Parliament of Australia
Department of Parliamentary Services

PARLIAMENTARY LIBRARY
INFORMATION ANALYSIS ADVICE

BACKGROUND NOTE 24 October 2012

Telecommunications data retention—an overview

Nigel Brew
Foreign Affairs, Defence and Security Section

Contents

Introduction

The Government's interest in establishing a data retention scheme appears to date back to at least early 2010 when rumours that the Government was considering such a scheme were revealed in June of that year.[1] The parliamentary inquiry into *The adequacy of protections for the privacy of Australians online* by the Senate Standing Committees on Environment and Communication which commenced a week after the rumours broke, focused part of its investigations on the issue of data retention. In its April 2011 report, one of the Committee's recommendations in relation to data retention, amongst a number of criticisms, was to 'consult with a range of stakeholders'.[2]

On 4 May 2012, the Government announced plans to review via public consultation a range of national security legislation, including that which covers 'lawful access to telecommunications … to ensure that vital investigative tools are not lost as telecommunications providers change their business practices and begin to delete data more regularly'.[3]

In July 2012 the Commonwealth Attorney-General's Department released a Discussion Paper, *Equipping Australia against emerging and evolving threats*, on the proposed national security reforms. Chapter One outlines the terms of reference for an inquiry by the Parliamentary Joint Committee on Intelligence and Security (PJCIS) into the 'potential reforms of National Security Legislation', namely the:

- Telecommunications (Interception and Access) Act 1979
- Telecommunications Act 1997
- Australian Security Intelligence Organisation Act 1979, and the
- Intelligence Services Act 2001.[4]

The Attorney-General has grouped the proposals into three categories—those the Government wishes to progress, those the Government is considering, and those on which the Government is expressly seeking the views of the Committee. Of the eighteen primary proposals and the forty-one individual reforms that they comprise, the suggestion that carriage service providers (CSPs) be required to routinely retain certain information associated with every Australian's use of the

1. B Grubb, 'Inside Australia's data retention proposal', *ZDNet*, 16 June 2010, viewed 16 October 2012, http://www.zdnet.com/inside-australias-data-retention-proposal-1339303862/
2. Senate Standing Committees on Environment and Communication, *The adequacy of protections for the privacy of Australians online*, The Senate, Canberra, April 2011, p.69, viewed 16 October 2012, http://www.aph.gov.au/Parliamentary_Business/Committees/Senate_Committees?url=ec_ctte/online_privacy/report/c04.htm
3. N Roxon (Attorney-General), *Public consultation for national security legislation reform*, media release, 4 May 2012, viewed 24 September 2012, http://www.attorneygeneral.gov.au/Media-releases/Pages/2012/Second%20Quarter/4-May-2012---Public-consultation-for-national-security-legislation-reform.aspx
4. Australian Government, *Equipping Australia against emerging and evolving threats,* Attorney-General's Department, Canberra, July 2012, viewed 12 September 2012, see http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/index.htm

Internet and phone services for a period of up to two years ('data retention') is the issue that seems to have attracted the most attention:[5]

> 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.[6]

This is despite the fact that the data retention proposal appears in the third category of reforms referred to above (as part of reforms to the *Telecommunications (Interception and Access) Act* 1979—the TIA Act), perhaps making data retention a less certain prospect than many of the other suggested reforms in categories one and two.

Debate on the pros and cons of this and other proposals has quickly gathered pace. However, while there has been a lot of talk about the cost, practicalities, and privacy implications of such a scheme, there has been comparatively little discussion of what sort of data is generated and what 'data retention' actually means.

By drawing on information related to similar proposals introduced in the United Kingdom (UK) in June 2012, this Background Note outlines the types of communications data generated by use of the Internet, email and phones, why law enforcement agencies want it retained, and what existing access law enforcement agencies have to such data. In this context, it also explores the reasons for the proposals, outlines some of the concerns and touches on some of the challenges involved. However, it does not specifically examine the arguments for and against a data retention scheme, or the growing debate over its privacy implications.

What is communications data?

Put simply, communications data is information about an electronic communication—a footprint left after accessing the Internet, sending an email, or making a phone call. It might, for example, include customer registration details, the date, time and duration of a communication, the phone number or email address of the sender and recipient, the amount of data up/downloaded, or the location of a mobile device from which a communication was made.

It is important to recognise, however, that it does not include the actual *content* of a communication. It is in this way that communications data differs from 'stored communications' (for example, emails and text messages that have already been sent) and telecommunications interception (listening to or recording telephone conversations), both of which are also dealt with very differently.

