5

Data Retention

Introduction

5.1 The Attorney-General's Department (AGD) Discussion Paper notes that the Australian Government is seeking the Committee's views on a mandatory data retention regime.[1]

5.2 Specifically, the Discussion Paper states that the Committee should consider:

> Applying tailored data retention periods for up to 2 years for parts of a data set, with specific timeframes taking into account agency priorities and privacy and cost impacts.[2]

5.3 The Discussion Paper discusses the importance of accessing communications data in investigating crime and threats to national security:

> Lawful interception and access to telecommunications data are cost-effective investigative tools that support and complement information derived from other sources.[3]

---

1 Attorney-General's Department, *Equipping Australia Against Emerging and Evolving Threats*, July 2012, p. 13.

2 Attorney-General's Department, *Equipping Australia Against Emerging and Evolving Threats*, July 2012, p. 13.

3 Attorney-General's Department, *Equipping Australia Against Emerging and Evolving Threats*, July 2012, p. 14.

5.4 Furthermore:

> Telecommunications data is commonly the first source of important lead information for further investigations and often provides a unique and comprehensive insight into the behaviour of persons of interest.[4]

5.5 The Discussion Paper also explains why reforms in this area are necessary:

> Currently, authorised access to telecommunications data, such as subscriber details, generated by carriers for their own business purposes is an important source of information for agencies. As carrier's business models move to customer billing based on data volumes rather than communication events (for example number of phone calls made), the need to retain transactional data is diminishing. Some carriers have already ceased retaining such data for their business purposes and it is no longer available to agencies for their investigations.[5]

5.6 In subsequent correspondence to the Committee, the Attorney-General clarified the data set, noting that it is similar to that set out under the European Union data retention directive.

5.7 In this letter, Attorney-General the Hon Nicola Roxon MP stated that:

> 'Telecommunications data' is information about the process of a communication, as distinct from its content. It includes information about the identity of the sending and receiving parties and related subscriber details, account identifying information collected by the telecommunications carrier or internet service provider to establish the account, and information such as the time and date of the communication, its duration, location and type of communication.[6]

5.8 Furthermore, Attorney-General Roxon noted that the Government does not 'propose that a data retention scheme would apply to the content of communications', including 'the text or substance of emails, SMS messages, phone calls or photos and documents sent over the internet'. Access to these would continue to be authorised only under warrants issues in accordance with the *Telecommunications (Interception and Access) Act 1979* (TIA Act).[7]

---

4 Attorney-General's Department, *Equipping Australia Against Emerging and Evolving Threats*, July 2012, p. 21.

5 Attorney-General's Department, *Equipping Australia Against Emerging and Evolving Threats*, July 2012, p. 21.

6 Letter from Attorney-General Nicola Roxon to the Hon Anthony Byrne MP, 17 September 2012, Appendix F.

7 Letter from Attorney-General Nicola Roxon to the Hon Anthony Byrne MP, 17 September 2012, Appendix F.

5.9 Many submitters to this inquiry expressed their concerns about content being retained under any mandatory data retention regime. However, the Attorney-General and AGD categorically ruled out retaining content in evidence to the Committee.[8] This would preclude access to content such as the substance of text messages and emails, about which many submitters expressed concern. Nevertheless, the vital definitional issue of what constitutes 'data' and 'content' is examined.

The current regime

5.10 According to the report on the TIA Act that is published by AGD annually, enforcement agencies are able to access certain communications data under part 4-1 of TIA Act, however access to the actual content of this communication is prohibited except under a warrant.[9]

5.11 The communications data that can be accessed includes:

- subscriber information;
- telephone numbers of the parties involved in the communication;
- the date and time of a communication;
- the duration of a communication;
- Internet Protocol (IP) addresses and Uniform Resource Locators (URLs) to the extent that they do not identify the content of a communication; and
- location-based information.[10]

5.12 A table listing the telecommunications data currently provided to agencies by Telstra under the provisions of the TIA Act is available at Appendix H.

5.13 Under the current regime, law enforcement agencies may access historical communications data in circumstances where it is considered reasonably necessary for:

- the enforcement of criminal law;
- the enforcement of a law imposing a pecuniary penalty; or
- the protection of public revenue.[11]

---

8 A letter from the Secretary of AGD, Mr Roger Wilkins AO, clarifying the data set can be found at Appendix G.

9 Attorney-General, *Telecommunications (Interception and Access) Act: Report for the year ending June 2011*, Commonwealth of Australia, 2011, p. 10.

10 Attorney-General, *Telecommunications (Interception and Access) Act: Report for the year ending June 2011*, Commonwealth of Australia, 2011, p. 10.

11 Attorney-General, *Telecommunications (Interception and Access) Act: Report for the year ending June 2011*, Commonwealth of Australia, 2011, p. 11.

5.14 Access to prospective communications data, however,

> ...may only be authorised by a criminal law-enforcement agency when it is considered reasonably necessary for the investigation of an offence with a maximum prison term of at least three years.[12]

5.15 For ASIO, these authorisations 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'.[13]

5.16 The TIA Act also sets out who is able to make these authorisations:

- Head of an agency;
- the deputy head of an agency; or
- an officer or employee of the agency covered by an approval, in writing, of the head of the agency.[14]

5.17 The regime governing access to prospective data is very similar to that for historical data. The key difference is that the authorisation for access to prospective data either ends at a specified time, or ends after 90 days.[15]

5.18 It is important to note that the AGD Discussion Paper proposes no changes to the regime for accessing communications data, and simply raises the possibility of making retention of the relevant data mandatory for carriers/carriage service providers (C/CSPs).

The international experience

5.19 During this inquiry, the experience of the European Union in implementing a data retention regime in its member countries was raised by several submitters and witnesses.[16] As a result, the Committee explored this experience to see what lessons it can offer in terms of potential data retention regimes in Australia.

5.20 The two relevant international examples of data retention regimes that the Committee explored were implementations of the European Union's data retention directive; particularly the controversy surrounding its implementation in Germany, and the United Kingdom's voluntary data retention scheme.

---

12 Attorney-General, *Telecommunications (Interception and Access) Act: Report for the year ending June 2011*, Commonwealth of Australia, 2011, p. 11.

13 *TIA Act*, Part 4-1.

14 *TIA Act*, Part 4-1.

15 *TIA Act*, Part 4-1.

16 See Blueprint for Free Speech, *Submission No. 165;* Law Council, *Submission No. 96;* Pirate Party of Australia, *Submission No. 134*; Human Rights Law Centre, *Submission No. 140.*

EU data retention directive

5.21 On 15 March 2006 the European Parliament and the Council of the EU passed a directive requiring all member states to transpose laws mandating the retention of telecommunications data for periods between six months and two years, according with their legal and constitutional processes.[17]

5.22 According to the Law Council, the EU Data Retention Directive:

> …requires providers of publicly available electronic communications services and public communication networks to retain communications data for the investigation, detection and prosecution of serious crime as defined by each Member State.[18]

5.23 This directive 'does not permit the retention of data revealing the content of the communication', and instead focuses on a 'wide range of other telecommunications data' that allows enforcement and security agencies to:

- Trace and identify the source of a communication, such as the calling telephone number, the name and address of the subscriber or registered user… or the name and address of the internet subscriber or registered user to whom an Internet Protocol (IP) address, user identification or telephone number was allocated at the time of the communication;
- Identify the destination of a communication, such as numbers dialled or the name and address of the internet subscriber or registered user and user ID of the intended recipient of the communication;
- Identify the data, time and duration of a communication, such as the data and time of the start and end of a telecommunication, the data and time of the log-in and log-off of the internet access service, the date and time of the log-in and log-off of the internet email service;
- Identify the type of communication; such as the telephone service used or the internet service used;
- Identify users' communication equipment, such as the International Mobile Subscriber Identity of the calling party or the digital subscriber line or other end point of the originator of the internet communication; and
- Identify the location of mobile equipment, such as the location label at the start of the telecommunication.[19]

5.24 The EU Data Retention Directive required member states to 'implement measures to ensure this data is retained for periods between six months and two years from the date of the communication', the Law Council told the Committee,

17 European Union Data Retention Directive 2006/24/EC.

18 Law Council, *Submission No. 224*, p. 6.

19 Law Council, *Submission No. 224*, p. 6.

and also makes provisions for access to the data and the security of the retained data.[20]

5.25 While the Directive has been implemented in several countries, and notably in the UK via a voluntary code of practice, it has been subject to successful constitutional challenges in three EU member states: Germany, Romania and the Czech Republic.

5.26 According to the Law Council:

> The Romanian Court accepted that interference with fundamental rights may be permitted where it respects certain rules and where adequate and sufficient safeguards are provided to protect against potential arbitrary state action. However, the Court found the transposing law to be ambiguous in its scope and purpose with insufficient safeguards. The Court held that a 'continuous legal obligation' to retain all traffic data for six months was incompatible with the rights to privacy and freedom of expression…[21]

5.27 In the case of Germany, the Law Council stated:

> The German Constitutional Court said that data retention generated a perception of surveillance which could impair the free exercise of fundamental rights. It explicitly acknowledged that data retention for strictly limited uses along with sufficiently high security of data would not necessarily violate the German Basic Law. However, the Court stressed that the retention of such data constituted a serious restriction of the right to privacy and therefore should only be admissible under particularly limited circumstances, and that a retention period of six months was at the upper limit of what could be considered proportionate. The Court further held that data should only be requested where there was already a suspicion of a serious criminal offence or evidence of a danger to public security, and that data retrieval should be prohibited for certain privileged communications which rely on confidentiality.[22]

5.28 Finally, in the case of the Czech Republic, the Law Council told the Committee:

> The Czech Constitutional Court annulled the transposing legislation on the basis that it was insufficiently precise and clear in its formulation. The Court held that the definition of authorities competent to access and use retained data and the procedures for such access and use were not sufficiently clear in the transposing legislation to ensure the integrity and

20 Law Council, *Submission No. 224*, p. 7.

21 Law Council, *Submission No. 224*, p. 9.

22 Law Council, *Submission No. 224*, pp. 9-10.

> the confidentiality of the data. Because of this, the individual citizen had insufficient guarantees and safeguards against possible abuses of power by public authorities. In obiter dictum the Court also expressed doubt as to the necessity, efficiency and appropriateness of the retention of traffic data given the emergence of new methods of criminality such as through the use of anonymous SIM cards.[23]

5.29 In addition to these successful challenges, there are currently cases in Bulgaria, Cyprus, Hungary and Ireland being mounted to challenge the implementation of the EU Data Retention Directive, the latter has 'been referred to the European Court of Justice'.[24] It must be noted, however, that these challenges took place in countries with human rights frameworks that are significantly different to those in Australia.

UK voluntary data retention

5.30 The Law Council told the Committee that the UK has implemented the EU data retention directive via a voluntary code of practice relating to data retention:

> The United Kingdom (UK) has a system of voluntary data retention which derives from Part 11 of the Anti-Terrorism, Crime and Security Act 2001. Telephone operators and Internet Service Providers retain some data under a voluntary arrangement with the UK Home Office.[25]

5.31 The NSW Young Lawyers elaborated on how this code works:

> In the UK, this convention has been the basis upon which the Home Office has issued a voluntary code of conduct under which telephone and internet service providers retain some data. The legislation enabling the Convention in the UK also provides that if the Secretary of State is unconvinced of the efficacy of such a voluntary program, then the Code may be made mandatory. The code has not subsequently been made mandatory and requires only a small subset of data be kept for up to 12 months, principally consisting of subscriber information that would be necessary for billing.[26]

5.32 The Australian Mobile Telecommunications Association (AMTA) and the Communications Alliance noted that the costs of the voluntary data retention are fully borne by the UK Government, and that this is a part of the voluntary code

23 Law Council, *Submission No. 224*, p. 10.
24 Law Council, *Submission No. 224*, p. 10.
25 Law Council, *Submission No. 96*, p. 38.
26 NSW Young Lawyers, *Submission No. 133*, p. 10.

of practice.[27] Further, in order to have these costs borne by the government, UK service providers must be a part of the voluntary code.[28]

5.33 The UK Parliament is currently considering a *Draft Communications Data Bill* that will, amongst other things, make the retention of data mandatory for 12 months.[29] However, the UK Bill differs significantly from the potential reform being considered in Australia. For instance, the data to be collected and stored under the UK Draft Bill is limited only in terms of what is considered 'necessary' by the UK Home Office, which extends to data such as 'web logs'.[30]

5.34 In this regard, a report produced by the UK Intelligence and Security Committee (ISC), was broadly supportive of the need for reform:

> The Agencies require access to communications data – in certain tightly controlled circumstances and with appropriate authorisation – in the interests of national security. We recognise that changing technology means that the Agencies are unable to access all the communications data they need, that the problem is getting worse, and that action is neeed now. We accept that legislation to update the current arrangements governing the retention of communications data offers the most appropriate way forward.[31]

5.35 At the end of its inquiry the Committee was provided with the ISC report published in February 2013. The ISC reached three key conclusions:

- The intelligence agencies need to continue to have access to telecommunications data;
- There is a gap emerging in their ability to access this data; and
- While legislation is not a perfect solution, it is the best available option in contrast to other investigatory methods and a voluntary approach.[32]

5.36 Furthermore, the Joint Committee on the Draft Communications Data Bill of the UK Parliament has produced a report on the draft bill which was also broadly supportive of the need for reform. However, this report also cautioned:

---

27 AMTA and Communications Alliance, *Submission No. 114*, p. 14.

28 UK Home Office, *Explanatory Memorandum to the Data Retention (EC Directive) Regulations 2009*, pp. 1-2.

29 *Draft Communications Data Bill 2012*, United Kingdom.

