Chapter 4

Law enforcement challenges arising from online technological advancements

4.1 While new technology has created numerous privacy protection issues for individuals and regulators in the online environment (as discussed in chapter 3), developments in web-based technology have also made it possible for individuals and organisations to obscure their identities in a range of circumstances. This has created a number of challenges for law enforcement, and led to a recent controversial proposal from the Attorney-General's Department to require internet service providers to retain specified personal data for law enforcement purposes.

A data retention proposal

4.2 A number of submitters commented on reports and rumours that the Commonwealth Attorney-General's Department was considering implementing a mandatory data retention framework.[1] Prior to this inquiry, very little was known about the proposal, and submissions relied on information from scant news reports.

4.3 On 16 June 2010, an article was published on *ZDNet*, a website dedicated to technology news and discussion, reporting that the government was considering implementing a mandatory data retention regime similar to that in place in the EU.[2] The *ZDNet* report explained that:

> Data retention requires telecommunications providers, including internet service providers (ISPs), to log and retain certain information on subscribers for local enforcement agencies to access when they require it.
>
> The regime sees certain data logged before any suspect is identified, meaning that every internet users' online activities are logged by default.[3]

4.4 The report also noted that various ISP sources have claimed that the mandatory data retention regime 'could extend as far as each individual web page an internet user had visited', however the Attorney-General has denied that web browser history would be logged.[4]

4.5 Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, reiterated this point when she appeared before the committee, also explaining that the government is only

---

1 See for example Pirate Party, *Submission 4*, p. 6; Rule of Law Institute of Australia, *Submission 17*.

2 Ben Grubb, 'Inside Australia's data retention proposal', ZDNet, 16 June 2010 at www.zdnet.com.au/inside-australia-s-data-retention-proposal-339303862.htm (accessed 15 September 2010).

3 Ben Grubb, 'Inside Australia's data retention proposal', ZDNet, 16 June 2010.

4 Ben Grubb, 'Inside Australia's data retention proposal', ZDNet, 16 June 2010.

considering the retention of 'metadata' in relation to online communications, and not content.[5]

4.6 Ms Smith also emphasised that no decision has been made by government yet about whether to implement such a regime:

> I should say that no decision has been made by government about a data retention proposal.[6]

4.7 However, even at this early stage, there was a lot of confusion amongst witnesses about the specifics of the proposal and particularly about what information would and would not be retained. It seems that this is due to the limited range of organisations with which the Attorney-General's Department has consulted on the proposal at this stage.

4.8 A number of witnesses expressed concern about the lack of consultation during the development of the data retention proposal. For example, the Law Institute of Victoria (LIV) criticised the lack of consultation and transparency in the development of the policy to date.[7] Similarly, Dr Clarke, Chair, Australian Privacy Foundation (APF), informed the committee that the APF had been 'unable to get a place at the table in discussions on this matter'.[8] Dr Clarke continued:

> The government will not consult with us. They will consult with industry; they will not consult with civil society. When I say ‘us’, there is no reason why the APF has to be chosen as one of the organisations that government agencies interact with if there are other alternative organisations that cross into the same space. Civil liberties organisations do; in other contexts, consumer organisations do. Our argument is that civil society is not being engaged...[9]

4.9 Officers from the Attorney-General's Department disputed this, informing the committee that:

> We actually did consult with a broad range of people and have done so over some time within the industry.[10]

4.10 Ms Smith specified that the Department had consulted with the following organisations:

- ISPs;

---

5 Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, 1 December 2010, p. 53.

6 Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, 29 October 2010, p. 85.

7 Law Institute of Victoria (LIV), *Submission 9*, p. 1.

8 Mr Roger Clarke, Chair, APF, *Committee Hansard*, 1 December 2010, p. 9.

9 Mr Roger Clarke, Chair, APF, *Committee Hansard*, 1 December 2010, p. 9.

10 Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, 29 October 2010, p. 88.

- 'a wide range of the carrier network';
- bodies like the Internet Industry Association, the Communications Alliance and the AMTA [Australian Mobile Telecommunications Association];
- state and Commonwealth agencies including non-interception agencies like ASIC and ACCC; and
- the Office of the Privacy Commissioner.[11]

4.11 Ms Smith concluded that:

> It was very broad consultation within government and industry.[12]

4.12 Ms Smith explained that the purposes of consultations on the data retention proposal to date were 'for the purposes of developing a model, not to actually consult on a model'.[13] She argued that the proposal is not yet at a stage where it was appropriate to begin consultations with public interest and privacy advocacy organisations:

> In regard to the development of this particular issue, to date we are still not at a point where we think it is suitable to actually go out for that further consultation. In any policy development, you have to look at the outcome you are trying to achieve, the problem and how to address the problem, and you have to talk to the key stakeholders to see what is viable. When I say key stakeholders, I am talking about the agencies and the industry that are going to be primarily working to effectively build a solution. We do not want to pre-empt consultation with the public until we have a view around what that could possibly be.[14]

The EU mandatory data retention scheme

4.13 A model of mandatory data retention has existed in the European Union since March 2006. EU Directive 2006/24/EC requires Member States to adopt measures to ensure that metadata related to email, telephony and internet access is retained for between six months and two years.[15]

---

11 Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, 29 October 2010, p. 88.

