mr Chris Berg, Senior Fellow, Institute of Public Affairs, *Submission 94*, p. 12.

132 Communications Alliance (CA) and the Australian Mobile Telecommunications Association (AMTA), *Submission 6*, p. 16; Mr Ben Johnston, *Submission 36,* pp. 1–2; Mr Bernard Keane, *Submission 37*, pp. 5–6.

2.132 The Attorney-General's Department addressed this argument, to the extent possible in public testimony, in evidence to the Senate Legal and Constitutional Affairs References Committee:

> I am sure you will appreciate that in this forum I need to be careful about talking about the capabilities of the agencies, but it is fair to say that notwithstanding that there is a variety of means by which those people who are engaged in criminal and security relevant activities might seek to engage and subvert any lawful access to their data or their activities, it remains the case … that data present a critical and unique tool and key lead piece of information in progressing their investigations.[133]

2.133 A number of law enforcement and national security agencies gave evidence that telecommunications data is used most frequently in complex investigations where agencies would be expected to routinely encounter suspects practicing counter-surveillance techniques, indicating that it remains of considerable value in such circumstances. The AFP provided evidence that telecommunications data has been used in all recent cybercrime investigations, which inherently tend to involve highly technologically-sophisticated criminals, as well as virtually all counter-terrorism, child protection and organised crime investigations, where suspects tend to adopt significant more advanced tradecraft than the average criminal.[134]

2.134 Similarly, ASIO gave evidence that it uses telecommunications data in its counter-espionage and cyber-security investigations, and emphasised that:

> the 10 per cent or the two per cent outside, at the longest length of retention, is actually the most crucial information that you are looking for in terms of networks and … in terms of particularly espionage cases and cyber cases.[135]

2.135 The Uniting Church Justice and International Mission Unit strongly opposed the argument that the uptake of counter-surveillance tools undermines the case for a data retention regime, noting that 'the argument… would appear to be that because some offenders may adapt their behaviour… the capacity of law enforcement should be permitted to be eroded.'[136] The Unit provided a detailed rebuttal of the argument, focusing in particular on the case of child exploitation:

---

133 Ms Anna Harmer, Acting First Assistant Secretary, Attorney-General's Department, *Committee Hansard*, Senate Legal and Constitutional Affairs References Committee, Canberra, 2 February 2015, p. 45.

134 Commissioner Andrew Colvin, *Committee Hansard*, Canberra, 17 December 2014, p. 3.

135 Ms Hartland, *Committee Hansard*, Canberra, 17 December 2014, p. 21.

136 Uniting Church Justice and International Mission Unit, *Submission 76*, p. 8.

> The argument is deeply flawed. While any improvement in tools for law enforcement to combat online criminal activity is likely to see some offenders adapt and use more sophisticated tools to avoid detection and capture, experience of law enforcement agencies is that many offenders do not adapt their behaviour and are more likely to get caught. The fact that many offenders engaged in extreme forms of online criminal activity do not currently make use of all the online tools available to them that would assist them in avoiding detection and capture is evidence that not all offenders have the knowledge or simply do not behave in a way that maximizes their ability to get away with their online criminal behaviour.
>
> For example, offenders who access child sexual abuse material do not appear as sophisticated as is often assumed. The [United Nations Office on Drugs and Crime] commented only 6% of offenders in one sample used encryption technology. In another sample, 17% used password protection, 3% evidence eliminating software and only 2% used remote storage systems. They note more sophisticated consumers could have evaded detection. However, such statistics serve as a warning that simply because a counter-strategy is technologically available does not mean that all offenders will avail themselves of the strategy.[137]

2.136 The Unit also drew the Committee's attention to the assessment of the Virtual Global Taskforce, which is an international coalition of law enforcement from 11 countries, as well as INTERPOL and Europol, dedicated to protecting children from sexual exploitation:

> [A]wareness is not the same as execution. Very few offenders are 100% secure all of the time or in all respects. The collecting impulse and sexual drive of offenders often prevents them from being as secure as they would like.
>
> Equally, offenders cannot entirely control the behaviour of others. Participating in online forums, while necessary to access newer material, was deemed by some respondents to be something of a risk in itself, even in those environments in which administrators enforce security standards. In this respect, anonymity is never absolutely assured.[138]

2.137 Communications Alliance noted that counter-surveillance tools may not entirely defeat agencies attempting to identify communications as part of a

137 Uniting Church Justice and International Mission Unit, *Submission 76*, p. 7.

138 Uniting Church Justice and International Mission Unit, *Submission 76*, p. 8.

lawful investigation,[139] and that the existence of such tools may in fact represent a further justification for data retention:

> Equally you could make the argument that because there are holes you should make the pieces you can cover as absolutely stringent as possible. That is not an argument we are advancing, but we think it is an issue worthy of considering in the overall picture.[140]

2.138 The European Commission's *Evaluation Report* also noted that, despite concerns expressed by civil society groups that the introduction of data retention could lead to people to change their communications behaviour, 'there is no corroboratory evidence for any change in behaviour having taken place in any Member State concerned or in the EU generally'.[141]

Can data retention meet the test as being proportionate for a legitimate aim?

2.139 The Committee received a number of submissions arguing that mandatory telecommunications data retention would constitute a disproportionate interference with the rights to privacy and freedom of expression. As noted above, the Statement of Compatibility with Human Rights confirms that the retention of telecommunications data constitutes an interference with the rights to privacy and freedom of expression. [142]

2.140 Dr Lesley Lynch, Secretary of the New South Wales Council for Civil Liberties, emphasised the value of privacy to individuals and society:

> [P]rivacy, like security, does matter; it is not a trivial consideration in the balancing equation. Serious intrusions into privacy have real consequences for persons and for societies, and that is what we are grappling with balancing in this context.[143]

2.141 Mr Chris Berg of the Institute of Public Affairs provided a more detailed explanation of the individual value of privacy:

> [W]e all require privacy to function and thrive. Let's start with the mundane. Obviously we desire to keep personal details safe – credit card details, internet passwords - to protect ourselves against identity theft. On top of this, we seek to protect ourselves against the judgment or observation of others. We close the door

139 Mr Stanton, *Committee Hansard*, Canberra, 17 December 2014, p. 39.

140 Mr Stanton, *Committee Hansard*, Canberra, 17 December 2014, p. 39.

141 European Commission, *Report from the Commission to the Council and the European Parliament: Evaluation Report on the Data Retention Directive (Directive 2006/24/EC)*, p. 26.