30 Joint Committee on the Draft Communications Data Bill, UK Parliament, Draft Communications Data Bill, December 2012, p. 24.

31 UK Intelligence and Security Committee, Press release, 11 December 2012, viewed 18 December 2012, <http://isc.independent.gov.uk/news-archive/11december2012>.

32 UK Intelligence and Security Committee, *Access to Communications Data by Intelligence and Security Agencies*, UK Parliament, February 2013.

> …the current draft Bill is too sweeping, and goes further than it need or should. We believe that, with the benefit of fuller consultation with CSPs than has so far taken place, the Government will be able to devise a more proportionate measure than the present draft Bill, which would achieve most of what they really need, would encroach less on upon privacy, would be more acceptable to CSPs and would cost the taxpayer less.[33]

Responses to data retention

5.37 The potential data retention regime attracted a large amount of criticism and comment from organisations and concerned individuals. These organisations and individuals generally considered any potential data retention regime a significant risk to both the security of their information, and their privacy. In addition to these general comments, the Committee received a large volume of form letter correspondence. A collective sample of some of these comments and the form letters can be found in Box 5.1.

5.38 Conversely, the data retention regime received a high level of support from law enforcement and national security agencies. These agencies largely argued that data retention was necessary for them to maintain their current capabilities into the future.

5.39 This section outlines these perspectives by grouping them under the following headings:

- Privacy and civil liberties;
- Security;
- Feasibility and efficacy; and
- Cost.

33 Joint Committee on the Draft Communications Data Bill, UK Parliament, *Draft Communications Data Bill,* December 2012, p. 74, viewed 18 December 2012, <www.parliament.uk/business/committees/committees-a-z/joint-select/draft-communications-bill/publications/>.

Box 5.1 Community responses to the mandatory data retention regime proposal

'As both an Australian citizen and a small business owner I am seriously concerned about the over-reaching changes proposed by this reform. I believe it is inherently wrong to log and track activity via an individual's ISP and/or participation in social network/s.' (Mr Craig Veness, *Submission No. 13*, p.1 and other submitters (in common form).)

'By tracking and recording every single Australian online, and keeping these records for two years, this proposal will destroy our online privacy, make every Australian into a criminal, give too much power to the government, and go far and beyond what is necessary. Specifically, I oppose the proposals to: 1)Keep all Australians' online data for two years 2)Track everything said on Twitter, Facebook & other social media…' (Ms Rhonda Palmer, *Submission No. 20*, p. 1 and other submitters (in common form).)

'The proposal that internet services providers retain all data on all users for a period of two years turns all citizens into suspects. This proposal is undemocratic and unacceptable; it also creates a security risk as the preserved data can be made available and misused.' (Mr Josh Fergeus, *Submission No. 53*, p. 1 and other submitters (in common form).)

'[I] have a concern that the data collection proposed by the Australian government will increase the fear and nervousness that as people living in a free democratic country we should be free from feeling, an untrusted, and being watched for criminal behaviour by our own government, by businesses not designed to monitor the information its customers disclose to each other in private conversation.' (Ms Odette Stephens, *Submission No. 1*, p. 1.)

'I am strongly opposed to the draconian proposals from Australia's intelligence community, that telephone and internet data of every Australian be retained for up to two years and intelligence agencies be given increased access to social media sites such as Facebook and Twitter. Such data retention schemes are extremely unpopular, have been a subject of much global debate and outrage, most ISPs and the majority of Australians share these sentiments.' (Mr Mark Simpson, *Submission No. 2*, p. 1.)

'I don't believe national security justifies the proposed levels of intrusion into citizens' private lives.' (Mr Malcolm Rieck, *Submission No. 21*, p.1.)

'It would be a great shame if a country such as ours were to adopt such an invasive and unnecessary data retention policy that infringes on the basic privacies of citizens, which instead of presuming innocence until guilty, collects data on them and stores it as if they were criminals. Should it become law that conversations between two people walking down the street were to be recorded by the government, it would be considered a gross

invasion of privacy akin to the invasions of privacy that were present in Soviet era Russia.' ('James', *Submission No. 7*, p. 1.)

'This concept of long term data retention is especially concerning these days, considering how much of our life takes place on the internet.' (Mr Peter Serwylo, *Submission No. 22*, p. 1.)

'This is crazy. ALL customers, and ALL their data? The people who thought this up are sick.' (Mr Joe Stewart, *Submission No. 32*, p. 1.)

'We do not need our government to spy on us all the time. I would rather we had the occasional act of terrorism than live under an oppressive government.' (Mr Sam Watkins, *Submission No. 29*, p. 1.)

'I am a middle-aged, middle class, professional woman with no dark secrets to hide and nothing to fear from anyone knowing anything whatsoever about my online activities, but I can hardly believe that this is even being considered in Australia. When I first heard it I thought "Surely this is a joke."' (Ms Mary Annesley, *Submission No. 73*, p. 1.)

'The vast majority of Australians are decent people and we do not need or want the spectre of the government hovering over our most intimate moments.' (Dr James G. Dowty, *Submission No. 35*, p. 2.)

Privacy and civil liberties

Community views

5.40 A range of organisations and individuals objected to the potential data retention regime on civil liberties and privacy grounds.

5.41 The Law Council of Australia expressed its concerns about this proposal, stating:

> Introducing a requirement to retain certain data for up to two years, even with accompanying safeguards, constitutes a significant expansion of the telecommunications interception and access regime, and one that the Law Council considers has not yet been shown to be a necessary or proportionate response to investigating serious criminal activity or safeguarding national security, particularly given the very serious impacts such a reform will have on the privacy rights of many members of the community.[34]

5.42 The Institute of Public Affairs (IPA) was similarly strident in its criticism of the potential impacts of data retention, stating that the 'imposition of such an extraordinary, systematic and universal program would render any presumed or existent Australian right to privacy empty'.[35]

5.43 The IPA characterised any potential data retention regime as representing 'a significant incursion on the civil liberties of all Australians', stating that:

> Data retention would be a continuous, rolling, systematic invasion of the privacy of every single Australian, only justified because a tiny percentage of those Australians may, in the future, be suspects in criminal matters. Indiscriminate data retention is an abrogation of our basic legal rights.[36]

5.44 Blueprint for Free Speech shared the overall concerns about the impact of any data retention scheme on the privacy of internet users in Australia, stating 'this measure would dramatically reduce privacy in Australia, with very few demonstrated national security benefits'.[37]

5.45 The Pirate Party told the Committee that the data retention proposal was:

> …indicative of a shift in focus by law enforcement and intelligence organisations from protecting the populace and the presumption of

34 Law Council of Australia, Submission No. 96, p. 37.
35 Institute of Public Affairs, *Submission No. 139*, p. 4.
36 Institute of Public Affairs, *Submission No. 139*, p. 3.
37 Blueprint for Free Speech, *Submission No. 165*, p. 6.

> innocence to one of constant surveillance and suspicion of the populace. Where the existing targeted surveillance is akin to spear fishing, mandatory data retention is more like drift net fishing. The risk to individual privacy is enormous.[38]

5.46 The Human Rights Law Centre took a similar view, stating that the 'vast quantity of private data that could be stored and accessed', coupled with its extension to ancillary providers, could 'severely limit the right to privacy'. As such, any data retention scheme would need to be shown to be proportionate to the desired outcomes:

> …if the Government wishes to limit the right to privacy, it must state the overriding public interest in limiting the right and establish that the means used are reasonable, necessary and proportionate. In this instance, the Government has not provided any significant information to show that there is an overriding public interest in implementing a data-retention system.[39]

5.47 In regard to maximising the privacy of consumers of telecommunications services, Mr Daniel Nazer raised the concept of 'data minimisation', noting that it is considered by privacy experts as 'an essential tool for privacy protection'. Mr Nazer quoted the Canadian Privacy Commissioner, Dr Ann Cavoukian, on the benefits of data minimisation:

> Data minimization is essential to effective privacy protection, and can save organizations the risk and expense of managing personal information they may have no need for. Where there is no personal information, there is no consequent duty of care, with all that it implies. Further, data minimization requirements assists organizations to think through what personal information is actually necessary for their purposes, and guards against secondary uses and possible function creep.[40]

5.48 Mr Nazer went on to note that:

> Mandatory data retention flatly contradicts the principle of data minimisation. Instead, it forces service providers to store enormous amounts of data for which they have no business need.[41]

5.49 Similarly, Liberty Victoria told the Committee of its view that 'the very collection of the data would in and of itself raise significant privacy concerns'.[42] It went on

38 Pirate Party, *Submission No. 134*, p. 26.

39 Human Rights Law Centre, *Submission No. 140*, p. 7.

40 Mr Daniel Nazer, *Submission No. 110*, p. 4

41 Mr Daniel Nazer, *Submission No. 110*, p. 4

42 Liberty Victoria, *Submission No. 143*, p. 5.

to state that data retention is 'inherently more invasive' than the traditional 'targeted interception' approach, noting:

> It constitutes a significant intrusion into the privacy of each end user of telecommunications services and creates a situation in which a single security breach would have dramatic consequences. It represents a significant move away from the 'targeted' approach of the [TIA Act] which requires specific identification of communications and their relevance to an agency's activities before information can be collected.[43]

5.50 Furthermore, Liberty Victoria also submitted that 'it is inevitable that, once a database of retained communications data is established, efforts will be made to extend its use for new purposes'. As such, Liberty Victoria proposed that safeguards be put in place to ensure the retained data was used 'only where there is a demonstrated need'.[44]

5.51 The New South Wales Council for Civil Liberties (NSW CCL) noted similar concerns about the perceived diminution in privacy, and drew attention to the international experience:

> ...the present data retention laws contravene international standards. The German Constitutional Court in March 2010 declared the German data retention laws unconstitutional, because of lack of proportionality in balancing right of privacy against interest in prosecuting crime. One of the aspects which the Court held was disproportional was that it applied to too wide a range of crimes, and should be permitted only for investigation of crimes of the most serious kind.[45]

5.52 The Australian Interactive Media Industry Association's Digital Policy Group raised its concerns about the presumption of guilt which it perceived was inherent in any blanket data retention proposal. As a result, it suggested an alternative approach:

> A system allowing for requests for preservation and retention of user data made by a judge or authorised law enforcement officials would lessen the risk from such blanket intrusion into privacy.[46]

5.53 Ms Stella Gray, submitting in a private capacity, shared the concern about the presumption of innocence, noting:

> Pre-emptive surveillance of an entire population does away with the legal principle of the presumption of innocence. Any serious consideration of

43 Liberty Victoria, *Submission No. 143*, p. 2.

44 Liberty Victoria, *Submission No. 143*, p. 6.

45 NSW Council for Civil Liberties, *Submission No. 175*, p. 16.

46 Australian Digital Media Industry Association, *Submission No. 198*, p. 4.

> implementing such a system, in a democratic country such as Australia, should be anathema to policy makers.[47]

5.54 Western Australian Greens Senator Scott Ludlam echoed these concerns about the presumption of innocence, saying that indiscriminate data retention is 'unacceptable' as it essentially treats all citizens as suspects.[48] The Institute of Public Affairs similarly characterised data retention regimes as making 'internet users guilty until proven innocent'.[49]