12 Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, 29 October 2010, p. 88.

13 Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, 29 October 2010, p. 89.

14 Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, 1 December 2010, p. 48.

15 Directive 2006/24/EC of the European Parliament and of the Council, 15 March 2006, Official Journal L105, 13/04/2006, pp 54-63, at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:HTML, (accessed 18 October 2010).

4.14 Metadata is the information about the communication—the time and location—proving the fact that it occurred, rather than information about its content.[16] The EU Directive specifies that member states must require the retention of the following metadata:

- data necessary to identify the source of a communication (e.g. the name and address of the subscriber, phone number, user identification etc);
- data necessary to identify the destination of a communication (e.g. the phone number or email address of the recipient and their name and address if they subscribe to the same service/network);
- data necessary to identify the date, time and duration of a communication (including the time a user logs in and out of their internet access service);
- data necessary to identify the type of the communication;
- data necessary to identify users' communication equipment (e.g. the digital subscriber line (DSL) or telephone number);
- data necessary to identify the location of mobile communication.[17]

4.15 Article 5(2) provides that 'no data revealing the content of the communication may be retained pursuant to this directive'.

4.16 The EU Directive is still in the process of being implemented into national law, however in some countries where it has already been implemented, the laws have attracted significant controversy. For example, EFA noted:

> In March this year [2010], Germany's Federal Constitutional Court suspended German law implementing the Directive, ruling it was unconstitutional. Among other reasons, they cited a lack of transparency in the potential uses of the data.[18]

4.17 Mr Jacobs, Chair, EFA, informed the committee that in that case:

> The judge pointed out that even though it was just the data about communications there would be sufficient data gathered to enable the compilation of a profile on somebody's interests, which political party they might be leaning towards, et cetera, and that it was out of proportion to the needs of law enforcement.[19]

4.18 There has also been criticism of the Directive by other EU members and by prominent civil liberties organisations. For example, Mr Jacobs explained:

---

16 Ms Wendy Kelly, Director, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, 29 October 2010, p. 96.

17 Directive 2006/24/EC of the European Parliament and of the Council, 15 March 2006, Official Journal L105, 13/04/2006, pp 54–63, Article 5.

18 EFA, *Submission 20*, p. 2 (references omitted).

19 Mr Colin Jacobs, Chair, EFA, *Committee Hansard*, 29 October 2010, p. 62.

> Sweden has declined to implement the directive and so they are subject of a suit by the European Commission. In Romania a court found that the data retention provisions violated the European Convention on Human Rights. Also the ACLU [American Civil Liberties Union] and others have come out and claimed that data retention schemes such as this one are in violation of the Universal Declaration of Human Rights, and I believe that others have pointed out in their submissions to the committee that you would violate the National Privacy Principles in Australia including fairness, being unobtrusive, and collecting data only for its stated purpose.[20]

4.19 When asked about the impact of the EU directive on Google's global operations, Mr Flynn, Head of Public Policy and Government Affairs, Google Australia said:

> Our view is that any requirement to retain data to enable the investigation and detection and prosecution of serious crimes has to be proportionate to the resultant privacy impact and anonymity loss for internet users, as well as the costs to search providers of implementing something like that. I guess the key thing that we would take out of it is transparency. That is something that we emphasise in our efforts around privacy and we think it is very, very important.[21]

4.20 Mr Flynn continued:

> On the transparency front, we have launched a tool which you may have seen. It is a website and it actually gives details of the requests we get from governments around the world for two things. One is for data on users and the second is requests to remove content from our different services—like YouTube, for example. We think it is important because it is a step on the road to having greater transparency around these kinds of efforts and we think that is important. We would be interested to see others in industry take the same kind of approach.[22]

Current practice in Australia

4.21 Currently in Australia the data retained about an individual's online communication and internet usage may be used for law enforcement purposes in certain circumstances.