142 Data Retention Bill, *Explanatory Memorandum*, p. 14.

143 Dr Lesley Lynch, Secretary, New South Wales Council for Civil Liberties, *Committee Hansard*, Canberra, 30 January 2015, p. 79.

> to the bathroom. We act differently with intimates than we do with colleagues. We often protect our thoughts, the details of our relationships, our preferences, from prevailing social norms. We compartmentalise. How many people would be uncomfortable with a colleague flipping through their mobile phone – with the window into a life that such access would provide?[144]

2.142 Mr Berg also explained the value of a broad construction of freedom of speech, and the relationship between privacy and freedom of expression, insofar as 'the threat or actuality of government surveillance may psychologically inhibit freedom of speech',[145] arguing that:

> The potential of surveillance – and there is no doubt that the data retention bill threatens to inculcate a culture of being under surveillance, given its possible breadth and future expansion – to limit freedom of speech is significant. Once the government has introduced this legal regime it is, barring future judicial oversight, unlikely to be repealed, and almost certain to be extended. The so-called 'balance between liberty and security' is only ever moved in favour of security.[146]

2.143 The Victorian Commissioner for Privacy and Data Protection argued that 'the wide scale collection of metadata is an unjustified infringement on human rights',[147] and that retained data would:

> 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.[148]

2.144 Mr Jon Lawrence, of Electronic Frontiers Australia and the Australian Privacy Foundation, made similar arguments.[149]

2.145 Mr Lawrence also drew the Committee's attention to the conclusion of the Court of Justice of the European Union, in its decision in *Digital Rights Ireland*, that, where telecommunications data is required to be retained:

---

144 Mr Chris Berg, Senior Fellow, Institute of Public Affairs, *Submission 94*, p. 8.

145 Quoting G.L. White and P.G. Zimbardo, *The chilling effects of surveillance: Deindividuation and reactance*, Office of Naval Research, 1975.

146 Mr Chris Berg, Senior Fellow, Institute of Public Affairs, *Submission 94*, p. 10.

147 Commissioner for Privacy and Data Protection (Victoria), *Submission 39*, p. 9.

148 Commissioner for Privacy and Data Protection (Victoria), *Submission 39*, p. 8.

149 Mr Jon Lawrence, Executive Officer, Electronic Frontiers Australia, *Committee Hansard*, Canberra, 29 January 2015, p. 21; Australian Privacy Foundation, *Submission 75*, p. 1.

> Those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary place of residence, daily or other movements, the activities carried out, the social relationships of those persons, and the social environments.[150]

2.146 Dr David Lindsay, Vice Chair of the Australian Privacy Foundation, argued that the Bill is disproportionate, and a 'sledgehammer that unjustifiably breaches the right to privacy who are overwhelmingly neither criminals nor terrorists'. Dr Lindsay cited a report of the Office of the UN High Commissioner for Human Rights, which states that:

> Concerns about whether access to and use of data are tailored to specific legitimate aims… raise questions about the increasing reliance of Governments on privacy sector actors to retain data 'just in case' it is needed for government purposes. Mandatory third-party data retention – a recurring features of surveillance regimes in many States, where Governments require telephone companies and Internet service providers to store metadata about their customers' communications and location… - appears neither necessary nor proportionate.[151]

2.147 The Committee noted that the following paragraph of the Office's report went on to list 'factors that must be taken into account in determining proportionality' in relation to 'bulk data' programs, such as data retention.[152] Similarly, the preceding paragraph, which discussed the mass collection of communications or telecommunications data by government agencies (as opposed to third-party data retention) states that:

> Where there is a legitimate aim and appropriate safeguards are in place, a State might be allowed to engage in quite intrusive surveillance; however, the onus is on the Government to demonstrate that interference is both necessary and proportionate to the specific risk being addressed.[153]

---

150 *Digital Rights Ireland v Ireland*; *Kärtner Landesregierung, Seitlinger and Tschohl* (joined cases C-293/12 and C-594/12, Court of Justice of the European Union, 8 April 2014), [27].

151 Office of the United Nations High Commissioner for Human Rights, *Right to Privacy in the Digital Age*, A/HRC/27/37 (30 June 2014), [27], quoted by Dr David Lindsay, Vice-Chair, Australian Privacy Foundation, *Committee Hansard*, 30 January 2015, p. 77; the Law Institute of Victoria also referred the Committee to this paragraph of the report in *Submission 117*, p. 14.

152 Office of the United Nations High Commissioner for Human Rights, *Right to Privacy in the Digital Age*, A/HRC/27/37 (30 June 2014), [28].

153 Office of the United Nations High Commissioner for Human Rights, *Right to Privacy in the Digital Age*, A/HRC/27/37 (30 June 2014), [26].

2.148 Emeritus Professor Gillian Triggs, President of the Australian Human Rights Commission, drew a distinction between the magnitude of the privacy intrusion associated with *access* to telecommunications data by law enforcement and national security agencies, which she characterised as 'powerful',[154] compared to the mandatory *collection* and *retention* of telecommunications data by a third-party service provider, which she characterised as 'small'.[155]

2.149 Mr Peter Leonard, from the Law Council of Australia, supported this distinction:

> The fact that data is retained about me is not, of itself, pervasive surveillance, but it does enter into the balance between those three rights—that if there is a risk that data may be used to undermine the other rights that I should enjoy, then that should be assessed in determining the proportionality of the data retention. So I think it is necessary to look, firstly, at the data retention, and balance its effect on other rights before we got to the question of proportionality as to how the data is used.[156]

2.150 Mr Leonard went on to argue that whether telecommunications data should be retained and, if so, how much and for how long, are less significant issues than questions about the types of safeguards that should apply to protect that data from being improperly accessed or misused.[157]