5.55 The Victorian Privacy Commissioner, Dr Anthony Bendall, submitted that data retention was 'characteristic of a police state' as it goes against both the presumption of innocence, and 'essential dimensions of human rights and privacy law: freedom from surveillance and arbitrary intrusions into a person's life.'[50]

5.56 At a public hearing, Dr Bendall elaborated on this concern, noting that data retention:

> ...entirely undermines the fundamental underpinnings of privacy laws, which basically are that information should only be collected and stored where necessary and for a particular purpose, whereas these proposals seem to be that you store all the information just on the off chance that it might be useful down the track and you make up your mind how it would be useful at that point.[51]

5.57 The Law Council agreed that this approach 'does not sit easily with the notion of the presumption of innocence or other traditional criminal law or human rights principles', and thus may breach Australia's obligations under United Nations human rights instruments such as the International Covenant on Civil and Political Rights (ICCPR).[52]

5.58 The NSW CCL also suggested that any data retention regime would not conform to Australia's obligations under the ICCPR.[53]

5.59 Similarly, Senator Ludlam linked the privacy concerns to human rights and Australia's obligations under UN conventions. In particular, Senator Ludlam pointed to the resolution adopted by the UN Human Rights Council and the General Assembly in 2012, which noted the importance of 'the right of

47 Ms Stella Gray, *Submission No. 152*, p. 6.

48 Senator Scott Ludlam, *Submission No. 146*, p. 26

49 Institute of Public Affairs, *Submission No. 139*, p. 3.

50 Victorian Privacy Commissioner, *Submission No. 109*, p. 7.

51 Dr Bendall, *Transcript*, 5 September 2012, p. 1.

52 Law Council of Australia, *Submission No. 96*, p. 39.

53 NSW Council for Civil Liberties, *Submission No. 175*, p. 16.

individuals to seek, receive and impart information and ideas of all kind through the internet'.[54]

5.60 Senator Ludlam quoted the UN Special Rapporteur on the importance of governments upholding this principle:

> States are obliged to guarantee a free flow of ideas and information and the right to seek and receive as well as to impart information and ideas over the internet.[55]

5.61 In Senator Ludlam's view, any restrictions on this right must be demonstrated to be proportionate and necessary to the outcomes this restriction will achieve. He further contended that the Discussion Paper does not provide an adequate justification.[56]

5.62 The Law Council discussed the privacy implications of only retaining communications data, stating that even if it 'does not include the content and substance of a person's private communications', the communications data can still reveal 'crucial' information about a person, including such things as their associations and whereabouts.[57] As a result of these concerns, the Law Council recommended that the potential reform be rejected unless it could be clearly demonstrated that it is 'indispensable to protect the community from serious threats of criminal activity or national security'.[58]

5.63 iiNet agreed that any potential data retention regime could negatively impact privacy, and related this concern to Australia's National Privacy Principle (NPP) under the *Privacy Act 1988.*

5.64 iiNet noted that NPP 1.1 states that:

> ...an organisation must not collect personal information unless the information is necessary for one or more of its functions or activities. Therefore, if collection of telecommunications data or subscriber information is necessary for one or more of the functions or activities of a C/CSP (for example providing a telecommunications service), there will be no issue. However, if a C/CSP decided off its own bat (i.e. without any legal obligation to do so) to collect and retain data that is personal information solely because that data had the potential to be of use to law enforcement agencies, that C/CSP would likely be in breach of NPP 1.1. Therefore, the effect of the proposed reform is to effectively provide a

54 Senator Scott Ludlam, *Submission No. 146*, p. 2.
55 Senator Scott Ludlam, *Submission No. 146*, p. 2.
56 Senator Scott Ludlam, *Submission No. 146*, p. 2.
57 Law Council of Australia, *Submission No. 96*, p. 37
58 Law Council of Australia, *Submission No. 96*, p. 39.

> statutory exemption to NPP 1.1 and allow personal information to be collected and retained where the sole reason for the collection and retention of that personal information is the fact that it may be of use to law enforcement agencies.[59]

5.65 The AMTA and the Communications Alliance shared this concern, noting:

> Industry requires that any data retention legislation must also contain a caveat which expands upon the current concept of immunity to incorporate acting in good faith, and provide immunity to the reporting obligations under the *Privacy Act*.[60]

5.66 Mr Bernard Keane, submitting in a private capacity, argued that extending data retention from fixed line and mobile telephones to the internet constitutes a significant expansion of the powers held by law enforcement and security agencies, and thus would constitute a significant intrusion on privacy:

> Australians, like citizen around the world, do not use online communications in the same way, or for the same purposes, as they used phones. They did not commit huge amounts of personal information to permanent storage on the phone. They did not leave crucial financial details on the phone. The phone was not their primary tool for interacting with communities that are important to them. The telephone did not enable contact with communities around the globe that are of critical importance to citizens.[61]

5.67 As such, Mr Keane posited that:

> Any attempt therefore to impose the telecommunications interception laws on the internet represents not a logical extension of that law to 'keep up with technology' on a like-for-like basis but a dramatic extension of surveillance into citizens' lives far beyond that enabled by telecommunications interception.[62]

5.68 Mr Ian Quick, submitting in a private capacity, expressed a similar concern to that of Mr Keane, noting that if data on internet browsing is retained, this would constitute a much greater invasion of privacy than telecommunications data:

> It is a massive invasion of everyone's privacy, as the usage database will contain every page they accessed – such as every article they have read on a newspaper site, any online political activity they have done, anything they have done on ebay, what books they have bought on Amazon, which

59 iiNet, *Submission No. 108*, p. 12.

60 AMTA and Communications Alliance, *Submission No. 114*, p. 16.

61 Mr Bernard Keane, *Submission No. 117*, p. 13.

62 Mr Bernard Keane, *Submission No. 117,* p. 14.

> Facebook pages they have gone to, etc. - and a lot of information that is also often included in the URL.[63]

5.69 Electronic Frontiers Australia (EFA) took a similar view, and told the Committee that unlike the communications data associated with traditional telephony, internet communications data was far more intrusive:

> Even if it were to be specified that the actual content of communications is not to be retained, information such as addresses of websites visited, email addresses and phone numbers to which messages are sent and received from, details of phone calls sent and received, and other online communications activities, along with associated dates, times and locations does amount, in many cases, to content and is highly personal data.[64]

5.70 EFA raised its concern that, in aggregate, examination of this type of data 'will reveal highly intimate details of a person's life', including such things as 'religious and political affiliations, sexual orientation, health issues' and other 'highly-sensitive information'.[65]

5.71 Mr Adrian Gasparini, submitting in a private capacity, shared the concern that the data to be retained could reveal intimate details about people's lives:

> A person's browsing history is a very personal snapshot of that person's life and personality. A person should have the right to keep aspects of his personal life completely private. For example, take into consideration searches conducted on Google maps; the social networks a person may log into; medical symptom related searches on Google; and a snapshot of the adult content searched for on various websites. It would be easy to determine the identity and address of a person, their circle of friends and their partner, possibly identify any affairs being conducted, determine their sexual orientation, age, as well as any possible embarrassing medical conditions that the person may have searched for.[66]

5.72 Mr Daniel Judge, submitting in a private capacity, made a similar point about the potential privacy invasion inherent in retaining data on a person's internet browsing history:

> The Internet today is used for a broad range of things and in many cases is the first port of call for people before seeing a doctor, or psychologist, or lawyer or marriage counsellor or any range of professional services all of

63 Mr Ian Quick, *Submission No. 95*, p. 14.

64 Electronic Frontiers Australia, *Submission No. 121*, p. 5.

65 Electronic Frontiers Australia, *Submission No. 121*, p. 6.

66 Mr Adrian Gasparini, *Submission No. 88*, p. 1.

> which are activities that would be captured and detailed by a mandatory date retention scheme. Any such information could be highly embarrassing to individuals should it fall into the wrong hands or become public knowledge. As such, the decision to retain this data is a highly dangerous endeavour when viewed within the context of the damage that could be done to people should the wrong information be leaked or stolen.[67]

5.73 EFA told the Committee that, when it comes to people's internet browsing, it is very difficult to separate data from content, and that this raises further questions about the privacy impact of any data retention regime:

> A URL [uniform resource locator] will in many instances allow for the content of that website to be accessed well after the fact, providing a direct link to content. Many URLs contain sensitive information, such as user names and even passwords.[68]

5.74 iiNet made a similar point, noting that internet browsing data is often synonymous with content:

> When we go to attachment A [of the Attorney-General's letter noted above], we see it includes that certain categories of data must be retained—namely, data necessary for identifying (a) the source of a communication and (b) the destination of a communication. This is where it comes to the interesting part for us. The only conclusion we can draw about the destination of a communication when considering internet access is that what must be retained are the IP addresses. As noted previously, little to no specific guidance is given by the Attorney-General's Department on the data to be gathered, so we will continue to make assumptions. As I have mentioned, each object or piece of content on each page also has an IP address, none of which can be distinguished from any other on the page. It is therefore a paradox that requires resolution when the Attorney-General's letter has declared that the data revealing content must not be retained but the destination data must be retained.[69]

5.75 The Law Council drew on an example of this from the constitutional challenge to Germany's data retention laws:

> …even though the storage does not extend to the contents of the communications, the data may be used to draw content-related conclusions that extend into the users' private sphere. The observation

67 Mr Daniel Judge, *Submission No. 157*, p. 11.

68 Electronic Frontiers Australia, *Submission No. 121*, p. 5.

69 Mr Dalby, *Transcript*, 27 September 2012, p. 48.

> over time of recipient data, dates, times and place of telephone conversations permits detailed information to be obtained on social or political affiliations and on personal preferences, inclinations and weaknesses. So, even if it is restricted to telecommunications data in that sense, in other jurisdictions that has been considered sufficient to indicate that the jurisdiction does not consider the scheme to be appropriate.[70]

5.76 Even when it comes to traditional telephony, EFA told the Committee that 'any numbers input after connection, in response to a phone tree or other verbal prompts' are essentially content, and in some cases will contain highly sensitive information such as personal identification numbers or credit card details.[71]

5.77 EFA went on to note that this presents a civil liberties issue, in that the existence of such 'large scale databases of communications activity' could be abused by governments and police. As such, EFA stated:

> While we can earnestly hope that sufficient checks and balances would exist to prevent authorities abusing such databases to gather information on protesters (for instance), the only way to ensure that this never happens is to prevent the data being collected in the first place.[72]

5.78 Dr James Dowty, submitting in a private capacity, saw a similar potential for any data retention regime to 'be vulnerable to misuse by future governments'. Dr Dowty linked this to the amount of time the data is stored for, noting:

> Once the data retention begins, legislative change could immediately give an unscrupulous government access to the web viewing histories, emails and text messages of their political opponents and constituents. While the current government might be staunchly opposed to such misuses of the retained data, there is no guarantee that the government of 2050 will be as trustworthy. Of course, the data which is currently retained by CSPs is also open to misuse in this way, but the inappropriate use of two years' worth of data is likely to be far more damaging than the misuse of a few weeks' worth.[73]

5.79 The Pirate Party made a similar argument, noting that the types of data to be retained were open to misuse:

---

70 Ms Budavari, *Transcript*, 14 September 2012, p. 14.

71 Electronic Frontiers Australia, *Submission No. 121*, p. 5.

72 Electronic Frontiers Australia, *Submission No. 121*, p. 6.

73 Dr James Dowty, *Submission No. 35*, p. 1.

> It would provide the opportunity for law enforcement and intelligence organisations to trawl through available data looking for something which might, on the surface, be of interest to them.[74]

5.80 The Pirate Party also linked this concern to the exercise of individual rights and political freedoms:

> Analysis of the full data set could be used to map all connections and interactions of everyone in the country. Methods used to identify any criminal organisation or network could just as readily be applied to any group or organisation in the country. This could have a chilling effect on the exercise of individual rights and democratic participation. This type of analysis could then be exploited by law enforcement, intelligence organisations, elements within those organisations or other groups with which the analysis is shared to suppress organisations and groups which are not in and of themselves unlawful.