4.22 Australian Internet Service Providers (ISPs) are required to comply with the *Privacy Act 1988* with respect to personal information of their customers. However, they are also required to:

- assist authorities in enforcing the law;

---

20 Mr Colin Jacobs, Chair, EFA, *Committee Hansard*, 29 October 2010, p. 62.

21 Mr Iarla Flynn, Head of Public Policy and Government Affairs, Google Australia Pty Ltd, *Committee Hansard*, 29 October 2010, p. 5.

22 Mr Iarla Flynn, Head of Public Policy and Government Affairs, Google Australia Pty Ltd, *Committee Hansard*, 29 October 2010, p. 5.

- do their best to prevent their network from being used to commit offences; and
- ensure that authorities are able to intercept communications through their network in accordance with a validly issued warrant or order.[23]

4.23 Under Part 4-1 of the *Telecommunications (Interception and Access) Act 1979* the head, deputy head or authorised officer of a law enforcement agency may authorise the disclosure of documents or information if satisfied that the disclosure is reasonably necessary for the enforcement of criminal law, to impose a pecuniary penalty, or to protect public revenue.[24] The content or substance of communications (e.g. the contents of an email) cannot be obtained through this method, only the metadata.[25]

4.24 Authorisation may also be given for information likely to be collected in the future if the authorised officer is satisfied that such disclosure is reasonably necessary for the investigation of an offence punishable by imprisonment for at least three years.[26]

4.25 In order to obtain the content of online communications, law enforcement must obtain a warrant.[27]

4.26 Ms Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, advised the committee that while law enforcement agencies currently have the legal power to access the metadata from online communications, through the above described method, they can only do so if the relevant online service provider has retained the metadata, which there is currently no requirement for them to do.[28]

4.27 Ms Smith explained:

> The development of a data retention proposal is intended to ensure a national and systematic approach is taken for the availability of telecommunications data for investigative purposes. Data retention would not give agencies new powers. It would ensure that existing investigative capabilities remained available.[29]

---

23 ACMA, 'Internet Service Providers and Law Enforcement and National Security Fact Sheet', at www.acma.gov.au/WEB/STANDARD/pc=PC_100072 (accessed 28 September 2010).

24 *Telecommunications (Interception and Access) Act 1979*, ss 178 and 179.

25 *Telecommunications (Interception and Access) Act 1979*, s. 172.

26 *Telecommunications (Interception and Access) Act 1979*, s. 180.

27 Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, 29 October 2010, p. 86.

28 Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, 29 October 2010, p. 86.

29 Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, 29 October 2010, p. 86.

4.28 Ms Smith informed the committee that 'telecommunications data is an important investigative tool' which provides 'important leads for agencies, including evidence of connections and relationships'.[30] Law enforcement agencies have come to rely on the information kept by traditional methods of communication, such as fixed-line phones. Ms Smith explained:

> In the good old days when we all had a fixed-line phone there was information kept about—for example, I called someone, their phone number, for how long, how much it cost, all that sort of information.[31]

4.29 Data about that telephone call, which was collected by the telephone company for billing purposes, could then be used by law enforcement agencies following the procedure under the *Telecommunications (Interception and Access) Act 1979* for investigations, and to provide evidence justifying a warrant, for example for a telephone interception.

4.30 However, more modern forms of communication, such as Voice over Internet Protocol (VoIP), and email do not require providers to retain detailed information for billing purposes. Ms Smith told the committee:

> Internet based service providers tend to charge on the quantity of data used rather than on a per call basis. Over time, as telecommunications services such as voice-telephone migrate to voice-over-internet based services, less and less information will be retained and stored. Therefore, this means that traditionally available telecommunications data—as: 'Person X called person Y at this time'—may no longer be available.[32]

4.31 This means that the information is less likely to be retained by providers, and therefore, even though law enforcement may have the power to obtain it, it does not exist. Ms Smith explained:

> Despite the increased reliance on telecommunications data and the acknowledgement of the importance of telecommunications data, industry have confirmed that there will be changes to and reductions in the type of telecommunications data which will be retained into the future. They indicate that this is a natural evolution as a result of advances in technology and business models. For example, the telecommunications sector is quickly migrating from the traditional telephone network to internet protocol based networks.[33]

---

30 Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, 29 October 2010, p. 85.

31 Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, 29 October 2010, p. 98.

32 Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, 29 October 2010, p. 86.

33 Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, 29 October 2010, p. 86.