5. A Carriage Service Provider (CSP) is defined in the *Telecommunications Act 1997* as a person who supplies services for carrying communications. An Internet Service Provider (ISP) is one type of Carriage Service Provider which provides access to the Internet.
6. Australian Government, *Equipping Australia against emerging and evolving threats,* op. cit., p. 13.

The Attorney-General's Department's Discussion Paper notes that communications data:

> … is not defined in the TIA Act but is generally understood to refer to information about a communication that is not the content or substance of a communication. Data is increasingly understood as falling into two categories: subscriber data, which provides information about a party to a communication such as name or billing address; and traffic data, which relates to how a communication passes across a network, such as the location from which the communication was made.[7]

In a subsequent letter to the PJCIS clarifying the data retention aspects of the inquiry's terms of reference, the Attorney-General states:

> "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.[8]

The Australian Communications and Media Authority (ACMA) has previously described communications data similarly as being data which indicates the 'identity, source, path and destination' of a particular service, which may come from a variety of sources including:

- customer registration details;
- destination and origin email addresses for (user) target communications;
- calling line identification (for user access links);
- geographical location of a target service;
- network/traffic related data; and
- log files (for example, back up tapes showing details of a subscribers *[sic]* internet sessions, including files received).[9]

According to the *Telecommunications (Interception and Access) Act 1979 report for the year ending 30 June 2011*:

> While telecommunications data is not defined in the TIA Act, it is taken to mean anything that is not the content or substance of a communication. It can include:
>
> - subscriber information
> - telephone numbers of the parties involved in the communication
> - the date and time of a communication

7. Ibid., p. 25.
8. N Roxon (Attorney-General), letter to Anthony Byrne MP, Chair of the Parliamentary Joint Committee on Intelligence and Security, no date (2012), received by the PJCIS on 19 September 2012, p. 1, viewed 20 September 2012, see http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/index.htm
9. Australian Government, *Internet service providers and law enforcement and national security fact sheet*, ACMA, Canberra, 25 July 2012, viewed 24 August 2012, http://www.acma.gov.au/WEB/STANDARD/pc=PC_100072

- 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]

In the UK, where an extension to its existing data retention scheme was proposed earlier this year, communications data has been categorised into three types—subscriber data, use data, and traffic data. These are defined in more detail by the UK Government as follows:

> ***Subscriber Data*** – Subscriber data is information held or obtained by a provider in relation to persons to whom the service is provided by that provider. Those persons will include people who are subscribers to a communications service without necessarily using that service and persons who use a communications service without necessarily subscribing to it. Examples of subscriber information include:
>
> - subscribers or account holders' account information, including names and addresses for installation, and billing including payment method(s), details of payments;
> - information about the connection, disconnection and reconnection of services to which the subscriber or account holder is allocated or has subscribed to (or may have subscribed to) including conference calling, call messaging, call waiting and call barring telecommunications services;
> - information about the provision to a subscriber or account holder of forwarding/redirection services;
>
> information about apparatus used by, or made available to, the subscriber or account holder, including the manufacturer, model, serial numbers and apparatus codes.
>
> information provided by a subscriber or account holder to a provider, such as demographic information or sign-up data (to the extent that information, such as a password, giving access to the content of any stored communications is not disclosed).
>
> ***Use Data*** – Use data is information about the use made by any person of a postal or telecommunications service. Examples of use data may include:
>
> - itemised telephone call records (numbers called);
> - itemised records of connections to internet services;
> - itemised timing and duration of service usage (calls and/or connections);
> - information about amounts of data downloaded and/or uploaded;
> - information about the use made of services which the user is allocated or has subscribed to (or may have subscribed to) including conference calling, call messaging, call waiting and call barring telecommunications services;
> - information about the use of forwarding/redirection services;
> - information about selection of preferential numbers or discount calls;

10. Australian Government, *Telecommunications (Interception and Access) Act 1979 report for the year ending 30 June 2011,* Attorney-General's Department, Canberra, 2011, p. 10, viewed 6 September 2012, http://www.ag.gov.au/Documents/Final+TIA+Act+Annual+Report+2010-11+-+amended+after+publication+-+v5+(3).pdf