5.81 Blueprint for Free Speech raised similar concerns about political freedom, arguing that any potential data retention regime would have 'a serious effect on freedom of speech'.[75]

5.82 Blueprint for Free Speech argued that:

> Part of freedom of expression is the individual's right to determine the manner in which they communicate. In other words, it is to determine who they wish to communicate with and when they wish to stop that communication or delete it.[76]

5.83 By making the retention of communications data mandatory, Blueprint for Free Speech contended that this right could be undermined:

> People have a legitimate expectation that when they delete electronic information, it is gone. They do not expect their service provider to secretly retain it against their wishes. The [data retention] proposal is analogous to secretly collecting everyone's garbage for two years and storing it in case it might assist a criminal investigation at some point in the future. In addition, it effectively prevents people from deleting their information, which is analogous to passing a law making it illegal to destroy your own documents.[77]

5.84 As such, Blueprint for Free Speech told the Committee that this diminution in privacy, coupled with the inability to, in essence, retract communications after

74 Pirate Party, *Submission No. 134*, p. 26.
75 Blueprint for Free Speech, *Submission No. 165*, p. 6.
76 Blueprint for Free Speech, *Submission No. 165*, p. 1.
77 Blueprint for Free Speech, *Submission No. 165*, p. 6.

the fact, 'would have a chilling effect on freedom of expression'.[78] Similarly, Dr Bendall stated that data retention could have 'an extreme chilling effect on online transactions'.[79]

5.85 Mr James McPherson elaborated on how data retention could lead people to not say or write things they might otherwise:

> Even if the only data which was logged was email message headers, or a list of visited websites, there is more than enough information there to build accurate profiles of people, their opinions and their social networks. The most likely outcome of such surveillance is self-censorship, to avoid harassment by covert agencies 'just in case' an expressed opinion might fit some criteria which the agencies make up to justify invasive actions.[80]

5.86 Ms Stella Gray shared the concerns that any data retention regime would have a 'chilling effect on political speech and public discourse'.[81]

5.87 Australian Lawyers for Human Rights argued that, in order to maintain the 'expectation of privacy' of legitimate users of telephony and internet communications, 'the minimum amount of confidential data' should be 'retained for the smallest period of time possible'.[82]

5.88 AMTA and the Communications Alliance were similarly concerned about the privacy implications of retaining too much data:

> There is likely to be some additional social cost, constituting both the cost of loss of privacy and a further additional risk to security as the retained data becomes itself a target for unlawful access. Industry believes it is generally better for consumers that service providers retain the least amount of telecommunications information necessary to provision, maintain and bill for services (including calls and transmissions).[83]

5.89 Ms Ashley Hull also suggested that, if privacy is to be maintained to the greatest possible extent, the data retained should be targeted:

> ISPs shouldn't be told to keep data for customers whom have not yet been targeted by law enforcement with an open case and a warrant. As the lines between terrorism, civil disobedience and healthy dissent are deliberately blurred, our rights must be protected from these overarching sweeping reforms which target the select few while touching all of us. We

78 Blueprint for Free Speech, *Submission No. 165*, p. 1.
79 Dr Bendall, *Transcript*, 5 September 2012, p. 3.
80 Mr James C. McPherson, *Submission No. 28*, p. 4.
81 Ms Stella Gray, *Submission No. 152*, p. 6.
82 Australian Lawyers for Human Rights, *Submission No. 194*, p. 8.
83 AMTA and Communications Alliance, *Submission No. 114*, p. 15.

> need to ensure there is no room for ambiguity - The crosshair must be aimed precisely.[84]

5.90 The IPA suggested that it would be possible to minimise the intrusion into privacy at the same time as maintaining the efficacy of law enforcement if the data was retained in a targeted fashion, stating that:

> Strictly limited, supervised, and transparent data preservation orders on targeted suspects would strike the right balance between individual rights and law enforcement.[85]

5.91 Mr Nazer made a similar suggestion, noting that Australia should draw on the Canadian approach by instituting:

> …a process whereby an agency can secure a temporary preservation order that remains in effect only for as long as it takes law enforcement to return with a warrant. While any data preservation program would still require safeguards to protect privacy, it is certain to be less invasive and costly than massive and indiscriminate data retention.[86]

Law enforcement and security agencies' views

5.92 Law enforcement and national security agencies were adamant that any potential data retention regime does not represent an expansion of their powers, and thus does not translate into any serious diminution of privacy or a winding back of civil liberties.

5.93 As noted in the section describing the current regime above, law enforcement agencies are able to access telecommunications data (as distinct from content) under certain circumstances without a warrant. Collective examples arguing the importance of communications data to law enforcement agencies in investigations are included in Box 5.2.

5.94 As noted below, this access is tightly controlled by the C/CSPs themselves and is only disclosed when properly authorised, and no change is proposed to this aspect of the TIA Act by the AGD Discussion Paper. As such, mandating data retention will not lead to the removal of the presumption of innocence, as data will continue to be accessed only in connection with active investigations.

5.95 The Australian Federal Police (AFP) noted that access to communications data is both a necessary investigative tool and is far less privacy invasive than normal interception:

---

84 Ms Ashley Hull, *Submission No. 153*, p. 1.

85 Institute of Public Affairs, *Submission No. 139*, p. 4.

86 Mr Daniel Nazer, *Submission No. 110*, p. 7.

> Non-content telecommunications data is an important investigative tool for the AFP. It can provide important leads for agencies, including evidence of connections and relationships within larger associations over time, evidence of targets' movements and habits, a snapshot of events immediately before and after a crime, evidence to exclude people from suspicion, and evidence needed to obtain warrants for the more intrusive investigative techniques such as interception or access to content.[87]

5.96 Furthermore:

> There are no operational risks, and from a law enforcement perspective and as it relates to data about communications rather than its content, it raises fewer privacy concerns than the other covert investigative methods.[88]

5.97 Victoria Police noted that, as business practices change in the telecommunications sector, so does the length of time for which data is retained:

> As carriers change their business practices from billing based on volume/length of calls made to billing based on data volumes, the need for carriers to retain such data is diminishing. This has enormous implications for law enforcement agencies reliant on this data to target suspects involved in serious crime.[89]

5.98 The Corruption and Crime Commission of Western Australian made the point that, if data retention is not made mandatory, they could face a diminution in their capabilities:

> Agencies will face many challenges as telecommunications technologies migrate to IP networks. Investigations across almost all serious crime types including corruption, counter-terrorism and homicide rely significantly on telecommunications data. Without legislated data retention obligations the degradation of investigative capability will be significant.[90]

5.99 The AGD noted that there was evidence that this capability was already diminishing:

---

87 Australian Federal Police, *Submission No. 163*, p. 15. See also ASIO, *Submission No. 209*, p. 1; Attorney-General's Department, *Submission No. 218*, p. 1

88 Australian Federal Police, Submission No. 163, p. 15. See also Attorney-General's Department, *Submission No. 218*, p. 7

89 Victoria Police, *Submission No. 200*, p. 5. See also Attorney-General's Department, *Submission No. 218*, p. 7;

90 Corruption and Crime Commission of Western Australian, *Submission No. 156*, p. 11. See also Australian Competition and Consumer Commission, *Submission No. 192*, p. 1

> Anecdotal reporting from agencies is that increasingly requests for telecommunications data are not being met as carriers do not retain the particular telecommunications data requested. Unfulfilled requests waste agency resources, inhibit the making of requests, and can lead to investigations being stalled or abandoned with crimes going unsolved.[91]

5.100 Furthermore, the AGD disagreed with the submitters who suggested that a data preservation scheme would be more appropriate:

> Data preservation involves a 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.[92]

5.101 The AFP stated that a system of mandatory data retention would not mean any actual expansion in the powers of police and security agencies, and thus would not constitute an increased intrusion into the privacy of individuals:

> The development of a data retention proposal is intended to ensure a national and systematic approach is taken for the availability of non-content telecommunications data for investigative purposes. Data retention would not give agencies new powers. Rather it would ensure that existing investigative capabilities remained available and were adapted to these changes in industry.[93]

5.102 Furthermore, the AFP emphasised that there are constraints on the use of communications data in the current legislation:

> The TIA Act provides a high level of accountability and strict access requirements to obtain telecommunications information. These constraints recognise the responsibility of government to manage the competing interests of privacy and the expectations of the community that unlawful activity will be investigated and prosecuted, as well as the

91 Attorney-General's Department, *Submission No. 218*, p. 8.

92 Attorney-General's Department, *Submission No. 218*, p. 8.

93 Australian Federal Police, *Submission No. 163*, p. 16. See also NSW Government, *Submission No. 148*, p. 3

> important role that the telecommunications industry plays in supporting law enforcement and investigative activities.[94]

5.103 The AFP argued that retaining limited data on internet use bears some similarity to the current regime:

> Access to subscriber or account holder data is comparable in intrusiveness to open source information such as traditional fixed line telephone directories. It aids law enforcement in obtaining information to help establish further avenues of inquiry. For IP's where there are no analogous provisions to the directory service concept this non-content communications account data is imperative.[95]

5.104 Furthermore, the AFP, ASIO and the Australian Crime Commission (ACC) stated in their joint submission that they 'do not want the internet browsing history of every customer of an ISP to be retained'.[96]

5.105 These agencies recognised that browsing data may be considered the same thing as content, and thus noted that 'the TIA Act does not permit the disclosure of the contents or substance of a communication without a warrant', and further that they are not 'seeking any changes to this'.[97]

5.106 In regard to the difficulties of separating content from data in some cases, the AFP, ASIO and the ACC stated that the EU experience indicates that it is possible to separate the two, and further that 'the suggestion that it is not possible… is not consistent with information and feedback we have received from industry vendors'.[98]

5.107 Furthermore, the AGD told the Committee that there were safeguards in place in terms of separating data from content:

> But the safeguard is that a law enforcement agency has to satisfy internally that they are seeking information that would fall within a definition of data, and it is very clear that they cannot ask for anything that is content. The final decision on that is with the industry player, and if they cannot extrapolate data from content, then they cannot disclose that. In relation to data retention, there has never been a suggestion that it would be anything to do with web browsing where this problem has been identified.[99]

---

94 Australian Federal Police, *Submission No. 163*, p. 16.
95 Australian Federal Police, *Submission No. 163*, p. 16.
96 AFP, ASIO and ACC, *Submission No. 227*, p. 3.
97 AFP, ASIO and ACC, *Submission No. 227*, p. 8.
98 AFP, ASIO and ACC, *Submission No. 227*, p. 8.
99 Ms Catherine Smith, *Transcript*, 2 November 2012, p. 3.

5.108 At a public hearing, the AFP told the Committee that privacy was central to any new or reformed regime around data retention:

> I also want to be clear to the Committee that we understand the importance of individual privacy and we support this as a fundamental right in this country. I acknowledge that any reform in this area must be premised on maintaining appropriate levels of accountability for both intercepting agencies and industry in order to protect these rights.[100]

5.109 ASIO also told the Committee that there are currently safeguards in place when it comes to the use of communications data:

> ASIO accesses telecommunications-associated data (i.e. not content) from carriers/carriage service providers under internal authorisations which may only be made where the relevant ASIO officer is satisfied that the disclosure of the data specified in the authorisation would be in connection with the performance of ASIO's legal functions (and for no other purpose). [101]

5.110 Similarly, AGD noted the privacy protections that are a part of the TIA Act:

> The TIA Act contains numerous restrictions on the access, use and disclosure of communications lawfully obtained by agencies as well as comprehensive record keeping and reporting requirements with independent oversight. Broadly the prescriptive nature of the exceptions reflects the intrusive nature of the collection of the information as well as public expectations about how this information may be dealt with.[102]

5.111 Furthermore, ASIO noted that it always acts to ensure any access to communications data conform to the following guidelines:

- inquiries and investigations are to be undertaken using as little intrusion into individual privacy as possible;
- wherever possible, the least intrusive techniques of information collection should be used before more intrusive techniques; and
- any means used for obtaining information must be proportionate to the gravity of the threat posed and the probability of its occurrence.[103]

5.112 These protections notwithstanding, the AGD was supportive of the idea of inserting a privacy focused objects clause into the TIA Act as it 'will complement

100 Commissioner Negus, *Transcript*, 26 September 2012, p. 19.

101 ASIO, *Submission No. 209*, p. 3.

102 Attorney-General's Department, *Submission No. 218*, p. 10.

103 ASIO, *Submission No. 209*, p. 3.

the numerous safeguards built into the operation of the TIA Act by underpinning the ongoing interpretation of obligations under the Act.'[104]

Box 5.2 Law enforcement and national security agencies' use of communications data

'During a recent murder investigation there were a number of open lines of inquiry. When a human source provided information implicating a particular, previously unknown, person as responsible for the murder, telephone billing records were used to link the person nominated by the human source to another key suspect. The billing records also ultimately resulted in other lines of enquiry being discounted. The link between two of the principal offenders could not have been easily made without access to reliable telecommunications data. All the persons involved in that matter have been charged with the murder and associated offences and are currently before the courts.' (Letter from Attorney-General Nicola Roxon to the Hon Anthony Byrne MP, 17 September 2012, Appendix E.)