The government's proposal

4.32 The Department's proposal for a mandatory data retention scheme is 'intended to ensure a national and systematic approach is taken for the availability of telecommunications data for investigative purposes'.[34]

4.33 At this early stage, it is proposed that metadata 'about the process of communication, as distinct from its content' is retained by telecommunications and internet service providers.[35] Ms Smith, likened this metadata to the information retained by fixed-line phone companies for billing purposes—information about who contacted whom and when.[36]

4.34 Ms Smith emphasised to the committee that no decision has yet been made by government about a data retention proposal.[37] However, the Department has developed a 'data set' of the categories of information to be retained and has also engaged in discussions with industry about the data set and the period for which data would be retained.[38]

4.35 Those consultations revealed that:

> Advice from industry is that the majority of information that is included in that draft data set is currently retained. The issue is the length of time it is retained for. Some of the information is retained for days whilst some of it is retained for years. Some of that information is retained for audit and taxation purposes. Each individual industry participant currently holds a vast amount of information on every one of their customers.[39]

4.36 The Australian Federal Police (AFP) argued that a mandatory data retention scheme would not give the police additional powers, and that 'all we are asking for here is for the status quo to remain'.[40]

---

34 Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, 29 October 2010, p. 86.

35 Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, 29 October 2010, p. 85.

36 Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, 29 October 2010, p. 98.

37 Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, 29 October 2010, p. 85.

38 Ms Wendy Kelly, Director, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, 29 October 2010, pp 87–88. The Department provided the committee with a copy of the data set on a confidential basis.

39 Ms Wendy Kelly, Director, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, 1 December 2010, p. 50.

40 Assistant Commissioner Neil Gaughan, National Manager, High Tech Crime Operations, AFP, *Committee Hansard*, 29 October 2010, p. 87.

4.37 Assistant Commissioner Gaughan gave an example of when communications metadata has proven useful for law enforcement purposes, of Operation Centurion, a child pornography investigation:

> Centurion was a 2008 investigation in which the AFP received a number of referrals in relation to a particular activity. All we received to commence our investigation with were a number of Australian IP, internet protocol, addresses. As a result of that investigation we were able to go back to the metadata and ascertain that there were a large number of Australians who were involved in possessing child abuse material, because the ISPs had retained that information, which enabled us to then take actions in progress. As a result of that we executed in excess of 340 search warrants, we arrested in excess of 140 people, we seized 400,000 images and, more importantly from my perspective, we actually saved four children who were potentially at risk from child abuse. Without that metadata being retained, the AFP cannot do those types of investigations because we will not have that information to backtrack.[41]

4.38 In a private session, the committee heard details of a range of other ongoing investigations, which the Department and the AFP argued demonstrated why telecommunications data is an important investigative tool.[42]

Criticisms of the data retention proposal

4.39 The Attorney-General's Department's proposed data retention scheme attracted a great deal of criticism from witnesses and submitters. Major arguments against the proposal included that it:

- is inconsistent with the Privacy Act and its principles, and an unnecessary invasion of privacy generally;
- treats online and offline information differently without reason; and
- that it is unlikely to be effective or useful to law enforcement.

Breach of privacy principles

4.40 The Law Institute of Victoria (LIV) submitted that the proposal is inconsistent with the National Privacy Principles, as the information collected is unnecessary for both the functions of the ISP and in the vast majority of instances for law enforcement agencies.[43]

4.41 Specifically, the LIV identified that the proposal contradicts NPP 4.2 which relates to the time period that information is retained. NPP 4.2, which is included in proposed APP 11 in the government's Exposure Draft of amendments to the Privacy Act, provides that any personal data which is held by an organisation and is no longer

---

41 Assistant Commissioner Neil Gaughan, National Manager, High Tech Crime Operations, AFP, *Committee Hansard*, 29 October 2010, p. 89.

42 The committee conducted *in camera* hearing with officers from the Attorney-General's Department and the Australian Federal Police on 1 December 2010.

43 LIV, *Submission 9*, p. 1.

required for the purposes for which it was obtained, should be destroyed or de-identified. Ms Miller, Law Institute of Victoria, argued:

> Our opinion of that principle when applied to this policy is that this information could potentially be retained indefinitely because, basically, how is an ISP to know when a law enforcement agency no longer needs the information that is being collected for them?[44]

4.42 Ms Miller explained that requiring ISPs to retain enormous quantities of data for an extended period also leads to concerns about data security:

> There is also a concern about the sheer magnitude of the information that needs to be collected. That would all need to be stored somewhere, and the ISPs would have obligations under the National Privacy Principles to protect against the misuse of that data. The sheer scale of the information collected raises questions about how that would happen.[45]

4.43 The Privacy Commissioner, Mr Pilgrim, agreed that this was a concern:

> One of the issues that we face when we are looking at the retention and collection of personal information are the risks that are going to be associated with holding information for a long time when there may not be necessarily a clear or defined purpose for it. If you hold information—whether it be in databases or even if we look at it in the old style of a filing cabinet—and have it sitting around for a long time there is often a great risk that something could happen to it. It could be mishandled or used for inappropriate purposes.[46]