2.151 The Statement of Compatibility with Human Rights, which accompanies the Bill, notes that the proportionality of data retention cannot be considered in isolation from the purposes for which retained data can be lawfully used, and the safeguards that exist around the access to and use of such data:

> The Bill permissibly limits an individual's privacy in correspondence (telecommunications) in a way which is reasonable and proportionate by circumscribing the types of telecommunications data that are to be retained by service providers to the essential categories of data required to advance criminal and security investigations, permitting access to telecommunications data only in circumstances prescribed by existing provisions in the TIA Act and moreover reducing the range of agencies who may access data under those provisions.[158]

154 Professor Triggs, *Committee Hansard*, Canberra, 29 January 2015, p. 76.

155 Professor Triggs, *Committee Hansard*, Canberra, 29 January 2015, p. 78.

156 Mr Leonard, *Committee Hansard*, Canberra, 30 January 2015, p. 34.

157 Mr Leonard, *Committee Hansard*, Canberra, 30 January 2015, p. 35.

158 Data Retention Bill, *Explanatory Memorandum*, p. 11.

2.152 The Privacy Impact Assessment for the Bill notes that 'the kind of information that may be prescribed does not go beyond that which service providers are already generating to provide services, albeit that some service providers may not be recording the information or keeping it for very long',[159] and ultimately concludes that:

> we have concluded that the proposed changes set out in the draft Amendment Bill do not appear to have significant privacy implications.[160]

2.153 Dr Roger Clarke, Immediate Past Chair of the Australian Privacy Foundation, disagreed with Professor Triggs' and Dr Leonard's assessment that data retention, of itself, involves a small intrusion on privacy and is not pervasive surveillance:

> [T]his is mass surveillance that is to be imposed by the parliament on the Australian people. We have skirted around that and never used the word. There has been mention of personal surveillance—the collection of data about individuals who come to attention and about whom there is reasonable suspicion et cetera. That has been mentioned in passing. But this moves way, way beyond that, to mass surveillance.[161]

2.154 Professor Williams, while supporting data retention, emphasised that the fact that data retention will potentially apply to all Australians' communications is an important distinguishing factor from other law enforcement and national security measures, and emphasised the need for appropriate safeguards.[162]

2.155 In its submission, ASIO argued that the view that telecommunications data is, or will be, used for 'mass surveillance' is a misconception. In particular, ASIO advised the Committee that:

- ASIO does not engage in 'large-scale mass gathering of communications data', and that it 'does not have the resources, the need, or the inclination' to do so, and

---

159 Australian Government Solicitor, *Privacy Impact Assessment: Proposed amendments to the Telecommunications (Interception and Access) Act 1979*, 15 December 2014, p. 15 (appended to Attorney-General's Department, *Submission 27*).

160 Australian Government Solicitor, *Privacy Impact Assessment: Proposed amendments to the Telecommunications (Interception and Access) Act 1979*, 15 December 2014, p. 25 (appended to Attorney-General's Department, *Submission 27*).

161 Dr Roger Clarke, Immediate Past Chair, Australian Privacy Foundation, *Committee Hansard*, 30 January 2015, p. 78; see also, Dr Clarke, *Committee Hansard*, Senate Legal and Constitutional Affairs References Committee, 2 February 2015, p. 20.

162 Professor Williams, *Committee Hansard*, Canberra, 30 January 2015, p. 9.

- at most, a few thousand people come to ASIO's attention each year as part of security investigations, inquiries and leads that may require access to telecommunications data.[163]

2.156 In her submission, the Inspector-General of Intelligence and Security (IGIS) advised that the Attorney-General's Guidelines for ASIO require, among other things, that:

- any means used by ASIO for obtaining information must be proportionate to the gravity of the threat posed and the probability of its occurrence, and
- inquiries and investigations into individuals and groups must be undertaken using as little intrusion into individual privacy as is possible, consistent with the performance of ASIO's functions.[164]

2.157 As noted earlier, the Director-General of Security explained to the Committee how the legal restrictions contained in the Guidelines are applied in practice:

> It is not and will not be the case that ASIO automatically requests the maximum amount of data available. Should this bill become law, ASIO will continue to request access to historical communication data needed only for the purpose of carrying out our function, regardless of the length of time that data may be available for. We abide by the law.[165]

2.158 The IGIS confirmed that her Office inspects ASIO's access to and use of both historic and prospective telecommunications data, that there is a high rate of compliance in this area, and that she had not identified any concerns with ASIO's access to such information.[166]

2.159 Professor Triggs challenged the view that telecommunications data is less privacy sensitive than the content of communications, noting that:

> A great deal can be learned from metadata. Indeed, in many cases, more can be learned from metadata than can be learned from content, especially as many people are extremely cautious about content but forget that it is the metadata that can actually lead law enforcement agencies to a paedophile ring, to a terrorist group or to serious criminals.[167]

163 ASIO, *Submission 12.1*, p. 10.

164 IGIS, *Submission 131*, p. 6.

165 Mr Lewis, *Committee Hansard*, Canberra, 30 January 2015, p. 65.

166 IGIS, *Submission 131*, p. 5.

167 Professor Triggs, *Committee Hansard*, Canberra, 29 January 2015, p. 71.

2.160 However, the Explanatory Memorandum argues that telecommunications data is less privacy sensitive than the content of communications.[168] The Bill's Statement of Compatibility with Human Rights also identifies that the degree of this interference differs in relation to various elements of the proposed data set. For example, the Statement identifies that

> subscriber data, as the predominant data category which would be generated through the collection of customer information, raises relatively fewer privacy implications than traffic and location data comparators.[169]

2.161 The Attorney-General's Department, in its supplementary submission, drew the Committee's attention to the conclusion of the Court of Justice of the European Union that:

> even though the retention of data required by Directive 2006/24 constitutes a particularly serious interference with those rights, it is not such as to adversely affect the essence of those rights given that, as follows from Article 1(2) of the directive, the directive does not permit the acquisition of knowledge of the content of the electronic communications as such.[170]

2.162 Professor Williams noted that, 'I do think there are different degrees of information… I think there is a clear distinction between the stored communications as to content and metadata.'