'For example, the [Queensland Crime and Misconduct Commission] CMC recently identified significant on-line sharing of child exploitation material by the principal target who declared that he was abusing children. The principal target was based in Queensland. The investigative team provided information to the ISP identifying the internet service being used. The Carrier was unable to advise the CMC of the subscriber details for the principal target, despite the on-line sharing of child exploitation material being less than 24 hours prior. This resulted in the CMC not being able to identify the principal target's precise location or true identity.' (Queensland Crime and Misconduct Commission, *Submission No 147*, p. 8.)

'During 2010 an Operation obtained prospective call associated data (CAD) Authorisations in relation to a person suspected of war crime offences contrary to section 7(2)(a) of the Geneva Conventions Act 1957, namely torture, inhuman treatment and wilfully causing suffering or serious injury. The suspect was wanted for extradition to Croatia to face trial for these offences and was attempting to avoid location. The AFP's CAD Authorisations did not involve the provision of any content of the suspect's communications however the information the non-content data provided investigators regarding the general geographical location of the targets mobile handset was instrumental in assisting the AFP successfully locate the target.' (Australian Federal Police, *Submission No. 163*, p. 17.)

'ASIO receives intelligence that a particular IP address is subject to cyber attack. ASIO would need to identify who that IP address is assigned to before it could warn them that their computer has been taken over and their information stolen, and to commence working with them to improve their IT security.' (ASIO, Australian Crime Commission and Australian Federal Police, *Submission No. 227*, p. 6.)

104 Attorney-General's Department, *Submission No. 218*, p. 10.

Security

Community views

5.113 A very large number of the objections to data retention related to the security of the data retained.

5.114 The Australian Privacy Foundation told the Committee that mandatory data retention was actually 'contrary to security objectives':

> Mandating the creation and storage of records of communications that would not otherwise be kept increases risk and vulnerability, creating additional 'honeypots' of valuable personal information that would be a target for hackers and risk multiple abuses.[105]

5.115 Mr Bernard Keane told the Committee that such 'honeypots' would be a tempting target for criminals, regardless of the protections in place:

> Even assuming a strong commitment to data security by providers and a statutory law for data protection by government, such repositories of information would be highly-prized treasure troves for organised crime, corporations and even foreign governments, and inevitably targeted by crackers.[106]

5.116 Senator Ludlam was also concerned about the potential for retained data to be hacked, noting:

> The vast amounts of data that would be retained poses a security threat because it would be vulnerable to theft and hacking by unauthorised persons or governments, private entities or criminal actors.[107]

5.117 The potential for hackers and other criminals to access retained data was also raised by Dr Bendall:

> Retaining the data would create a massive security risk if an ISP suffers a breach of security, including a significant risk of identity theft. The immense amount of data would also create an incentive for hackers to view ISPs as a target.[108]

5.118 Mr Nazer considered the risks posed by hackers and criminals to be far greater than those posed by government agencies accessing the data:

---

105 Australian Privacy Foundation, *Submission No. 162*, pp. 9-10.

106 Mr Bernard Keane, *Submission No. 117*, p. 15.

107 Senator Scott Ludlam, *Submission No. 146*, p. 6.

108 Victorian Privacy Commissioner, *Submission No. 109*, p. 8.

> If all Australian's communications are stored, a security breach will expose data from hundreds of thousands, or even millions, of customers at once. Thus, while there is only very small probability that a particular user's retained data will ever be useful to law enforcement, there is a much larger probability that the user's data will be the subject of a security breach.[109]

5.119 AMTA and the Communications Alliance noted at a public hearing that different C/CSPs have different capabilities when it comes to the security of any retained data:

> There are large entities within the industry that are very skilled and expert and experienced but, with the changing dynamics in this sector and the number of entities in the sector, under a data retention regime there would be a wide range of people who do not have those skills and there would be attendant risks to privacy.[110]

5.120 Furthermore, the security threats to the retained data may originate within the telecommunications service providers themselves. Electronic Frontiers Australia (EFA) raised a recent incident where Telstra allegedly harvested 'the URLs visited by customers of its NextG mobile service in order to provide this information to a foreign company'. According to EFA, this was illustrative of what could occur:

> This incident also demonstrates the risk of misuse of data by organisations for their own internal marketing purposes, which is a serious likelihood as they will seek to offset the significant costs associated with maintaining storage facilities for such large volumes of data.[111]

5.121 Vodafone also commented on the potential for security breaches, particularly if the URLs associated with browsing histories were retained:

> At the moment the information is not particularly interesting—it is just an event—so very few rogues would get a significant benefit from hacking into our billing records, whereas if it starts to be about which URLs you went to and tracking your location in a lot of detail then that would be quite problematic.[112]

5.122 EFA also noted that the security risks inherent in data retention vary according to the size and capabilities of the organisation retaining the data. In EFA's view,

---

109 Mr Daniel Nazer, *Submission No. 110*, p. 5.

110 Mr Chris Althaus, *Transcript*, 14 September 2012, p. 31.

111 Electronic Frontiers Australia, *Submission No. 121*, p. 5.

112 Mr Matthew Lobb, *Transcript*, 27 September 2012, p. 18.

given that 'reports of significant data breaches' occur 'almost daily', it is 'all but guaranteed' that the retained data would be compromised.[113] NSW Young Lawyers noted that, in recent months, several major companies have had customer data stolen, including Twitter, Yahoo and Linkedin.[114] Mr Quick noted his concern that, were Telstra to be similarly hacked, 'millions of Australians would have their personal information shared across the globe'.[115] Mr Daniel Black argued that C/CSPs do not have the 'sufficient skill level' to effectively protect data.[116]

5.123 The Internet Industry Assocation (IIA), an industry body representing a wide range of businesses and individuals involved in internet commerce, also saw a potential for any retained data to be hacked were it not stored securely, noting that:

> …during the period of the Inquiry the international hacktivist group Anonymous has been reported to have laid claims to be responsible for a number of attacks on networks and websites to obtain secure data in protest of the [data retention] proposal.[117]

5.124 The IIA raised a similar concern:

> Indeed most recently the vulnerability for further exposure was highlighted by the so-called hacktivist group 'Anonymous' who exposed data belonging to a prominent service provide.[118]

5.125 Furthermore, the IIA told the Committee that these attacks:

> …highlight the need to ensure that any proposed reforms imposed on C/CSPs are cognisant of the level of security mechanisms required to protect such data.[119]

5.126 Australian Lawyers for Human Rights also emphasised the security threat to any retained data, and noted that even large C/CSPs have some problems protecting their data from hacking:

> While the Committee's terms of reference which contain the proposals suggest guidelines on security of stored data, there have been a substantial number of recent breaches of security, resulting in the disclosure of private user data. These disclosures have not been by small

113 Electronic Frontiers Australia, *Submission No. 121*, p. 5.
114 NSW Young Lawyers, *Submission No. 133*, p. 11.
115 Mr Ian Quick, *Submission No. 95*, p. 14.
116 Mr Daniel Black, *Submission No. 97*, p. 6.
117 Internet Industry Association, *Submission No. 187*, p. 7.
118 Internet Society of Australia, *Submission No. 145*, p. 5.
119 Internet Industry Association, *Submission No. 187*, p. 7.

> businesses or organisations which lack the financial means to employ or train staff who are capable of managing secure environments.[120]

5.127 Mr R Batten related his concerns about the security of retained data from hacking attempts to the privacy of customers. Mr Batten argued that data retention diminishes the ability of individuals to protect their information:

> With data and identity theft now such a serious risk for the community, people have the right to protect their information. By mandating that all service providers retain user data, you remove the ability of citizens to effectively protect themselves from data and identity theft… This proposal would create virtual treasure troves for such thieves to raid and citizens would be able to do nothing to protect themselves. [121]

5.128 Likewise, Mr R Wigan was concerned about the enticing effect such a repository of personal data would have on criminals, noting that such a concentration of data places 'the community at risk', especially if it includes internet browsing data:

> The ISP databases containing these materials will be a honeypot like no other, and breaches inevitable... with all the passwords and other security protocols undermined thereby.[122]

5.129 Mr Mark Newton also expressed reservations about the security implications of creating 'enormous silos' of data:

> Data retention measures make our society less secure, by creating enormous silos of identifiable information in readily attackable locations. One single security breach risks losing everything, on a scale that leaves the United States' experience with Wikileaks in the shade. It is contemptible that the Government has learned no lessons from its own Wikileaks exposure, and still believes that concentrating large troves of leakable, attackable private data is a good idea.[123]

5.130 As a result of the concerns surrounding the ability of C/CSPs to effectively secure this data, and given that no C/CSP can ever be entirely certain the data is safe, Mr Daniel Black argued that it would be best if the data did not exist.[124]

5.131 Similarly, the IIA argued that the data collected should be kept to a minimum:

---

120 Australian Lawyers for Human Rights, *Submission No. 194*, p. 8.

121 Mr R Batten, *Submission No. 50*, p. 6.

122 Mr R Wigan, *Submission No. 178*, p. 2.

123 Mr Mark Newton, *Submission No. 87*, p. 9.

124 Mr Daniel Black, *Submission No. 157*, p. 12.

> Where ever there is an incentive for criminals to gain access to certain types of data then protecting and securing access to that data becomes more of a time, cost and technology burden. It is therefore important to ensure that data is not collected unnecessarily and that any proposals for retention of that data for extended periods can be justified by clearly demonstrating the necessity of that data to law enforcement activities.[125]

5.132 Australian Lawyers for Human Rights agreed with this view, noting that:

> Focusing on privacy, security standards and providing that the minimum amount of confidential data is retained for the smallest period of time possible would afford legitimate users a greater expectation of privacy, safety and less scope for exploitation of their data by unscrupulous third parties.[126]

5.133 According to Mr Bernard Keane, in some cases the data retained needs to be protected from lax processes within the organisations retaining the data:

> It has become clear over the last 18 months that even large corporations with strong incentives to keep data secure are vulnerable to cracking by organised crime, other states or activists, or simply lazy about security of personal information. This has included the Australia telecommunications provider Vodafone, which was revealed in early 2011 to have allowed – not via cracking or illegal action by outside actors, but through its own poor internal processes – widespread access to personal information about its 4 million customers.[127]

5.134 These concerns about security could result in any retained data having limited evidentiary value, according to Mr Keane:

> The recent history of personal information security in Australia and overseas suggests that both citizens and law enforcement agencies, intelligence agencies and prosecutors can have little confidence that information compiled under data retention laws would be effectively secured by all companies required to hold it, either from a privacy or from a investigative/prosecutorial point of view.[128]

5.135 Mr Black took a different approach, arguing that data breaches could lead to a loss of confidence of Australian internet users, and have a similar 'chilling effect' to that discussed in the previous section:

---

125 Internet Industry Association, *Submission No. 187*, p. 7.

126 Australian Lawyers for Human Rights, *Submission No. 194*, p. 8.

127 Mr Bernard Keane, *Submission No. 117,* p. 15.

128 Mr Bernard Keane, *Submission No. 117*, p. 15.

> Should any number of high profile leaks or revelations occur in relation to data from this data retention scheme, then the confidence of the Australian internet user would be compromised. Such loss in public confidence could result in a 'chilling effect' as users turn away from using the Internet for personal affairs. Alternately some people could turn to more secure means of masking their identity such as proxies or [virtual private networks] which could actually result in a net negative effect on law enforcement efforts as people train themselves to become more conscious of potential surveillance and learn how to more effectively bypass such surveillance, mask their identity or cover their tracks.[129]

5.136 Despite its opposition to mandatory data retention more generally, Blueprint for Free Speech argued that C/CSPs should not be responsible for storing any data retained, as they were 'not adequately equipped to protect large quantities of information'. They elaborated on this concern:

> Imposing an obligation on service providers to protect data is not an adequate solution to this problem. If anyone is going to keep data for government purposes — and we do not believe anyone should — it should be the Government, not the private sector, and appropriate constraints on its storage, access and disposal must be put in place.[130]