> ***Traffic Data*** - Traffic data is data that is comprised in or attached to a communication for the purpose of transmitting the communication. Examples of traffic data may include:
>
> - information tracing the origin or destination of a communication that is in transmission;
> - information identifying the location of equipment when a communication is or has been made or received (such as the location of a mobile phone);
> - information identifying the sender and recipient (including copy recipients) of a communication from data comprised in or attached to the communication;
> - routing information identifying equipment through which a communication is or has been transmitted (for example, dynamic IP address allocation, file transfer logs and e-mail headers – to the extent that content of a communication, such as the subject line of an e-mail, is not disclosed);
> - anything, such as addresses or markings, written on the outside of a postal item (such as a letter, packet or parcel) that is in transmission;
> - online tracking of communications (including postal items and parcels).[11]

Since the release of the Attorney-General's Department's Discussion Paper, and primarily in response to what she has labelled 'misunderstanding' and 'inaccurate reporting', the Attorney-General has repeatedly emphasised, in several different fora, that communications data (which she often describes as 'meta data') does not include the content of phone calls, emails, "tweets" or posts.[12] In her clarifying letter to the Chair of the PJCIS (received by the PJCIS on 19 September 2012, a month after submissions had closed and some two months after the release of the Discussion Paper) the Attorney-General explicitly states that 'the Government does not propose that a data retention scheme would apply to the content of communications'.[13]

However, some have argued that despite the Government's best intentions, from a technical perspective the distinction between content and non-content can be very difficult to maintain. In its submission to the PJCIS inquiry, the internet advocacy group Electronic Frontiers Australia has

11. UK Government, *Draft Communications Data Bill Privacy Impact Assessment*, Home Office, UK, 14 June 2012, pp. 21–22, viewed 30 August 2012, http://www.homeoffice.gov.uk/publications/counter-terrorism/comms-data-bill/communications-data-privacy-ia?view=Binary
12. See, for example, N Roxon (Attorney-General), 'Transcript of doorstop—Canberra', 4 September 2012, viewed 19 September 2012, http://www.attorneygeneral.gov.au/Transcripts/Pages/2012/Third%20Quarter/4September2012-TranscriptofdoorstopCanberra.aspx; N Roxon (Attorney-General), *Letter to the editor—Herald Sun*, media release, 7 September 2012, viewed 19 September 2012, http://www.attorneygeneral.gov.au/Media-releases/Pages/2012/Third%20Quarter/7-September-2012-Letter-to-the-editor-Herald-Sun.aspx; L Curtis, 'Interview on Capital Hill with Lyndal Curtis', *Capital Hill*, transcript, *ABC News 24*, 14 September 2012, viewed 19 September 2012, http://www.attorneygeneral.gov.au/Transcripts/Pages/2012/Third%20Quarter/14-September-2012-Interview-on-Capital-Hill-with-Lyndal-Curtis.aspx
13. N Roxon (Attorney-General), letter to Anthony Byrne MP, Chair of the Parliamentary Joint Committee on Intelligence and Security, op. cit., p. 1.

highlighted the difficulty in segregating content from non-content data, when, for example, email subject lines (content) may be inadvertently included in records of email headers (non-content).[14]

At the Senate Estimates hearings in October 2012, the AFP Commissioner, Tony Negus, acknowledged that 'there has been a lot of confusion in the media reporting about what is content and non-content data'.[15] However, perhaps at least part of this confusion has been due to the lack of detail in the information released about the proposal by the Government. It was not until the October Senate Estimates hearings that the Attorney-General's Department released any sort of official definition of what the Government means by non-content communications data in the context of the current data retention proposal, and then only in response to a request from Senator Scott Ludlam for such information.[16] Under the definition, communications data falls into two categories—'information that allows a communication to occur', and 'information about the parties to the communications'—and applies to Internet usage as well as both fixed and mobile phones.[17]

Ms Roxon has also stated on several occasions that communications data does not include records of website visits.[18] The Australian Security Intelligence Organisation (ASIO), too, has stated that 'in relation to internet usage ... we are simply not looking to track everyone's internet usage, or even to have data on people's internet usage stored'.[19] In evidence to the October Senate Estimates hearings, the Attorney-General's Department confirmed that communications data does not include records of web browsing, and that to obtain even a URL (website address) from a person's internet records, a warrant would be required (as with access to any other content-related data):

> **Senator LUDLAM:** That a URL, for the purposes of the way you are currently interpreting these requests, is content and not communications data?
> **Mrs Smith:** Correct.