4.44 The LIV also raised concerns about the inconsistency of a data retention scheme with NPPs 8 and 10 (which are included in proposed APPs 2 and 3 respectively). Ms Miller argued that:

> The problem with the amount of information that is being collected about people is that it renders it almost impossible to be anonymous, because of the profile that can be developed about you. Also, some of the information may include 'sensitive information', as defined under the principles, which is things such as gender, political opinion, sexual preferences and health information.[47]

---

44 Ms Kathryn Miller, Member, Executive Committee; Member, Administrative Review and Constitutional Law Committee, Administrative Law and Human Rights Section, LIV, *Committee Hansard*, 1 December 2010, p. 24.

45 Ms Kathryn Miller, Member, Executive Committee; Member, Administrative Review and Constitutional Law Committee, Administrative Law and Human Rights Section, LIV, *Committee Hansard*, 1 December 2010, p. 24. The LIV submission made similar points by referring to the risks of data misuse, loss, and unauthorised access associated with requiring ISPs to retain such vast quantities of data; *Submission 9*, p. 2.

46 Mr Timothy Pilgrim, Australian Privacy Commissioner, *Committee Hansard*, 29 October 2010, p. 18.

47 Ms Kathryn Miller, Member, Executive Committee; Member, Administrative Review and Constitutional Law Committee, Administrative Law and Human Rights Section, LIV, *Committee Hansard*, 1 December 2010, p. 24.

4.45 Mr Jacobs, Chair, Electronic Frontiers Australia, noted that even though the government is not proposing to require ISPs to retain the content of online communications 'it is still very, very possible to use information of the kind that you described—when an email was sent and to whom—to build up a profile of somebody's habits'.[48] Mr Jacobs argued that this level of monitoring is unnecessary and invasive:

> Even if you do not know the content of the webpage that somebody viewed or the information that they posted in a form when they interacted with the website, just knowing what websites they go to and the fact that they are using them would enable you to build up a full profile of somebody's interests and habits.[49]

4.46 Mr Jacobs argued that the proposal has significant privacy implications, describing it as 'mass surveillance':

> The scheme as proposed has huge drawbacks as well for a society, and we have yet to hear a very good case for why such power should be necessary. We do not think it is hyperbolic to describe such a system has 'mass surveillance' because it does involve the most private communications of pretty much everybody in the country who uses the internet for communication—and if it is not everybody yet, it is going to be.[50]

4.47 Furthermore, Mr Jacobs argued that there was no justification for the proposal:

> I have not heard a compelling case that the system we have now is broken. With a warrant, with a court order, a law enforcement agency can go to a company that provides email services, like Google or Yahoo, or to an internet service provider and determine the identity of somebody who was at a particular IP address or view their emails. Until I hear a compelling case that that is just not enough data, that we need to go further back in time, that we need to have the information on everybody, whether or not they are of interest to law enforcement at the moment, we certainly cannot support the data retention proposal.[51]

4.48 The Privacy Commissioner, Mr Pilgrim, agreed with the general principles espoused by EFA, Liberty Victoria and the LIV, and was uncomplimentary about the proposal generally (although he did not comment on its specifics). Mr Pilgrim stated:

> A central principle in the Privacy Act is that agencies and organisations should only collect the personal information that is necessary for their functions or activities. Generally, my office would not support the collection of personal information on the chance that it may be just useful at some later date. As noted in our submission: … broad scale collection and

48 Mr Colin Jacobs, Chair, EFA, *Committee Hansard*, 29 October 2010, p. 68.

49 Mr Colin Jacobs, Chair, EFA, *Committee Hansard*, 29 October 2010, p. 69.

50 Mr Colin Jacobs, Chair, EFA, *Committee Hansard*, 29 October 2010, p. 61.

51 Mr Colin Jacobs, Chair, EFA, *Committee Hansard*, 29 October 2010, pp 71–72.

> retention of web browsing information could significantly impact on the privacy of individuals.[52]

4.49 Mr Pilgrim explained that it is important to ensure that for any data retention proposal:

> …we need to first of all understand what the exact problem is that is trying to be responded to by proposing something such as data retention. Is the response—be it setting a timeframe of six months, one year, two years or however many years—proportionate to the risk that is being proposed? You need to clearly understand what the risk is that we are trying to address by maintaining and keeping this information.[53]

4.50 Mr Pilgrim suggested that before any proposal is implemented a privacy impact assessment should be done to identify the risks to privacy, including requiring ISPs to hold personal data for an extended period of time.[54]