2.163 However, Professor Williams also observed that:

> I think the community is sending a pretty strong signal to your committee that they do see this information as sensitive. You only need to look at the public debate and the public reaction about this to see that the community does not see this as ordinary information but is actually very concerned as to the circumstances in which government agencies would access it.[171]

2.164 A number of submissions and witnesses argued that the Government should consider less privacy-intrusive alternatives to data retention.[172]

2.165 Mr Vaile and Mr Remati drew the Committee's attention to a recent report of the US National Research Council, entitled *Bulk Collection of Signals*

---

168 Data Retention Bill, *Explanatory Memorandum*, p. 3.

169 Data Retention Bill, *Explanatory Memorandum*, p. 14.

170 Attorney-General's Department, *Submission 27.2*, p. 9, referring to *Digital Rights Ireland v Ireland*; *Kärtner Landesregierung, Seitlinger and Tschohl* (joined cases C-293/12 and C-594/12, Court of Justice of the European Union, 8 April 2014), [39].

171 Professor Williams, *Committee Hansard*, Canberra, 30 January 2015, p. 8.

172 See, for example: Privacy International, *Submission 80*, p. 11; Mr Lawrence, *Committee Hansard*, Canberra, 29 January 2015, p. 22.

Intelligence: Technical Options.[173] The report, released on 15 January 2015, evaluated whether viable alternatives existed to the bulk collection of signals intelligence by US intelligence agencies, and concludes that:

> there are no technical alternatives that can accomplish the same functions as bulk collection and serve as a complete substitute for it; there is no technological magic.[174]

2.166 Some submitters argued that viable alternatives existed to a mandatory data retention regime, such as the use of the existing preservation notice regime under Part 3-1A of the TIA Act. The Australian Privacy Foundation argued that:

> [I]n proposing a mandatory blanket data retention regime, the government has given insufficient consideration to the potential benefits of a targeted data preservation regime, in which relevant agencies may selectively require the preservation of telecommunications data, provided always that satisfactory procedural safeguards are met … In any case, no consideration appears to have been given to the merits of adapting and extending a regime such as the Chapter 3 preservation notice regime, to appropriately apply to the preservation of non-content telecommunications data.[175]

2.167 Similarly, Mr Keane argued that agencies could currently use these notices to preserve telecommunications data as an alternative to data retention:

> The 'going dark' argument is further undermined by the fact that ASIO simply doesn't use existing tools designed explicitly to enable data retention.
>
> For two years, ASIO, the AFP and state police forces have had the power, under the *Cybercrime Legislation Amendment Act 2012*, to require communications companies to store information that may help in the investigation of a 'serious contravention' — an offence punishable by three years or more in jail — for up to 90 days before getting a warrant to access the data. The only limitation on the requests apart from the seriousness of the offence is that it

173 Mr Vaile and Mr Remati, *Submission 194*, p. 8.

174 United States National Research Council, *Bulk Collection of Signals Intelligence: Technical Options*, pp. 4–5; The Committee notes that the report primarily concerns foreign intelligence collection by US Government agencies, as quite distinct from the Government's proposal to require Australian telecommunications companies to keep records at arms-length from Australian agencies. Nevertheless, much of the Council's core analysis around the utility of retaining information and possible alternative approaches is relevant to this Committee's consideration of the Bill.

175 Australian Privacy Foundation, *Submission 75*, p. 30.

> must be targeted at one person, but an agency can issue as many preservation notices as necessary.[176]

2.168 Mr Berg raised the question of whether any inadequacies within the preservation notice regime could be rectified, as an alternative to implementing data retention.[177]

2.169 This Committee previously received evidence from the Attorney-General's Department about whether preservation notices are a viable alternative to data retention as part of its *Inquiry into potential reforms of Australia's national security legislation*:

> Data preservation involves a [carrier or carriage service provider (C/CSP)] preserving specific telecommunications data identified by an agency that it has available on its network in relation to a relevant investigation or intelligence gathering activity on notification by an agency. Given the current authority under the TIA Act for agencies to access telecommunications data from a C/CSP when it has been identified as being relevant to a specific investigation or intelligence gathering activity, agencies already have the ability to access telecommunications data that the C/CSP has on hand at the time of the request or that comes into existence into the future, negating the need for data preservation.[178]

2.170 The Department's submission to this inquiry contained further discussion on this issue.[179] In particular, the Department explained that such notices, which are currently issued under Part 3-1A of the TIA Act ('Preserving stored communications') apply only to 'stored communications', such as emails and SMS messages, and the associated telecommunications data.[180] This is consistent with the Department's previous evidence to the Joint Select Committee on Cyber-Safety that preservation notices apply only to 'stored computer data', as defined in the *Convention on Cybercrime* and which equates to 'stored communications' under the TIA Act.[181]

---

176 Mr Bernard Keane, *Submission 37*, p. 7.

177 Mr Chris Berg, Senior Fellow, Institute of Public Affairs, *Submission 94*, p. 13.

178 Attorney-General's Department, *Submission 218 to the Inquiry into potential reforms of Australia's national security legislation*, p. 8, quoted at p. 163 of the *Report of the inquiry into potential reforms of Australia's national security legislation*.

179 Attorney-General's Department, *Submission 27*, pp. 17–18.

180 TIA Act, section 107J.

181 See: Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, Joint Select Committee on Cyber-Safety, 1 August 2011, p. 31; Mr David Cramsie, Senior Legal Officer, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, Joint Select Committee on Cyber-Safety, 1 August 2011, p. 32.