5.137 Senetas made a similar point, recommending:

> …that the government mandate how collected and retained data is secured – both in motion (when moving between locations) and at rest (when stored) through certified encryption technology and a regime for data breach notification to ensure the interests of all stakeholders is aligned.[131]

5.138 The Pirate Party emphasised that the nature of the potential threats to the security of the data would require some form of controls to prevent unauthorised access:

> Data retained under this policy would need to be stored in a secure manner which would be capable of preventing unauthorised access; either internally by employees of the company or organisation, or any external party (e.g. hackers, organised crime, foreign intelligence organisations, etc). Access controls would be required to prevent unauthorised access and to provide a thorough audit trail of all access to the system. Access controls and logging systems would need to be

129 Mr Daniel Black, *Submission No. 157*, p. 12.

130 Blueprint for Free Speech, *Submission No. 165*, p. 6.

131 Senetas, *Submission No. 237*, p. 1.

> designed in a manner which prevents tampering with those logs in order to guarantee fidelity of those records.[132]

5.139 Similarly, in addition to making sure the data was stored securely, iiNet saw a need for effective accountability measures to make sure the retained data was secure from misuse. iiNet argued that the government needs to 'assure Australians that data retained under any such scheme will be subject to appropriate accountability and monitoring mechanisms'.[133]

5.140 The Pirate Party noted that the data retained would 'need to be securely backed up' and that this backup system would be more complex than is the norm with backup systems. It posited that it would need to include the following:

- Backups older than the mandatory retention period would need to be purged in a similar manner to that of the data retention system.
- The backups would need to be protected by similar access controls to the data retention system.
- A means of ensuring that backups could not be 'restored' to another system by someone familiar with the system in order to freely access that data. Were that to occur they could retrieve any data, copy it and then wipe the system on which the backup had been restored to in order to conceal their actions.
- The amount of data retained, even when limited to traffic data, would be huge, even if compression and encryption were used when storing the data.[134]

5.141 The Pirate Party raised the need for the retained data to be securely destroyed once the retention period had expired:

> The data would also need to be stored in a manner such that data no longer covered by the mandatory retention period (e.g. more than two years old) can be securely destroyed.[135]

Law enforcement and national security agencies' views

5.142 In regard to the security of the data captured and retained, the AFP, ASIO and the ACC stated that analogous data is retained and protected by providers already:

> Some data, including personal information such as subscriber details, is already collected and retained by industry. The protection of this data remains paramount and is one of the main drivers behind the proposed

132 Pirate Party, *Submission No. 134*, p. 25.

133 iiNet, *Submission No. 108*, p. 13.

134 Pirate Party, *Submission No. 134*, pp. 25-6.

135 Pirate Party, *Submission No. 134*, p. 25

> Telecommunications Sector Security Reform which aim to increase the level of security in telecommunications networks.[136]

5.143 Furthermore, the AFP, ASIO and the ACC noted that under the National Privacy Principles telecommunications and internet service providers are already required to 'take reasonable steps to protect the personal information it holds from misuse, loss and from unauthorised access, modification or disclosure'.[137]

5.144 The Office of Australian Information Commissioner (OAIC) also related the need for retained data to be stored security to the proposed telecommunications sector security reform, noting that:

> …the OAIC supports possible amendments to the Telecommunications Act to create an industry wide obligation on all C/CSPs to protect their infrastructure and the information held on it or passing across it from unauthorised interference.[138]

5.145 The OAIC stated that this reform was particularly important in light of any future potential data retention regime.[139]

5.146 Dr Bendall told the Committee that Australia does not have a data breach notification scheme, stating:

> …where there is a major data breach there is no specific legal impetus for those organisations to notify the individuals involved in order to mitigate their losses—for instance, even where it involves financial information and that sort of thing. My interpretation of the privacy legislation is that the information security principle would include some responsibility to do that because it mandates them to take reasonable steps to prevent misuse or unauthorised disclosure. But it is not a specific, unlike in other jurisdictions…[140]

5.147 The AGD made a similar point, noting:

> Although many companies voluntarily report data breaches to the Office of the Australian Information Commissioner (OAIC), there is no requirement under the Privacy Act to notify the OAIC or any other individual in the event of a data breach.[141]

5.148 Similarly to Senetas, the OAIC suggested:

---

136 AFP, ASIO and ACC, *Submission No. 227*, p. 8.

137 AFP, ASIO and ACC, *Submission No. 227*, p. 9.

138 Office of the Australian Information Commissioner, *Submission No. 183*, p. 16.

139 Office of the Australian Information Commissioner, *Submission No. 183*, p. 16.

140 Dr Bendall, *Transcript*, 5 September 2012, p. 4.

141 Attorney-General's Department, *Submission No. 235*, p. 21.

> While notification of a data breach is currently not required by the Privacy Act, the OAIC suggests that it be considered as part of the proposed framework as an important mitigation strategy against privacy risks. [142]

5.149 In this regard, the AGD noted the role that mandatory data breach notification requirements could play:

> If enacted, mandatory data breach notification laws could complement the current legislative security requirements and a data retention regime in a least four ways by: (1) mitigating the consequences of a breach; (2) creating incentives to improve security; (3) tracking incidents and providing information in the public interest; and (4) maintaining community confidence in legislative privacy laws.[143]

5.150 As such, AGD noted that:

> …on 17 October 2012, the Attorney-General released a Discussion Paper entitled Australian Privacy Breach Notification which has sought views by 23 November 2012 on the possible introduction of mandatory data breach notification laws. […]The Government is currently considering responses to the discussion paper.[144]

5.151 Telecommunications sector security reform is discussed in Chapter Three of this report.

Feasibility and efficacy

Community views

5.152 Several submitters raised concerns about the feasibility of any potential data retention regime, and whether it would be an effective tool for law enforcement and national security agencies. For instance, the Law Council noted that it was 'not clear' how such a regime would be 'technically feasible or even useful'.[145]

5.153 In this regard, the Law Council raised several questions which it considered require an answer before any mandatory data retention regime is introduced:

> Once the data has been retained, how will it be matched with a particular person or communication? How will it be verified, and if it is used as evidence in court, how will it be protected from public disclosure? In

142 Office of the Australian Information Commissioner, *Submission No. 183*, p. 20.

143 Attorney-General's Department, *Submission No. 235*, p. 21.

144 Attorney-General's Department, *Submission No. 235*, p. 21.

145 Law Council, *Submission No. 108*, p. 38.

> addition, how will authorised agencies deal with the sheer volume of data retained when attempting to identify and request the data needed for a particular investigation?[146]

5.154 The Internet Society of Australia drew the volume of data that would be produced to the Committee's attention, noting that it would be difficult to deal with:

> …the capacity of modern network equipment to produce terabytes of data with attendant storage, management and analysis costs for both the communications service providers as well as law enforcement agencies should not be underestimated. The potential for law enforcement agencies to be swamped by data is very real.[147]

5.155 Likewise, Ms Stella Gray also commented on the volume of data that would be generated by capturing data on web browsing:

> A web browser hops through multiple IP addresses before reaching its destination to the page a user is navigating to. A web user is not in control of every IP address their web browser visits. Dozens of analytic trackers (measuring page view statistics) and advertising servers all run in the background on many websites that people frequent daily. That is a lot data that CSPs will need to be trusted to store, and a lot of data that law enforcement will need to sift through every time they are suspicions of someone.[148]

5.156 It should be noted that these views on feasibility, particularly as they relate to the amount of data that would be generated, were based on the assumption that the data would include URLs. Given that the Attorney-General has subsequently ruled out retention of data relating to internet browsing histories, the volume of data that would be retained is significantly reduced.

5.157 The Internet Industry Association raised the difficulties presented by the disaggregated nature of the data, particularly when its involves overseas countries:

> Another key issue is that service supply in the internet environment is disaggregated – there are many over the top (OTT) services ranging from things like Hotmail, Gmail, instant messaging, etc. to social networking such as Facebook, to Cloud storage and application hosting. If those

146 Law Council, *Submission No. 108*, p. 38.

147 Internet Society of Australia, *Submission No. 145*, p. 4.

148 Ms Stella Gray, *Submission No. 152*, p. 5. See also Pirate Party, *Submission No. 134*, p. 26.

> services are hosted outside of Australia, then data retention obligations have little to no effect.[149]

5.158 Telstra raised a similar issue at a public hearing, noting that even if Australian providers were required to capture and retain communications data, it would still not be able to capture data from over the top services like Skype and other voice over the internet telephony services, YouTube or Google. Telstra elaborated on the effect this would have:

> The simple evolution of technology would mean that we could not capture or provide any metadata or any content around something like Gmail, because it is Google owned, it is offshore and it is over the top on our network. The real value of what we might have in our data-retention scheme would be greatly diminished as soon as the good, organised criminals and potential terrorist cells knew that we were not capturing that data.[150]

5.159 However, iiNet told the Committee that it was still feasible to retain data relating to the source and destination of a particular communication, be it via traditional telephony or internet browsing:

> Technically anything is possible, it is just a question of how much money you want to throw at it. We have not said it is too expensive for us, but if we are forced to do it we will pass those costs through and that is normal.[151]

5.160 One possible method of capturing and extracting relevant data that was raised during the course of this inquiry was Deep Packet Inspection (DPI). Telstra noted that, should a mandatory data retention regime proceed:

> Where additional information was required that does not form part of Telstra's available pool of data then DPI could be one of the mechanisms available to meet these obligations.[152]

5.161 Telstra described its understanding of DPI:

> DPI equipment is typically deployed for the purposes of inspecting [IP] traffic in detail (deep inspection of the IP packets). The results of such an inspection may be used, along with policy enforcement technology, to manage certain types of traffic. […] DPI equipment may be deployed either 'in-line' to achieve policy enforcement outcomes (manage traffic

149 Internet Industry Association, *Submission No. 187*, p. 8.

150 Mr James Shaw, *Transcript*, 27 September 2012, p. 12.

151 Mr Stephen Dalby, *Transcript*, 27 September 2012, p. 51. See also Mr Chris Althaus, *Transcript*, 14 September 2012, p. 31; Mr Andrew Pam, *Transcript*, 5 September 2012, pp. 62-3.

152 Telstra, *Submission No. 238*, p. 1.

> based on its type or intended use, for example VOIP calls to the emergency call service) or DPI may be deployed 'off to the side'. Deploying DPI 'off to the side' is used when carriers are analysing (but not altering) IP traffic on their network.[153]However, Telstra noted that, while it 'would be possible for a carrier to capture and extract specific data using DPI', this would depend on the 'configuration of the DPI equipment' and it would mean that 'the volume of data subject to such capture and extraction would need to be constrained.'[154]

5.162 In the context of the *Draft Communications Data Bill* currently under consideration in the UK, the Joint Committee on the Draft Communications Data Bill noted:

> [DPI] would be used to isolate key pieces of information from data packets in a CSP's network traffic. The Home Office seemed confident that this was technically possible.[155]

5.163 The UK Joint Committee went on to note that the main technical challenge in terms of the feasibility of using DPI was 'dealing with encrypted data' captured from over the top service providers such as Gmail and Skype.[156]

5.164 In terms of whether DPI could be used to capture only data and not content, Telstra advised the Committee that:

> DPI is able to be configured to perform in a range of different roles. It may be possible to configure DPI equipment to examine header data without inspecting content. This configuration is highly dependent on the volumes of data and specific meta-data being sought…this is a question of traffic volumes, equipment performance and cost.[157]

5.165 In addition to stating that any potential data retention regime would be difficult, although not impossible, to implement due to the size and nature of the data needing to be retained, some groups also questioned whether the data would be effective in assisting to combat crime and terrorism.

5.166 For instance, Telstra raised the possibility that the means C/CSPs use to obtain the data could result in issues if it is presented as evidence in courts:

153 Telstra, *Submission No. 238*, p. 1.

154 Telstra, *Submission No. 238*, p. 1.

155 Joint Committee on the Draft Communications Data Bill, UK Parliament, *Draft Communications Data Bill,* December 2012, p. 30, viewed 18 December 2012, <www.parliament.uk/business/committees/committees-a-z/joint-select/draft-communications-bill/publications/>.

156 Joint Committee on the Draft Communications Data Bill, UK Parliament, Draft Communications Data Bill, December 2012, p. 30, viewed 18 December 2012, <www.parliament.uk/business/committees/committees-a-z/joint-select/draft-communications-bill/publications/>.