4.51 Mr Pilgrim also noted that:

> One of the other key issues that we would need to see addressed in any proposal for data retention is what the accountability mechanisms are going to be. Are there sufficient accountability mechanisms to ensure that if that information is being held it is being held securely and that it is not being misused or used for any other purpose that would be beyond the expectation of the individual? Finally, there should be review mechanisms to ensure that those processes are in place and to make sure that, for example, the risk that led to the establishment of those sorts of proposals is still there and still warrants that sort of retention.[55]

4.52 The importance of accountability and appropriate oversight was also emphasised by the Rule of Law Institute and Electronic Frontiers Australia.[56]

The proposal treats online and offline information differently

4.53 A second key concern of submitters and witnesses opposed to the data retention proposal was that it treats online and offline information differently. Ms Miller of the Law Institute of Victoria, noted:

> The best way of illustrating that is simply to point out that if this proposal was that all mail sent and received within Australia be logged and retained for seven years, or that all phones be intercepted and recorded, then I think

---

52 Mr Timothy Pilgrim, Australian Privacy Commissioner, *Committee Hansard*, 29 October 2010, pp 17–18.

53 Mr Timothy Pilgrim, Australian Privacy Commissioner, *Committee Hansard*, 29 October 2010, p. 19.

54 Mr Timothy Pilgrim, Australian Privacy Commissioner, *Committee Hansard*, 29 October 2010, p. 19.

55 Mr Timothy Pilgrim, Australian Privacy Commissioner, *Committee Hansard*, 29 October 2010, p. 19.

56 Rule of Law Institute of Australia, *Submission 17*, p. 2; Mr Colin Jacobs, Chair, EFA, *Committee Hansard*, 29 October 2010, p. 72.

> it is not stepping outside the bounds of my expertise to say that there would be significant public outcry. What we have here is the electronic equivalent, and it really means that the government is proposing to treat online privacy in a way that is different to offline privacy simply because the technology makes it possible.[57]

4.54 Ms Miller argued that there is no justification for treating online and offline privacy differently:

> I do not think that people make that distinction in their personal lives, their private lives, their professional lives. We do not think that it is appropriate that the parliament make a distinction in legislation between online privacy and offline privacy.[58]

4.55 Ms Miller surmised that when it comes to the possible benefits of technology, law enforcement agencies seem to ask 'Can we do it?' as opposed to 'Is it appropriate or reasonable to do it?', and use invasive investigative techniques because they can, rather than because it is appropriate.[59] She argued:

> The question should always be 'Is it appropriate and reasonable?' It should not be the case that just because we can we will.[60]

4.56 Mr Pilgrim, Privacy Commissioner, agreed that it is not appropriate to distinguish between online and offline privacy simply because it is possible:

> I would say that my position is that I would favour a consistent approach to data protection. I have not seen demonstrated necessarily why there should be any difference between whether the information is being handled online or offline. I have not seen a strong case put forward to explain that to me. [61]

4.57 In response to arguments by the Attorney-General's Department and the AFP that the proposal simply retains the status quo, requiring the retention of the same information that is available in relation to fixed-line telephone calls to be retained for

---

57 Ms Kathryn Miller, Member, Executive Committee; Member, Administrative Review and Constitutional Law Committee, Administrative Law and Human Rights Section, LIV, *Committee Hansard*, 1 December 2010, p. 24.

58 Ms Kathryn Miller, Member, Executive Committee; Member, Administrative Review and Constitutional Law Committee, Administrative Law and Human Rights Section, LIV, *Committee Hansard*, 1 December 2010, p. 25.

59 Ms Kathryn Miller, Member, Executive Committee; Member, Administrative Review and Constitutional Law Committee, Administrative Law and Human Rights Section, LIV, *Committee Hansard*, 1 December 2010, p. 25.

60 Ms Kathryn Miller, Member, Executive Committee; Member, Administrative Review and Constitutional Law Committee, Administrative Law and Human Rights Section, LIV, *Committee Hansard*, 1 December 2010, p. 25.