2.171 The Department acknowledged that the preservation notice regime could be amended or expanded, as suggested by Mr Berg, but argued that while preservation notices could complement data retention, they would not be a substitute for it:

> The purpose of preservation notices is to 'quick freeze' volatile or perishable electronic evidence that a provider possesses for a short period of time, to allow agencies time to apply for and obtain a warrant to access that information. Evidence cannot be preserved if it was never retained, or if it has already been deleted.
>
> …
>
> As such, data retention is in fact a prerequisite to preservation of data, rather than preservation offering an alternative to retention.[182]

2.172 The Director-General of Security provided the Committee with his views about the circumstances in which preservation notices are, and are not, of use to ASIO:

> It is something we use and it is absolutely the case that if we were aware that something was likely to happen that you can in fact put in place a preservation order around that particular set of circumstances to understand it better going forward. But all of that of course is prospective. Your earlier question… is a retrospective issue and retrospectivity is a different set of issues here.[183]

2.173 The Australian Commission for Law Enforcement Integrity (ACLEI) drew the Committee's attention to the fact that preservation notices are of limited value, in particular, as part of anti-corruption investigations:

> ACLEI notes that data retention alternatives, such as preservation notices, are currently available under the TIA Act. However, ACLEI's experience is that these alternatives are most relevant when it is desirable to ensure preservation of future information, such as when a person is under investigation and is likely to commit further crimes. Preservation of past data is entirely limited to the carrier's business practices.
>
> The nature of corruption – particularly in a law enforcement context where officers are more aware of surveillance limitations and able to defeat them – means that relevant conduct is covert and may not come to light for some months or years after the event. It follows that preservation notices cannot assist an

182 Attorney-General's Department, *Submission 27*, p. 17.

183 Mr Lewis, *Committee Hansard*, Canberra, 30 January 2015, p. 69.

> investigation if the data sought has already been deleted by the carrier.[184]

2.174 The AFP also argued that, without data retention, agencies would frequently lack the necessary information to identify a suspect and serve a preservation notice, rendering the preservation notice power 'ineffective' in many situations:

> In many instances, the role that data place in the early stages of investigations is to assist in attribution: that is, data is a crucial tool in identifying the suspect in a criminal act or event, and in clearing other persons from suspected involvement. Where this data is unavailable because it has not been retained, investigations have been unable to progress.[185]

2.175 The US National Research Council's report considered the comparative value of retained data compared to targeted collection or preservation:

> If past events become interesting in the present for understanding new events… historical facts and the context they provide will be available for analysis only if they were previously collected.
>
> …
>
> Targeted collection provides data only on present and future actions of parties of interest at the time of collection, but not their past activities.[186]

2.176 In its submission, the Department drew the Committee's attention to a number of international evaluations of whether preservation notices are a viable substitute for data retention, including the Council of Europe's *Assessment Report: Implementation of the preservation provisions of the Budapest Convention on Cybercrime*,[187] the European Commission's *Evidence of the Potential Impacts of Options for Revising the Data Retention Directive: Current approaches to data preservation in the EU and in third countries*,[188] and the Netherlands Government's *The Dutch implementation of the Data Retention Directive*.[189] Each of these reports concluded that preservation notices are not a substitute for accessing existing telecommunications data.

184 Australian Commission for Law Enforcement Integrity, *Submission 48*, p. 8.

185 AFP, *Submission 7.1*, p. 13.

186 United States National Research Council, *Bulk Collection of Signals Intelligence: Technical Options*, p. 4-1.

187 Council of Europe, *Assessment Report: Implementation of the preservation provisions of the Budapest Convention on Cybercrime*, 2012, pp. 75-76.

188 European Commission, *Evidence of the Potential Impacts of Options for Revising the Data Retention Directive: Current approaches to data preservation in the EU and in third countries,* 2012, pp. 22-23.

189 Netherlands Government, *The Dutch implementation of the Data Retention Directive,* 2014, pp. 110–111.

2.177 As noted above, Mr Leonard of the Law Council argued that the available evidence shows that existing arrangements for the retention of telecommunications data by service providers are adequate for the purposes of national security and law enforcement investigations.[190]

2.178 Similarly, the Australian Interactive Media Industry Association (AIMIA) Digital Policy Group (DPG) argued that:

> law enforcement are not fully utilising the data that is currently available to them, particularly metadata that is publicly available. The DPG members expect that law enforcement should make full use of such information before embarking on a fishing expedition by requiring businesses to retain data for a defined period of time.[191]

2.179 The substance of this issue is largely addressed in the preceding discussion about the necessity of data retention. However, the Attorney-General's Department, in evidence to the Senate Legal and Constitutional Affairs References Committee, observed that:

> [A] number of commentators I think have referred to the existing practices of industry in retaining telecommunications data and that that provides an avenue to avail agencies of the data that they need to conduct investigations. In that regard, the key thing that we would note is that telecommunications industry practices are changing and that they are changing at a rapid rate. A number of providers have indicated in evidence before committees, most recently the PJCIS, the fact that they have significant gaps in their holdings of data, particularly in relation to more modern telecommunications services as opposed to traditional telephony services. And of course the range of service s is constantly changing and their business practices are being driven by the profitability of their particular companies. They are driven by commercial needs rather than the needs of law enforcement and security agencies. So the alignment between what has historically been a coincidence between the business practices of the telecommunications industry and the needs of law enforcement and security agencies is moving apart and that is why there is in part the need to address the retention of telecommunications data.[192]

190 Mr Leonard, *Committee Hansard*, Canberra, 30 January 2015, p. 31.

191 AIMIA Digital Policy Group, *Submission 34,* p. 5.

192 Ms Harmer, *Committee Hansard*, Senate Legal and Constitutional Affairs References Committee, Canberra, 2 February 2015, pp. 44–45.

2.180 In evaluating the proportionality of a data retention regime for national security and law enforcement purposes, the Committee received a range of evidence on comparable international regimes. As the Committee has noted above, Australia's human rights obligations at international law derive from, among other instruments, the International Covenant on Civil and Political Rights. Nevertheless, the reasoning of the Court of Justice of the European Union, in its decision in *Digital Rights Ireland*, provides useful guidance for evaluating the proportionality of a proposed data retention scheme:

> [A]ny limitation on the exercise of the rights and freedoms laid down by the Charter must be provided for by law, respect their essence and, subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others. [193]

2.181 The Court went on to conclude that the form of data retention established by the Data Retention Directive (upon which the Bill is based):

- was provided for by law,
- respected the essence of the right to privacy, as it did not 'permit the acquisition of knowledge of the content of electronic communications', [194]
- respected the essence of the right to the protection of personal data, as Member States were required under separate EU Directives to 'ensure that appropriate technical and organisational measures are adopted against accidental or unlawful destruction, accidental loss or alternation of the data', [195] and
- 'genuinely satisfie[d] an objective of general interest', namely being to contribute to public security through the fight against international terrorism, the maintenance of international peace and security, the fight against crime and, in particular, organised crime, and the promotion of the right of any person to security. [196]

---

193 *Digital Rights Ireland v Ireland*; *Kärtner Landesregierung, Seitlinger and Tschohl* (joined cases C-293/12 and C-594/12, Court of Justice of the European Union, 8 April 2014), [38].