157 Telstra, *Submission No. 238*, p. 2.

> With very few exceptions, the current communications data that C/CSPs provide to the [law enforcement and national security agencies] can be validated, by defence counsel, by comparison with a defendant's telecommunications service account ('bill'). This will no longer be the case with 'created' communications data and Telstra believes that prosecutors are highly likely to be challenged in court to substantiate the accuracy of the data in evidentiary proceedings.[158]

5.167 EFA thought it 'highly questionable' whether data retention would aid in the investigation of terrorism, organised crime, or other serious illegal activities:

> It is worth noting that determined criminals will have little difficulty disguising or anonymising their communications. There are many relatively simple and very effective tools available that allow for the protection of communications from surveillance. While these tools will not be appealing to the vast majority of users as they can degrade connection speeds and reduce functionality, they are a viable option for those individuals that are determined to communicate in secrecy.[159]

5.168 Dr Bendall also expressed scepticism as to whether data retention would aid law enforcement and national security agencies due to the incentive this would provide to anonymise communications:

> There is some evidence that I am aware of, from having read various reports, of that happening in other jurisdictions where people have engaged less with electronic transactions or they have done it in a way where they have used various devices to encrypt and anonymise their transactions. One of the concerns with that, of course, is that that actually lessens the amount of information available to law enforcement organisations.[160]

5.169 iiNet was sceptical that data retention would be effective, due to the ease with which individuals can mask their identity. iiNet discussed one example with the Committee at a public hearing:

> We think it should be noted that in the internet environment a range of applications—apps—may run simultaneously over the same servers. These apps can emulate telephony or video communications, texts and other communications on the same platform using what is called internet protocol. Many of these apps allow a person wishing to mask either their

158 Telstra, *Submission No. 189*, p. 11.

159 Electronic Frontiers Australia, *Submission No. 121*, p. 4.

160 Dr Anthony Bendall, *Transcript*, 5 September 2012, p. 4.

> identity or location via wireless networks, proxy servers or other techniques to communicate in a covert way.[161]

5.170 Blueprint for Free Speech provided the Committee with a large volume of material relating largely to the efficacy of the EU Data Retention Direction in preventing crime. This material led Blueprint for Free Speech to conclude that:

> There is no evidence to suggest data retention would assist with the prevention of crime or terrorism. A 2011 study of Germany's Data Retention Directive found it had no impact on either the effectiveness of criminal investigations or the crime rate. Further, the study specifically found that countries *without* data retention laws are not more vulnerable to crime.[162]

5.171 According to one analysis conducted by Arbeitskreius Vorratsdatenspeicherun of the effectiveness of data retention in Germany provided to the Committee by Blueprint for Free Speech:

> Blanket data retention can actually have a negative effect on the investigation of criminal acts. In order to avoid the recording of sensitive information personal information under a blanket data retention scheme, citizens increasingly resort to internet cafes, wireless internet access points, anonymisation services, public telephones, unregistered mobile telephone cards, non-electronic communications channels and suchlike. This avoidance behaviour can not only render retained data meaningless but even frustrate targeted investigation techniques (eg wiretaps) that would possibly have been of use to law enforcement in the absence of data retention. Because of this counterproductive effect, the usefulness of retained communications data in some investigation procedures does not imply that data retention makes the prosecution of serious crime more effective overall.[163]

5.172 Mr Ben Lever cited the same report in his submission, noting that:

> It seems that under the current model - wherein most people are not surveilled, but certain persons suspected of crime are surveilled with warrants – many criminals will fail to take appropriate precautions, will use various telecommunication services, and will have that communication intercepted; however, under a data retention model - wherein all communication between citizens is monitored - criminals

161 Mr Stephen Dalby, *Transcript*, 27 September 2012, p. 47.

162 Blueprint for Free Speech, *Submission No. 165*, p. 6. Emphasis in original.

163 Arbeitskreis Vorratsdatenspeicherung, *Data Retention Effectiveness Report*, 20 May 2011. See also Mr Chris Berg, *Transcript*, 5 September 2012, p. 45.

> know this and deliberately avoid using telecommunications, to the detriment of those listening in.[164]

5.173 The Pirate Party agreed with these perspectives on efficacy, noting:

> It is likely that implementing data retention in Australia would have similar effects to those observed in Germany. The effect would not be to prevent organised crime or terrorism; it would merely result in greater concerted effort by organised criminals and terrorists to conceal their activities and communication. Meanwhile, the privacy and security of innocent, law abiding citizens would certainly be threatened and probably breached.[165]

5.174 Similarly, Mr Ian Quick told the Committee that those seeking to commit crimes will simply use alternative methods to communicate:

> If everyone knows all internet traffic is monitored, people with things to hide - or who are just irritated with the government spying on everyone - will simply bypass the monitoring by either hiding what they are browsing or who is doing the browsing.[166]

5.175 Furthermore, Mr Quick listed a range of ways to avoid having communications data retained:

- Browsing with a public internet service ie internet café, public library.
- Using some else's wifi connection (many are not properly secured).
- Using someone else's computer, ie a friends or work colleague.
- Using Tor or a similar online anonymity tool.
- Using any number of open proxy services.
- Using a [virtual private network] to somewhere outside of Australia and browsing over that.[167]

5.176 Tor, originally developed by the US Navy, uses:

> …a network of virtual tunnels that allows people and groups to improve their privacy and security on the Internet. It also enables software developers to create new communication tools with built-in privacy features. Tor provides the foundation for a range of applications that

164 Mr Ben Lever, *Submission No. 71*, p. 3.

165 Pirate Party, *Submission No. 134*, p. 28.

166 Mr Ian Quick, *Submission No. 95*, p. 14. See also Liberty Victoria, *Submission No. 109*, p. 7; Pirate Party, *Submission No. 213*, p. 3; Mr Patrick Potter, *Submission No. 212*, p. 4; Mr Daniel Judge, *Submission No. 157*, p. 12;

167 Mr Ian Quick, *Submission No. 95*, p. 14.

> allow organizations and individuals to share information over public networks without compromising their privacy.[168]

5.177 Virtual Private Networks (VPNs) are similar, in that they allow users to anonymise their internet use by 'encrypt and tunnel their traffic to another country for retransmission'.[169]

5.178 Likewise, Mr Johann Trevaskis notes that there are yet more ways in which persons seeking to do so can mask their identity during online communications:

- A person who intended to communicate something about a serious offence on the internet could generate 'millions' of dummy exchanges on the internet. While those exchanges would all be recorded and available to law enforcement, the person could die of old age before the last exchange had been checked out by law enforcement.
- Every person who objected to the data retention proposal on principle could generate 'millions' of dummy exchanges on the internet thereby making the data retention mechanism itself less practical.
- Data retention for stored communications that are email can be avoided by anyone merely by not using the ISP for email. This is to be recommended anyway because anyone who uses their ISP's email address then finds it more difficult to change ISP. That is, national economic efficiency says that people should not use an email address provided by their ISP. (Hence, for example, if a person used the gmail.com web site for all their email needs, the ISP would never see a single email. It is true that the web traffic to gmail.com instead would be seen by the ISP but that raises a number of practical difficulties for 'data retention' as compared with simply keeping copies of emails that are being handled by the ISP.)[170]

5.179 In light of the questions about whether any data retention regime would be worthwhile pursuing, Mr Nazer considered that a cost-benefit analysis should be conducted.[171]

Law enforcement and security agency views

5.180 The AGD responded to the concerns raised by telecommunications companies about over the top services, and the fact that the companies would have great difficulty capturing any data generated by these at a public hearing. The AGD noted that, because many of these over the top service providers are based in the United States:

---

168 Tor Project website, *About Tor*, viewed 15 November 2012, <www.torproject.org/about/overview.html.en>.

169 Mr Cameron Blackwood, *Submission No. 208*, p. 3.

170 Mr Johann Trevaskis, *Submission No. 62*, p. 9.

171 Mr Daniel Nazer, *Submission No. 110*, p. 3.

> There are ways through mutual assistance that we are able to access this information that has been held onto by the US providers. If they do retain the information offshore then it is unlikely that any law about data retention would apply to them, because the US law would actually override ours in that context. However, I think what we want to be satisfied of is that we can get access to the information. From what we understand from talking to the social network providers and these different providers in the US, they are happy to retain information as long as they are satisfied that a lawful order will come along at some point…[172]

5.181 Furthermore, the AGD noted that:

> We have been advised, in the policy development work we were previously doing on this, that, if there is an obligation under Australian law which has extraterritorial application for these foreign service providers, they will actually be required—and we can compel them—to assist us in relation to the services they provide to Australians or provide in Australia. There will have to be a geographical boundary around this sort assistance. We cannot go and ask for assistance about something which is happening in another country. But, if the assistance is related to communications which, at some point, pass through the Australian telecommunications system, the advice we have had—or that we are working on—is that generally they will be able to be compelled. There are certainly ways—some as simple as terms and conditions of service. If they are Australian terms and conditions of service when you sign up in Australia, they will have the force of Australian law rather than the force of US law.[173]

5.182 In regard to whether data retention would be an effective tool for law enforcement, the AFP told that Committee that it already is a vital tool. Furthermore, the AFP argued that, as the telecommunications sector changes, their ability to draw on communications data could potentially diminish:

> In the absence of urgent reform, agencies will lose the ability to effectively access telecommunications content and data, thereby significantly diminishing the collective ability to detect, investigate and prosecute threats to security and criminal activity. The diversification of the sector and technological change mean that while a greater array of non-content communications data is being created increasingly less is being retained. This negatively impacts investigations and is exploited by individuals involved in the commission of a range of serious offences including

172 Ms Catherine Smith, *Transcript*, 2 November 2012, p. 6.

173 Ms Catherine Smith, *Transcript*, 2 November 2012, pp. 6-7.

> cybercrime, terrorist activity and the exchange of child exploitation material.[174]

5.183 Given that, as stated by ASIO, the AFP and the ACC, communications data is 'essential for the majority of investigations':

> Loss of access to such data, for technical or legal reasons, would result in a loss of a fundamental investigative capability and the ability of security and law enforcement agencies to function effectively.[175]

5.184 The AFP considered that if data retention were *not* made mandatory, it would lose important capabilities that would result in:

- Limited ability to track and pursue offenders in a timely and effective way;
- Limited ability to conduct thorough and complete investigations;
- Inability to present best evidence to courts;
- Inability for police to react to some life threatening situations;
- Inability to follow through on potential leads and gather evidence and identify criminals, and
- Ability for criminal enterprises / organised crime groups to exploit this vulnerability.[176]

5.185 Thus, it was submitted that mandatory data retention will not necessarily result in a direct decrease in crime or terrorism, or a direct increase in clearance rates for criminal investigations, but that failure to mandate data retention will result in a diminution of law enforcement and security agencies' ability to fulfil their functions over time.

5.186 The AGD contested the view presented above that data retention in the EU has not assisted in investigations:

> The European Directive included a requirement for an evaluation of the application of the Directive and its impact which was to be prepared by the European Commission. This report was published on 18 April 2011. The report concluded that overall, the evaluation had demonstrated that data retention is a valuable tool for criminal justice systems and for law enforcement in the EU. The evaluation highlighted the lack of harmonisation in transposition of the directive in areas such as purpose limitation, retention periods and reimbursement of costs for industry (which is outside the scope of the Directive).[177]

---

174 Australian Federal Police, *Submission No. 163*, p. 18.

175 AFP, ASIO and ACC, *Submission No. 227*, p. 6.

176 Australian Federal Police, *Submission No. 163*, p. 17.

177 Attorney-General's Department, *Submission No. 218*, p. 9.

5.187 In response to concerns about criminals and terrorists turning to anonymisers like Tor and VPNs, the AGD told the Committee that:

> …we are well aware that there are, unfortunately, as you mentioned, Tor and suchlike ways to very cleverly evade any level of detection. The advice that I have had from agencies is that still being able to determine patterns of behaviour through access to data, even if it is to get feels of where they are setting up their blockages, gives a pattern of particular behaviour.[178]

Cost

5.188 A range of individuals and organisations – particularly C/CSPs – raised concerns in regard to the potential costs that any data retention regime could impose on C/CSPs and consumers of telecommunications services.