61 Mr Timothy Pilgrim, Australian Privacy Commissioner, *Committee Hansard*, 29 October 2010, p. 18.

online communications,[62] many witnesses strongly disagreed. For example, Ms Miller argued:

> The first distinction that I would make between call charge records and metadata of internet websites is that a phone number is just a phone number unless you have other information to interpret what the phone number is. And even if you know who owns the phone number and who the usual users of that number might be, you still know very little about the content of the conversation. I would suggest that when it comes to websites the website address and the type of information that is commonly found on that website can in fact be readily ascertained, even just from the metadata. So, even if the proposal is restricted to metadata as opposed to the actual web pages, there is still a great deal of extra information that can be obtained that you could not get from something like a call charge record.[63]

4.58 Another difference that Ms Miller noted was the important fact that data relating to fixed line telephone calls is collected for billing purposes, not law enforcement purposes. ISPs do not need to retain metadata for billing purposes, so that 'the only reason that they would be collecting this information is because it might be useful to law enforcement agencies not because of how they provide or charge for their service'.[64]

4.59 The LIV argued that this is inconsistent with key recommendations in the ALRC's report on Australian privacy law and practice,[65] submitting that:

> The large-scale collection of personal information by governments because it *may* be helpful to some government functions, rather than because it is necessary, constitutes a serious threat to online privacy. The power of the internet should not be used by governments to achieve measures of control that would not be possible without the internet.[66]

4.60 Ms King-Siem, Vice President, Liberty Victoria agreed:

> I understand security issues, but this is where you take a targeted approach where there is a justification and reasonable suspicion that that information is required, not collect information and worry about it later. I think there is a tendency both at government and at corporate level—and in fact it is

---

62 Assistant Commissioner Neil Gaughan, National Manager, High Tech Crime Operations, AFP, *Committee Hansard*, 29 October 2010, p. 87.

63 Ms Kathryn Miller, Member, Executive Committee; Member, Administrative Review and Constitutional Law Committee, Administrative Law and Human Rights Section, LIV, *Committee Hansard*, 1 December 2010, p. 26.

64 Ms Kathryn Miller, Member, Executive Committee; Member, Administrative Review and Constitutional Law Committee, Administrative Law and Human Rights Section, LIV, *Committee Hansard*, 1 December 2010, p. 26.

65 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108, 2008.

66 LIV, *Submission 9*, p. 2. Emphasis in original.

> perhaps just a natural tendency—to collect more than you need and then swallow it later.[67]

Will the data be useful for law enforcement

4.61 Finally, a number of witnesses and submitters questioned whether the data proposed to be retained would even be of use to law enforcement.

4.62 The LIV argued that the proposed regime would be 'unworkable for law enforcement agencies' due to the huge amounts of data collected.[68]

4.63 Ms Miller, LIV, also argued that the proposal is unnecessary as:

> Law enforcement agencies can currently apply for warrants to obtain information such as browsing histories from ISPs. If there is a concern that some ISPs do not contain significant browsing history, then the LIV considers that that can be dealt with on a case-by-case basis.[69]

4.64 There is also a risk that a data retention scheme will be ineffective because criminals and others wishing to evade detection will simply use the various mechanisms available to them to hide their online identity. The committee received evidence of various international online services dedicated to protecting the identity of domain name owners. For example, Fraudwatch International submitted that:

> Some domain registrars now provide a "Domain Privacy Protection" service, where the domain owners contact information is not listed in the WHOIS database, but is replaced by standard contact information for either the domain registrar or the privacy service, making it virtually impossible to actually find, or contact the real owner of the domain.[70]

4.65 This obviously makes it incredibly difficult to identify the owners of fraudulent phishing websites and shut them down. Mr Trent Youl, CEO, Fraudwatch International, informed the committee that:

> One of the issues we face when we are trying to have phishing websites taken down is that we find a hacked website and suddenly we cannot contact the website owner because their information is hidden. If the website owner has subscribed to this type of service that is apparently protecting their privacy and they do not have any contact information on their website, which many websites do not, it makes it very difficult for us sometimes to do our job and get these fraudulent websites taken down as quickly as possible.[71]

---

67 Ms Georgia King-Siem, Vice-President, Liberty Victoria, *Committee Hansard*, 1 December 2010, p. 16.

68 LIV, *Submission 9*, p. 2.

69 Ms Kathryn Miller, Member, Executive Committee; Member, Administrative Review and Constitutional Law Committee, Administrative Law and Human Rights Section, LIV, *Committee Hansard*, 1 December 2010, p. 24.