14. Electronic Frontiers Australia Inc, submission to the Parliamentary Joint Committee on Intelligence and Security, *Inquiry into potential reforms of National Security Legislation*, submission no. 121, 2012, p. 5, viewed 15 October 2012, http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/subs.htm
15. Legal and Constitutional Affairs Legislation Committee, *Estimates*, Attorney-General's Portfolio, Supplementary Budget Estimates 2012–2013, 16 October 2012, p. 59, viewed 18 October 2012, http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22committees%2Festimate%2F0e2bb940-ccdc-4a20-b4e0-b3e6031771e8%2F0000%22
16. See ibid., pp. 59–60.
17. For a brief outline of the definition of data under each category, see Legal and Constitutional Affairs Legislation Committee, *Estimates*, Attorney-General's Portfolio, Supplementary Budget Estimates 2012–2013, tabled documents, 16 October 2012, 'Definition of Telecommunications Data', viewed 22 October 2012, http://www.aph.gov.au/Parliamentary_Business/Committees/Senate_Committees?url=legcon_ctte/estimates/sup_1213/ag/ag_tableddoc3.pdf
18. See, for example, L Curtis, op. cit.; R Epstein, 'Transcript of interview on ABC 774 Melbourne with Rafael Epstein and Joe Hockey', transcript, *ABC Radio*, 5 September 2012, viewed 19 September 2012, http://www.attorneygeneral.gov.au/Transcripts/Pages/2012/Third%20Quarter/5September2012-TranscriptofinterviewonABC774MelbournewithRafaelEpsteinandJoeHockey.aspx
19. David Irvine, Director-General, ASIO, cited in Legal and Constitutional Affairs Legislation Committee, op. cit., p. 106.

Mr Wilkins: That is right.[20]

This is despite the fact that at the end of September 2012 it was reported that the Commissioner of the NSW Police, Andrew Scipione, 'wants records of where people have been on the net as well—"to the extent that we know where people were or what their ISP was that they were using, or the URL that they did visit"'.[21]

Data use and retention

Telecommunications data is generated whenever someone makes a phone call, accesses the Internet, or sends an email. Traditionally, CSPs have used much of this data for their own business purposes, such as providing itemised billing, monitoring download limits, marketing (for example, promoting new or additional services to existing customers based on usage), and monitoring and maintaining their networks. As there is currently no requirement in Australia for carriage service providers to routinely retain communications data for law enforcement or national security purposes, without any further need for this information, CSPs would most likely then delete it. As one unnamed industry source puts it, '"Most ISPs that I'm aware of flush out the data they don't need to keep as quickly as possible after they've completed their billing operations because storing data costs money"'.[22]

Law enforcement agencies are able to access historical/existing telecommunications data (where it is still held by a CSP) by authorisation under the *Telecommunications (Interception and Access) Act 1979*, in cases where the information is considered reasonably necessary for the enforcement of the criminal law or a law imposing a pecuniary penalty, or the protection of public revenue.[23] Disclosures of prospective data (that which comes into existence after an authorisation is received and during the period it remains in force) can only be made in cases where it is considered reasonably necessary for the investigation of an offence that is punishable by imprisonment for at least three years.[24] Data can also be released under authorisation to ASIO in cases where it can be demonstrated that it would assist ASIO in the performance of its functions.[25]

20. Australian Greens Senator Scott Ludlam, Catherine Smith (Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department), and Roger Wilkins (Secretary, Attorney-General's Department), cited in ibid., p. 62.
21. Peter Lloyd, 'Police insist tougher data retention laws needed', *PM*, Australian Broadcasting Corporation (ABC radio), 27 September 2012, viewed 27 September 2012, http://www.abc.net.au/news/2012-09-26/police-insist-tougher-data-retention-laws-needed/4282156
22. Cited in B Grubb, 'New web spy powers: for and against', *Sydney Morning Herald*, 12 July 2012, viewed 12 July 2012, http://www.smh.com.au/technology/technology-news/new-web-spy-powers-for-and-against-20120712-21y34.html
23. See *Telecommunications (Interception and Access) Act 1979*, sections 177–179, http://www.comlaw.gov.au/Details/C2012C00381/e501a9c7-3036-4877-acf8-e3a6d7eb4e35
24. Ibid., section 180.
25. Ibid., sections 174–176.