194 *Digital Rights Ireland v Ireland*; *Kärtner Landesregierung, Seitlinger and Tschohl* (joined cases C-293/12 and C-594/12, Court of Justice of the European Union, 8 April 2014), [39].

195 *Digital Rights Ireland v Ireland*; *Kärtner Landesregierung, Seitlinger and Tschohl* (joined cases C-293/12 and C-594/12, Court of Justice of the European Union, 8 April 2014), [40].

196 *Digital Rights Ireland v Ireland*; *Kärtner Landesregierung, Seitlinger and Tschohl* (joined cases C-293/12 and C-594/12, Court of Justice of the European Union, 8 April 2014), [41]–[44].

2.182 As summarised in the Australian Human Rights Commission's submission, the Court's decision to strike down the Directive was, therefore, based on 'several characteristics of the Data Retention Directive that rendered the regime disproportionate'.[197]

2.183 The Attorney-General's Department summarised the key issues identified by the Court, being that the Directive:

- 'cover[ed], in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception',
- 'fail[ed] to lay down any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions' (such matters were left to each member-State of the EU to determine),
- 'require[ed] that those data be retained for a period of at least six months, without any distinction being made between the categories of data … on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned',
- '[did] not provide for sufficient safeguards… to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data', and
- '[did] not require the data in question to be retained within the European Union'.[198]

2.184 The effect of this decision, in the Australian Human Rights Commission's view, was to 'define the limits of permissible data retention pursuant to human rights law',[199] rather than to prohibit data retention outright. The Committee noted that similar conclusions have been reached by the German Constitutional Court and the Czech Republic's Constitutional Court, striking down domestic laws on particular grounds while confirming that data retention may, in principle, be a necessary and proportionate response.[200] Similarly, courts in Cyprus and Bulgaria have

197 Australian Human Rights Commission, *Submission 42*, p. 5.

198 Attorney-General's Department, *Submission 27*, p. 39.

199 Australian Human Rights Commission, *Submission 42*, p. 5.

200 Judgement of the Bundesverfassungsgericht, 1 BvR 256/08, of 2 March 2010; Official Gazette of 1 April 2011, Judgment of the Constitutional Court of 22 March on the provisions of section 97 paragraph 3 and 4 of Act No. 127/2005 Coll. on electronic communications and amending certain related acts as amended, and Decree No 485/2005 Coll. on the data retention and transmission to competent authorities.

annulled individual elements of their national laws, without affecting the validity of data retention as a whole in those countries.[201]

2.185 The Romanian Constitutional Court held data retention to be unconstitutional in 2009.[202] Additionally, as the Department notes in its submission:

> The invalidation of the Directive has resulted in the annulment of a number of data retention laws in member States where the Directive was implemented, in particular in jurisdictions that had effectively transposed the Directive without incorporating additional, national safeguards.[203]

2.186 The outcomes of these international decisions indicates that the assessment of the proportionality of a mandatory data retention scheme must take into account the existence and extent of safeguards to protect against unlawful or improper access to or use of retained information.

Privacy concerns relating to legal professional privilege and obligations of professional confidence

2.187 The Committee received evidence from a number of submitters and witnesses identifying particular privacy concerns regarding access to telecommunications data about communications that may be subject to legal professional privilege or to obligations of professional confidence, such as a journalist's obligation to protect the confidentiality of their sources.[204]

2.188 The Parliamentary Joint Committee on Human Rights has requested the advice of the Attorney-General as to whether access to telecommunications data under the TIA Act may impact on legal professional privilege and, if so, how this is proportionate with the right to privacy.[205]

2.189 The Attorney-General's Department noted that existing safeguards under the *Public Interest Disclosures Act 2013* immunise Commonwealth officials

---

201 Supreme Court of the Republic of Cyprus, Decision in civil applications 65/2009, 78/2009, 82/2009 and 15/2010-22/2010, 1 February 2011; Supreme Administrative Court of Bulgaria, No. 13627, 11 December 2008.

202 Decision no 1258 from 8 October 2009 of the Romanian Constitutional Court, Romanian Official Monitor No 789, 23 November 2009.

203 Attorney-General's Department, *Submission 27*, p. 39.

204 See, for example, Law Council of Australia, *Submission 126*, p. 22; Media, Entertainment and Arts Alliance, *Submission 90*, p. 4.

205 Parliamentary Joint Committee on Human Rights, *Fifteenth Report to the 44th Parliament*, p. 17.

from any form of criminal, civil or administrative liability for making a legitimate public interest disclosure, and that:

> As such, data access powers will generally not be available to law enforcement agencies in relation to genuine whistleblowers by reason of those disclosures.[206]

2.190 The Department's submission further argued that, where particular conduct has been determined to be criminal in nature, agencies should have access to appropriate tools to investigate that conduct :

> Disclosures of data are available to support the enforcement of the criminal law, administration of pecuniary penalties and the protection of the public revenue. It is not appropriate to afford a special status to particular types of communications as powers of this type should, by their nature, be applied generally.[207]

2.191 The Law Council of Australia acknowledged that there are circumstances in which access to telecommunications data about a lawyer's communications will be justifiable, including where the communications are in furtherance of the commission of a crime.[208] Similar reasoning would apply to communications within other relationships that are subject to obligations of confidence.