70 Fraudwatch International, *Submission 22*, p. 2.

71 Mr Trent Youl, CEO, Fraudwatch International Pty Ltd, *Committee Hansard*, 29 October 2010, p. 74.

4.66 Fraudwatch submitted that domain privacy protection:

> ...allows people to anonymously run websites which may be using dubious business practices, fraud, or theft [and] it allows criminals to hide their contact information and appear to be legitimate.[72]

4.67 There is a good chance that increased law enforcement monitoring of online communications will result in the proliferation of this, and similar options for internet users to hide their identity, provided that they are sufficiently tech-savvy. Mr Jacobs, Chair, EFA, explained:

> Given that you can host a website in any country and given that regulations vary, the way the internet works is anonymity is something that is probably going to apply to people who run websites as well as people who use them. So I think it is inevitable that such technology will exist. We will see a bit of an arms race when it comes to the technology itself and, perhaps, with the laws; but, no, I do not find that surprising. I think it is inevitable. We will have to have other ways to deal with it.[73]

4.68 There are already services available for consumers who wish to evade the EU's data retention scheme and other monitoring, such as Tor[74] and the Invisible Internet Project (I2P).[75]

Committee comment

4.69 The committee has a number of concerns, both with the Attorney-General's Department's data retention proposal itself, as well as with the way the consultation process has been handled so far.

4.70 There is a lot of misinformation and rumour about the scheme, and it seems to the committee that this is largely due to the Attorney-General's Department's narrow consultations on the issue to date. While industry has been consulted, there has not yet been any discussion with the broader community or public interest and civil liberties organisations. While the committee acknowledges the Attorney-General's Department's explanation for this,[76] the lack of information available to the public about the proposal has resulted in confusion, mistrust and fear about the proposal.

4.71 The committee's central concerns about the proposal are the very real possibilities that it is unnecessary, will not provide sufficient benefit to law enforcement agencies, and is disproportionate to the end sought to be achieved. The proposal has very serious privacy implications, even if one accepts the arguments of the Attorney-General's Department and AFP that the same information is already available for fixed-line telephone records. The fact is that much of the information

---

72 Fraudwatch International, *Submission 22*, p. 4.

73 Mr Colin Jacobs, Chair, EFA, *Committee Hansard*, 29 October 2010, p. 67.

74 www.torproject.org (accessed 12 January 2011).

75 www.i2p2.de (accessed 12 January 2011).

76 Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, 1 December 2010, p. 48.

intended to form part of the scheme does not need to be collected for any other purpose, so the only reason to retain it is the mere possibility that it may prove useful to law enforcement. This seems to the committee to be a significant departure from the core principles underpinning Australia's privacy regulation.

4.72 Furthermore, the committee considers that there is a very real risk that the most serious, tech-savvy criminals—particularly those involved in fraud and child pornography—will be able to evade monitoring in any respect as a result of technological developments.

4.73 Accordingly, the committee urges that prior to any proposal for data retention going any further, an extensive analysis of the costs, benefits and risks of such a scheme must be undertaken. Before pursuing such a scheme, it is incumbent upon government to:

- prove that the information is necessary to law enforcement agencies and justifies such a significant intrusion on the privacy of all Australians;
- quantify and justify the expense to ISPs and other companies which will be required to retain data under such a scheme;
- implement strong and appropriate accountability and monitoring mechanisms, and ensure that data retained under the scheme is able to be, and will in fact be, stored securely; and
- consult with a wide range of stakeholders on the proposal, including, but not limited to, civil liberties and public interest advocates, privacy policy experts such as the Australian Privacy Foundation, in particular.

Recommendation 9

4.74 The committee recommends that before pursuing any mandatory data retention proposal, the government must:

- **undertake an extensive analysis of the costs, benefits and risks of such a scheme;**
- **justify the collection and retention of personal data by demonstrating the necessity of that data to law enforcement activities;**
- **quantify and justify the expense to Internet Service Providers of data collection and storage by demonstrating the utility of the data retained to law enforcement;**
- **assure Australians that data retained under any such scheme will be subject to appropriate accountability and monitoring mechanisms, and will be stored securely; and**
- **consult with a range of stakeholders.**

4.75 The committee notes that the government is reviewing cyber security and cyber crime as part of its response to the recommendations of the recent House of Representatives committee report into Cyber crime (see paragraph 1.7).[77] The committee encourages the government to take the recommendations contained in this report into account in that review. The committee also expects the government will respond separately to the recommendations made in this report in the usual manner, noting that the Senate has declared that responses should be tabled within 3 months.[78]

Senator Mary Jo Fisher
Chair

Senator Doug Cameron
Deputy Chair

Senator Scott Ludlam

77 House of Representatives Standing Committee on Communications, *Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime*, June 2010, www.aph.gov.au/house/committee/coms/cybercrime/report.htm (accessed 7 March 2011); and the government response, 25 November 2010, www.aph.gov.au/house/committee/coms/governmentresponses/cybercrime.pdf (accessed 7 March 2011).

78 Senate Standing Orders, Procedural Order of Continuing Effect no 42, June 2009, p. 140, www.aph.gov.au/Senate/pubs/standing_orders/standingorders.pdf (accessed 6 April 2011).