5.189 Telstra told the Committee that mandatory data retention would impose costs on C/CSPs:

> Telstra believes that the costs involved in any new data creation and retention regime will be significant and we will need to undertake large scale and detailed technical feasibility studies in order to understand what network, IT, vendor changes would be necessary and the costs of implementation and compliance with any new data creation and retention regime.[179]

5.190 However, Telstra also noted that:

> …it is impossible for Telstra to speculate on the significant costs or timeframes for compliance until Government has settled on the final form of any data retention regime.[180]

5.191 Mr Bruce Arnold, a lecturer in privacy law at the University of Canberra but submitting in a private capacity, discussed the reasons why mandatory data retention would impose costs on C/CSPs:

> It involves substantial costs for connectivity providers and content hosts in the public and private sectors (eg mobile phone service providers, webhosting services, libraries and universities) that are being asked to act as agents of the state. The network management systems used by those organisations typically feature billing and customer support facets. They are not concerned with long-term data storage, particularly storage in

178 Ms Catherine Smith, *Transcript*, 2 November 2012, p. 4.

179 Telstra, *Submission No. 189*, p. 11. See also Mr Zull, *Transcript*, 5 September 2012, p. 10.

180 Telstra, *Submission No. 189*, p. 12.

> forms that can be readily parsed by government agencies. Restructuring those systems to provide storage is non-trivial. Its implications involve a reduction of competition in the ISP sector, driving small ISPs out of business, and imposing a tangible regulatory burden on entrants to the social network service market along with other entities whose clients engage in electronic communication.[181]

5.192 EFA was similarly concerned about the costs to ISPs:

> ISPs log certain types of data as part of their normal operations and for the purposes of billing or providing other services. However, maintaining records of all accessible data for long periods of time, as well as servicing law enforcement requests to access the data, would impose costs far above those of normal operations.[182]

5.193 EFA also raised the cost estimates of UK C/CSPs in relation to the UK data retention scheme, and that these costs would inevitably be passed on to consumers:

> According to the UK Internet Service Providers' Association one large UK-based ISP estimated that it would cost £26m a year to set up a data retention system along with £9m a year in running costs. These are costs that would inevitably be passed directly on to Australian businesses and consumers in the form of higher connectivity and other service charges.[183]

5.194 AMTA and the Communications Alliance, basing their estimates on a data set similar to that of the EU Directive, attempted to quantify the likely setup costs to industry:

> In terms of setup costs industry estimates place the cost of capture and retention at close to one hundred million dollars. If the source and destination IP addresses were to be included in the capture and retain requirement the setup costs would be likely to approach a figure in the region of five hundred to seven hundred million dollars ($500 million - $700 million). The inclusion of a single additional data element has the potential to increase the capture and retention cost by tens of millions of dollars.[184]

5.195 Mr Nazer commented on the disproportionate effect mandatory data retention would have on smaller providers:

---

181 Mr Bruce Arnold, *Submission No. 137*, p. 2.

182 Electronic Frontiers Australia, *Submission No. 121*, p. 7.

183 Electronic Frontiers Australia, *Submission No. 121*, p. 7.

184 AMTA and Communications Alliance, *Submission No. 114*, p. 14.

> Smaller providers may not yet have the infrastructure to store the additional data. Large scale data storage requires expensive hardware, software, and data security expertise. This burden would be especially devastating to online service providers (such as social networking sites) that would not otherwise track the source data of communications. Moreover, many such companies are small start-ups and compete against companies from all over the world. Ultimately, the burden of data preservation could drive smaller communications companies out of business and send innovation overseas.[185]

5.196 At a public hearing, iiNet discussed the likely costs it would incur as a smaller provider. Basing this estimate on several assumptions, including that internet browsing data would be retained and that the volume of data generated by internet browsing will continue to increase at current rates:

> We believe $20 million for the IT equipment and $10 million for the data centre building. That is to meet current levels. If we amortise the hardware over two years and the data centre over ten years, we estimate a cost of about $1 million per month, plus power and overheads.[186]

5.197 Furthermore, Mr Dalby elaborated on the costs iiNet, and its customers, were likely to incur:

> …assuming that we are efficient about it, we would still need, because of the growth in traffic, to double that to cater for two years, and we are therefore looking at something more like $60 million for a start. That flows through to our customers. If we take that cost and determine what it will cost our customers when we pass it through, we are assuming an increase in the cost of a service—any one of our services—of about $5 per month. That would be an increase to our customers.[187]

5.198 Telstra advised the Committee that even larger providers will incur significant costs as a result of mandatory data retention:

> There are significant costs involved in all of this. There is a variety of costs. There is the cost of collating the data: collecting it off the network to begin with. Then there is the cost of putting it into storage. Then we have the cost of putting the security around that such that we have the integrity of the data in terms of the privacy of the customers and also the integrity of the data for evidentiary reasons for the agencies. Then we have the cost of making that data available to the agencies in a form that they can use for their investigations. Then, not to be overlooked—and it can be a

185 Mr Daniel Nazer, *Submission No. 110*, pp. 6-7.

186 Mr Stephen Dalby, *Transcript*, 27 September 2012, p. 48.

187 Mr Stephen Dalby, *Transcript*, 27 September 2012, p. 49.

> significant cost—at the end of the whole life cycle of this we have the cost of construction of that data in a way in which the customers and others can be sure that we are looking after their interests. Equally, on the other side—and I do not think that this is a point should be lost in the debate here—is that the agencies themselves will face significant costs in that they will have costs of accessing that data and then manipulating and investigating it in a way that makes it usable for them and also their own destruction costs at the end of the process.[188]

5.199 Vodafone commented that the costs expand significantly when URLs or internet browsing data needs to be captured and retained:

> In the case of data, the problem with data in this space is that a data stream can cover a whole number of URLs, a whole number of places you go onto the web. In location terms, if you are talking just about the cell, that is manageable; if you are talking about location within the cell and you are asking us to capture that data, that is an enormous expense. If it is as simple as a data session occurred and maybe if it went to the first URL then that is manageable. It would be expensive but it would be manageable. It if it was every single URL they went to, the amount of data that was used in particular downloading events and similarly with the location, that is when the costs across all your categories increase dramatically and capture becomes extremely expensive—actually having the systems to get information for the agencies that we would not otherwise be interested in storing or capturing.[189]

5.200 Similarly, iiNet noted that there is a big difference between capturing data relating to internet telephony and other internet services:

> …when iiNet provide a telephony service to a customer we have a similar range of information available to us. Whether we are providing that service over a conventional copper loop or via an internet service, we know the IP address of our customer making the call. When we start shifting into other internet content, if we provide that service via a mobile phone and we resell services from Vodafone's network and Optus's network, then all we see from those carriers is that our customer used the internet for an unstated purpose generally—there is a little exception to that. All we see as the reseller is that they used it for an unstated purpose and moved a certain amount of data. So we know that our customer did something, we do not know what they did. We do not know what website

188 Mr James Shaw, *Transcript*, 27 September 2012, p. 4.

189 Mr Matthew Lobb, *Transcript*, 27 September 2012, p. 21.

> they connected to; we do not know what they downloaded; we just know that access happened.[190]

5.201 Furthermore, a large part of these costs were not in retaining data, but rather in generating and retrieving the data to begin with, as much of the data to be retained in not currently captured for business purposes. According to Telstra:

> The storage of data is one of the lesser elements of the cost, although it does give rise, as I have said, to the privacy and security risks to protect that data and, not least, to protect its integrity also. But, certainly, the costs—for the system to retrieve it and to then create a way of retaining it and then making it accessible and then on the other side, the agency side, creating the ability for them to access, understand and use it—would be substantial, in our view.[191]

5.202 Ms Gray expressed a concern that potentially increased costs to consumers could 'deprive people of lower socio-economic backgrounds' of their ability to connect to the internet.[192]

5.203 In order to prevent any data retention regime negatively impacting C/CSPs and consumers, AMTA and the Communications Alliance noted their preference was for government to pay:

> …so far as data retention is concerned, we believe that any move down the track of additional data retention requirements should be based on full cost-recovery from government, just as is occurring today in the UK.[193]

5.204 Similarly, the Australian Interactive Media Industry Association recommended:

> The costs of fulfilling law enforcement requests should be met by the law enforcement authorities that request the information, and not directly or indirectly on service users.[194]

Committee comment

5.205 The Committee received a great deal of evidence on the issue of a mandatory data retention regime. In addition to the public evidence presented in this

190 Mr John Lindsay, *Transcript*, 27 September 2012, p. 50.

191 Mrs Jane Van Beelen, *Transcript*, 27 September 2012, p. 11.

192 Ms Stella Gray, *Submission No. 152*, p. 5.

193 Mr John Stanton, *Transcript*, 14 September 2012, p. 29.

194 Australian Interactive Media Industry Association, *Submission No. 198*, p. 4. See also Mr Lobb, *Transcript*, 27 September 2012, p. 19.

chapter, the Committee took classified evidence. Both the public and the classified evidence have informed the Committee's consideration of this issue.

5.206 Throughout its deliberations, the Committee has grappled with the issue of how best to reconcile the important national security interests which, the agencies were unanimous, would be served by an appropriate mandatory data retention regime, and on the other hand with the very significant alteration of the relationship between the state and the citizen, which the introduction of such a regime would arguably involve. As well, the Committee has had to approach this task in the absence of any draft legislation, which would have enabled it to focus its consideration with greater precision. This was a serious constraint upon the capacity of the Committee to form recommendations.

5.207 There is no doubt that the enactment of a mandatory data retention regime would be of significant utility to the national security agencies in the performance of their intelligence, counter-terrorism and law enforcement functions. As well, it is clear that changes in the data retention practices of telecommunications providers mean that much data which was previously retained, in particular for billing purposes, is no longer retained; this has resulted in an actual degradation in the investigative capabilities of the national security agencies, which is likely to accelerate in the future.

5.208 However, the utility of such a regime to the national security agencies is not the only consideration. 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.

5.209 Ultimately, the choice between these two fundamental public values is a decision for Government to make.

5.210 The Committee would have been in a better position to assess the merits of such a scheme, and the public better placed to comment, had draft legislation been provided to it.

5.211 There is a diversity of views within the Committee as to whether there should be a mandatory data retention regime. This is ultimately a decision for Government. If the Government is persuaded that a mandatory data retention regime should proceed, the Committee recommends that the Government publish an exposure draft of any legislation and refer it to the Parliamentary Joint Committee on Intelligence and Security for examination. Any draft legislation should include the following features:

- any mandatory data retention regime should apply only to meta-data and exclude content;

- the controls on access to communications data remain the same as under the current regime;
- internet browsing data should be explicitly excluded;
- where information includes content that cannot be separated from data, the information should be treated as content and therefore a warrant would be required for lawful access;
- the data should be stored securely by making encryption mandatory;
- save for existing provisions enabling agencies to retain data for a longer period of time, data retained under a new regime should be for no more than two years;
- the costs incurred by providers should be reimbursed by the Government;
- a robust, mandatory data breach notification scheme;
- an independent audit function be established within an appropriate agency to ensure that communications content is not stored by telecommunications service providers; and
- oversight of agencies' access to telecommunications data by the ombudsmen and the Inspector-General of Intelligence and Security.

Recommendation 42

There is a diversity of views within the Committee as to whether there should be a mandatory data retention regime. This is ultimately a decision for Government. If the Government is persuaded that a mandatory data retention regime should proceed, the Committee recommends that the Government publish an exposure draft of any legislation and refer it to the Parliamentary Joint Committee on Intelligence and Security for examination. Any draft legislation should include the following features:

- **any mandatory data retention regime should apply only to meta-data and exclude content;**
- **the controls on access to communications data remain the same as under the current regime;**
- **internet browsing data should be explicitly excluded;**
- **where information includes content that cannot be separated from data, the information should be treated as content and therefore a warrant would be required for lawful access;**
- **the data should be stored securely by making encryption mandatory;**
- **save for existing provisions enabling agencies to retain data for a longer period of time, data retained under a new regime should be for no more than two years;**
- **the costs incurred by providers should be reimbursed by the Government;**
- **a robust, mandatory data breach notification scheme;**
- **an independent audit function be established within an appropriate agency to ensure that communications content is not stored by telecommunications service providers; and**
- **oversight of agencies' access to telecommunications data by the ombudsmen and the Inspector-General of Intelligence and Security.**

Recommendation 43

The Committee recommends that, if the Government is persuaded that a mandatory data retention regime should proceed:

- **there should be a mechanism for oversight of the scheme by the Parliamentary Joint Committee on Intelligence and Security;**
- **there should be an annual report on the operation of this scheme presented to Parliament; and**
- **the effectiveness of the regime be reviewed by the Parliamentary Joint Committee on Intelligence and Security three years after its commencement.**

Hon Anthony Byrne MP

Chair