2.192 In evidence, the Media, Entertainment & Arts Alliance argued that the Bill should not be passed, but that if it were passed it would be preferable that law enforcement and national security agencies should be precluded from accessing telecommunications data to investigate criminal offences involving the unlawful disclosure of information covered by the official secrecy provisions of the *Crimes Act 1914*:[209]

> The real concern of all this is that the use and the keeping of metadata makes the ability to identify confidential sources and the communication between a confidential source and a journalist transparent to the authorities. We have seen over the past 10 or 15 years an increasing amount of referral to particularly the Australian Federal Police for investigation of breaches under the Crimes Act.
>
> …
>
> There is no doubt under the current legislation, because of the failure of repeated governments to decriminalise the leaking of

206 Attorney-General's Department, *Submission 27*, p. 22.

207 Attorney-General's Department, *Submission 27*, p. 21.

208 Law Council of Australia, *Submission 126*, p. 22.

209 Mr Christopher Warren, Federal Secretary, Media, Entertainment & Arts Alliance, *Committee Hansard*, Canberra, 30 January 2015, p. 38.

> information, that a whistleblower or a confidential source of whatever nature is committing a crime—when they are a government employee—when they release information to a journalist.
>
> …
>
> The problem of having a criminalised approach like that is it acts as a very serious chilling effect. The main impact of this legislation is to have a chilling effect on any potential whistleblower or confidential source releasing information they would not want to release.

2.193 The Committee recognises the heightened public interest in ensuring the confidentiality of certain privileged or confidential communications, as well as in promoting public confidence in the confidentiality of those communications. This issue is considered in greater detail later in the report (see Chapter 6).

The security of retained telecommunications data

2.194 Whether or not telecommunications data retained under a mandatory data retention scheme can be effectively secured is critical to assessing whether such a scheme is a proportionate for national security and law enforcement purposes.

2.195 The Committee received a range of evidence that retained telecommunications data would be vulnerable to unauthorised access.[210] The risk of unauthorised access to or modification of telecommunications data retained by carriers is closely related to privacy and civil liberties concerns. The Australian Privacy Commissioner observed that data retention:

> creates a risk that the data may be misused, such as through inappropriate access or the risk of identity theft and fraud as a result of data breaches.[211]

2.196 Mr Tom Courtney submitted that ISPs would implement inadequate security controls to reduce costs:

---

210 See, for example: Ms Clark, Australian Communications Consumer Action Network, *Committee Hansard*, 29 January 2015, p. 81; Mr Lawrence, Electronic Frontiers Australia, *Committee Hansard*, Canberra, 29 January 2015, p. 21.

211 Mr Timothy Pilgrim PSM, Australian Privacy Commissioner, *Committee Hansard*, Canberra, 29 January 2015, p. 46.

> As storing the data will have to be implemented by the ISP's it will not necessarily have the appropriate security controls. It is very likely that ISPs will implement the cheapest solution at the expense of security which would lead to this data being easily hacked by any malicious person or organisation.[212]

2.197 Mr Courtney's concerns echo public comments previously made by the then Chief Regulatory Officer of iiNet that 'we'll be looking for the cheapest, lowest-cost option. That means cloud storage and the lowest-cost cloud storage in the world today is in China'.[213]

2.198 Telstra's Chief Information Security Officer explained to the Committee how implementing a data retention scheme may increase, but not fundamentally alter the nature of the information security risks currently faced by service providers:

> We do secure the data we have today. So we do have that problem today. The issue here is that now we are advertising that for a customer of Telstra there is a whole range of data, depending on what services they have, that for two years we can make available upon lawful request. If I were that way inclined as a hacker, you would go for that system, because it would give you the pot of gold as opposed to working your way through our multitude of systems today to try to extract some data. But your fundamental point is that, yes, we face this risk today—absolutely.[214]

2.199 Optus provided an alternative view on how the centralised storage of data may alter the level of information security risk:

> [H]aving a relatively limited, well-defined dataset as opposed to our entire internal commercial dataset … just makes that task a lot easier. Mr Burgess from Telstra did say that yes, there will be a—I think the word he used was 'honeypot'. Clearly just the existence of a database will attract people's interest. But if it is a well-defined database and it is not the entire set of data or processes that we maintain, it should be a relatively straightforward task to segregate it for security purposes, and possible encrypt it, if need be. It is a sensible thing to have things like electronic sand traps—

212 Mr Tom Courtney, *Submission 23*, p. 1.

213 Mr Steve Dalby, Chief Regulatory Officer, iiNet Ltd, quoted in 'New laws to stop web storage hackers', *Sydney Morning Herald*, 31 October 2014, <http://www.smh.com.au/federal-politics/political-news/new-laws-to-stop-web-storage-hackers-20141031-11f3qz.html> viewed 26 February 2015.

214 Mr Mike Burgess, Chief Information Security Officer, Telstra, *Committee Hansard*, Canberra, p. 9.

> all of the access protocols that we apply to the most sensitive information already.[215]

2.200 Optus further observed that, because information retained in accordance with data retention obligations may only need to be accessed by a provider's law enforcement liaison unit, providers may actually have options to secure such information to a greater extent than is possible for most telecommunications data currently held by industry:

> One of the options that may be considered is putting all of this data onto its own system, its own separate database, so that the only people who can access that system are the law enforcement liaison unit staff and it is not available for other people in the business and so, therefore, it is not linked out into the wide world where people can attack it from. That is one of the options that providers could give very serious consideration to.[216]

2.201 The telecommunications industry is currently subject to a range of information security obligations. Most service providers, with the exception of those with an annual turnover of less than $3 million, are required to comply with the information security provisions of the *Privacy Act 1988*. The Attorney-General's Department noted that these obligations require service providers to 'adopt a risk-based approach to protecting personal information in their possession from misuse, interference or loss, as well as from unauthorised access, modification or disclosure'.[217]

2.202 The Department also drew the Committee's attention to the guidelines issued by the Australian Information Commissioner, which explain that entities must consider a range of factors when determining how to protect information they hold, including the amount and sensitivity of the personal information, and the possible adverse consequences for an individual. In particular, the guidelines state that '[m]ore rigorous steps may be required as the quantity of personal information increases'.[218]

2.203 Communications Alliance also confirmed that service providers are currently required to comply with the Australian Government Protective Security Policy Framework (PSPF), which sets out mandatory requirements for physical, personnel and information security, and the Information Security Manual (ISM), which is developed by the Australian

---

215 Mr Epstein, *Committee Hansard*, Canberra, 30 January 2015, p. 22.

216 Mr Michael Elsegood, Member of Communications Alliance, *Committee Hansard*, Canberra, 17 December 2014, p. 40.

217 Attorney-General's Department, *Submission 27*, p. 37.

218 Australian Information Commissioner, *Australian Privacy Principles guidelines* (2014), [11.7].

Signals Directorate and sets out executive guidance, principles and technical security controls to mitigate risks to information and systems.[219]

2.204 The Committee notes that it is not common for private sector organisations to be required to comply with the PSPF and ISM.