Use by law enforcement

The Discussion Paper notes that communications 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', but does not elaborate any further on the particular use of such data by law enforcement and national security agencies.[26]

In its submission to the PJCIS inquiry, the Corruption and Crime Commission of Western Australia describes the importance of communications data to investigations:

> In simple investigations telecommunications data is used to provide information or evidence directly related to the investigation.
>
> In complex investigations telecommunications data is used to build a picture of suspected offences by identifying participants, establishing relationships and levels of contact. The use of telecommunications data to identify methods of communication is a crucial investigative tool.
>
> 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.[27]

The Australian Federal Police (AFP) makes a similar point in its submission:

> 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. Disclosure of non-content telecommunications data is one of the most efficient and cost effective investigative tools available to law enforcement.[28]

ASIO has also publicly described communications data as 'vital to law enforcement and security intelligence agencies', adding that it is 'used by agencies to determine who communicated with

---

26. Australian Government, *Equipping Australia against emerging and evolving threats,* op. cit., p. 14.
27. Corruption and Crime Commission of Western Australia, submission to the Parliamentary Joint Committee on Intelligence and Security, *Inquiry into potential reforms of National Security Legislation,* submission no. 156, 2012, p. 11, viewed 17 September 2012, http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/subs.htm
28. Australian Federal Police, submission to the Parliamentary Joint Committee on Intelligence and Security, *Inquiry into potential reforms of National Security Legislation,* submission no. 163, 2012, p. 15, viewed 17 September 2012, http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/subs.htm

whom, when, where to and where from' and that its use is 'often the most appropriate and proportionate response to investigative leads'.[29]

In one of the few examples (albeit, a dated one) to be provided by the Government in the current Australian context which demonstrates the use of communications data by police in a major investigation, the Attorney-General noted in a speech in early September 2012 the value of communications data to the investigation of the 1994 murder of New South Wales MP, John Newman:

> Many of you will recall the disturbing murder of Cabramatta MP John Newman in Sydney in 1994. Call charge records and cell tower information were instrumental in the investigation and subsequent conviction on Phuong Ngo. These records allowed police to reconstruct the crime scene.[30]

Another more generic example was cited by the Attorney-General in her letter to the PJCIS:

> 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 are are currently before the courts.[31]

In fact, agencies use communications data in a variety of ways for a range of different types of investigations, as the following detailed case studies from the UK (in which historical data was used) indicate:

> Case study: a terrorist investigation
>
> In June 2007 two separate attempted bomb attacks occurred in London's West End and at Glasgow airport. The subsequent police investigation used communications data extensively to establish the chain of events that led up to the attempted bombings, and as evidence in the trial. Phone records showed that the two conspirators established contact in February 2007. Mobile phones, that police established had been used by one of

29. Australian Security Intelligence Organisation, submission to the Parliamentary Joint Committee on Intelligence and Security, *Inquiry into potential reforms of National Security Legislation,* submission no. 209, 2012, pp. 1 & 4, viewed 21 September 2012, http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/subs.htm
30. N Roxon (Attorney-General), *Speech to the Security in Government Conference: protective security—policy in action*, 4 September 2012, viewed 17 September 2012, http://www.attorneygeneral.gov.au/Speeches/Pages/2012/Third%20Quarter/4September2012-SpeechtotheSecurityinGovernmentConferenceprotectivesecurity-policyinaction.aspx
31. N Roxon (Attorney-General), letter to Anthony Byrne MP, Chair of the Parliamentary Joint Committee on Intelligence and Security, op. cit., p. 2.

the conspirators before the attacks, were used as triggers for attempting to detonate the bombs in London's West End. This was later used as evidence to help to convict the bomber who survived his attack on Glasgow airport.[32]

Case study: a drugs arrest

A search of a Dutch-registered vehicle recovered 40 kilos of heroin, 150 kilos of amphetamine, 556 kilos of ecstasy tablets and 15 kilos of ecstasy powder with an estimated street value of £19 million. Eight mobile telephones were seized from the driver and the intended recipients. Combining physical evidence recovered from crime scenes with the associated communications data from these mobile phones enabled the investigating team to link the Sheffield based drug supplier and his brother and associates to the drugs seized from the lorry. This allowed further arrests and prosecutions to be brought.[33]

Case study: the murder of Rhys Jones

On 22nd August 2007, Rhys Jones, an 11-year-old schoolboy, was shot dead in the car park of the Fir Tree pub in Croxteth, Liverpool. He was walking home from football practice when he became the innocent victim of a feud between two rival gangs. Following a long and difficult investigation Sean Mercer was arrested, charged and subsequently convicted of the murder. Six other members of the gang were also convicted of assisting an offender and possession of prohibited firearms. Communications data was used to attribute telephones to each of the offenders, demonstrate association at key times and place individuals at specific locations. It also showed that the telephones of the key offenders were in the Kirby area some twenty minutes after the murder – helping to establish that Mercer and other convicted associates attended business premises in order to burn the gunman's clothing and douse him in petrol to remove firearms discharge residue. Communications data was essential to bringing the perpetrators to justice.[34]