2.205 The Government has also undertaken to implement further, industry-wide telecommunications sector security reforms (TSSR), recommended by this Committee in May 2013, before data retention is fully implemented.[220] In its submission, the Department explained that:

> TSSR is designed to ensure the security and integrity of Australia's telecommunication infrastructure by encouraging ongoing awareness and responsibility for network security by the telecommunications industry, and will extend to provide better protection of information held by industry in accordance with data retention obligations.
>
> TSSR will impose an obligation on service providers to do their best to prevent unauthorised access and unauthorised interference to telecommunications networks and facilities, including where the provider outsources functions.[221]

2.206 The Bill does not introduce new information security obligations for retained telecommunications data. However, the Department argued:

> it is preferable to implement a holistic security framework for the telecommunications sector, rather than imposing specific, stand-alone and potentially duplicative security obligations that apply only to a relatively narrow subsection of the information held by industry.[222]

2.207 Mr Peter Froelich, appearing as an industry member of the Communications Alliance, stressed that, beyond their legal obligations, providers have commercial and ethical incentives, as well as a range of tools, to secure customer information:

> [A]s an industry, we have every reason and every intention to protect the privacy and security of our customers. For our industry members, there would be no reason why we do anything less with their data under this regime than we do under anything else. All of those security structures and tools available to us—firewalls,

219 Mr Stanton, *Committee Hansard*, Canberra, 17 December 2014, p. 39.

220 The Hon Malcolm Turnbull MP, Minister for Communications, *House of Representatives Hansard*, 30 October 2014, p. 12562; Ms Jones, Attorney-General's Department, *Committee Hansard*, Canberra, 17 December 2014, p. 2.

221 Attorney-General's Department, *Submission 27*, p. 38.

222 Attorney-General's Department, *Submission 27*, p. 37.

> physical security and encryption—we would put in place to ensure that our customers' privacy and security is maintained along with the interface with government as well. Those are standard practices now in the way we deal with law enforcement and national security and the way we deal with customers' data.[223]

Committee comment

2.208 The Committee received a great deal of evidence on the question of whether mandatory data retention is a necessary and proportionate measure for national security and law enforcement purposes. Much of this evidence was received in public. The Committee has also received classified and commercially confidential evidence. The Committee has carefully weighed the totality of the evidence before it when considering this issue.

2.209 The value of telecommunications data to national security and law enforcement investigations is indisputable. Its value is rising as criminals and persons engaged in activities prejudicial to security increasingly rely on communications technology to plan, facilitate and carry out their activities, while the ability of agencies to lawfully intercept the content of those communications declines.

2.210 Several submissions and witnesses argued that this Bill is not urgent, due to the long-term nature of the challenges facing agencies and the fact that, should this Bill be passed, it would take up to two years following Royal Assent for data retention to be fully implemented.[224] This is an argument which the Committee has carefully considered.

2.211 Nearly two years ago, the previous Committee concluded that the ability of national security and law enforcement agencies to safeguard national security and public safety, and to combat serious crime, had already been degraded as a result of service providers keeping fewer records about the services they provide. This degradation has continued.

2.212 This Committee has been briefed on numerous, major investigations into serious criminal activity that have failed as a result of these changes. For example, the AFP have been unable to identify nearly half of all suspects in a current child exploitation investigation, because a number of Australian service providers do not retain basic IP address allocation

223 Mr Peter Froelich, Industry Member, Communications Alliance, *Committee Hansard*, Canberra, 17 December 2014, pp. 39–40.

224 See, for example, Mr Lawrence, *Committee Hansard*, Canberra, 29 January 2015, p. 25.

records—which are akin to a person's phone number—for any length of time.[225] In South Australia, service providers not retaining telecommunications data for mobile phones has stalled murder investigations.[226] In New South Wales, more than 80 per cent of requests for internet-related data for police investigations have been unsuccessful.[227] In Queensland, the unavailability of critical telecommunications data prevented police from identifying an offender in a child exploitation investigation; that offender continued to sexually abuse a young girl for more than four years until his identity was discovered as part of a separate investigation.[228]

2.213 The Committee has also received detailed, classified evidence on the impact that the inconsistent retention of telecommunications data has had on national security investigations, including counter-terrorism, counter-espionage and cyber-security investigations. This long-term decline in the availability of telecommunications data has undermined ASIO's ability to detect and prevent threats to national security and public safety. ASIO has confirmed that these changes in commercial retention practices have prevented it from replicating previous, specific successes in safeguarding national security.[229]

2.214 Accordingly, the Committee accepts that introducing a mandatory data retention regime is necessary to support our national security and law enforcement agencies' capabilities.

2.215 In the Committee's view, the appropriate balance is to implement a data retention scheme that is strictly limited to what is necessary and proportionate, while ensuring that appropriate limits, safeguards and oversight mechanisms are in place to address privacy and civil liberties concerns. In examining the Bill, the committee has given careful consideration to the appropriate safeguards and oversight mechanisms that can be implemented to ensure the integrity of a data retention regime, and to protect and promote fundamental human rights and civil liberties, as the Australian public expects.

225 AFP, *Submission No. 76*, p. 11.

226 South Australia Police, *Submission No. 9*, p. 3; Assistant Commissioner Dickson, *Committee Hansard*, Canberra, 30 January 2015, p. 48.

227 Assistant Commissioner Lanyon, *Committee Hansard*, Canberra, 30 January 2015, p. 43.

228 Bravehearts, *Submission No. 33*, pp. 5-6.

229 ASIO, *Submission 12.1*, p. 30.