Case study: protecting vulnerable children

A 10-month international police investigation into an online peer-to-peer network was coordinated by the Child Exploitation and Online Protection Centre (CEOP). The investigation centred on a network used by paedophiles to request, trade and create hundreds of child abuse images. Through the investigation 700 suspects were identified in 35 countries around the world. This was only possible through the use of communications data and covert internet investigative techniques. As a result over 30 children were rescued from sexual abuse.[35]

32. UK Government, *Protecting the public in a changing communications environment*, UK Home Office, UK, April 2009, p. 9, viewed 5 September 2012, http://www.official-documents.gov.uk/document/cm75/7586/7586.pdf
33. Ibid.
34. Ibid., p. 10.
35. Ibid., p. 9.

In 2010, a national survey was conducted of all police requests for communications data made in the UK over a two-week period (with the exception of requests related to terrorism investigations). The results indicated that investigations into 'other serious crime' (for example, violence against the person, robbery, fraud, forgery and firearms offences) and drug trafficking together accounted for more than half of the requests made (29 and 26 per cent, respectively), with investigations into 'other non-serious crime', sexual offences and murder making up the bulk of the rest.[36]

More recently, the UK Home Office has asserted that 'communications data has played a role in every major Security Service counter-terrorism operation over the past decade and in 95 per cent of all serious organised crime investigations'.[37]

In Australia, a total of 251 631 authorisations were made in 2010–11 under the TIA Act for access to communications data, over 240 000 of which were for the purposes of enforcing the criminal law.[38] Authorisations averaged around 264 000 a year over the three years from 2008–09 to 2010–11, and police agencies typically account for the vast majority of requests. Other bodies making requests included other enforcement agencies, such as the Australian Customs and Border Protection Service, and a variety of state and federal organisations, including, amongst others, Australia Post, Medicare Australia, the NSW Department of Primary Industries and the RSPCA. In the twelve months to 30 June 2012, the Australian Federal Police alone made 22 900 requests for historical communications data.[39]

Although not reliant on CSPs retaining communications data, it is worth noting that police are also able to access data in real time to help locate people in missing persons cases or search and rescue operations. Furthermore, recent developments mean that by the end of 2013 the National Emergency Alert System will enable the three major mobile phone service providers in Australia to issue emergency warnings to their subscribers in a natural disaster area based on the location of handsets.[40]

What is the problem?

As noted in the Discussion Paper, there is an ever-increasing number of ways to communicate and Australians are increasingly using multiple technologies and platforms to do so. According to ACMA, as at June 2011, there were in Australia:

36. UK Government, *Communications Data Bill*, background document, UK Home Office, UK, no date, p. 8, viewed 13 September 2012, http://www.homeoffice.gov.uk/publications/counter-terrorism/key-background?view=Binary
37. UK Home Office, 'Communications data', UK Home Office website, viewed 26 June 2012, http://www.homeoffice.gov.uk/counter-terrorism/communications-data/
38. Australian Government, *Telecommunications (Interception and Access) Act 1979 report for the year ending 30 June 2011*, op. cit., pp. 62–65.
39. Australian Federal Police, submission to the Parliamentary Joint Committee on Intelligence and Security, op. cit., p. 6.
40. See, for example, N Roxon (Attorney-General, Minister for Emergency Management) and P Ryan (Acting Premier of Victoria), *Optus to join National Emergency Alert System*, media release, 22 September 2012, viewed 25 September 2012, http://www.attorneygeneral.gov.au/Media-releases/Pages/2012/Third%20Quarter/22-September-2012---Optus-to-join-National-Emergency-Alert-System.aspx

- 29.28 million active mobile services (voice and data)—an increase of 13 per cent since June 2010[41]
- 10.54 million fixed-line telephone services—a decrease of 0.5 per cent since June 2010[42]
- 3.8 million home VoIP users—an increase of 31 per cent since June 2010[43]
- 10.9 million Internet service subscribers—an increase of 15 per cent since June 2010[44]
- 57 per cent of people using three communication technologies (fixed-line telephone, mobile phone and Internet)[45]
- 26 per cent of people using four communication technologies (fixed-line telephone, mobile phone, Internet and VoIP), and[46]
- 21 per cent of people (aged 14 and over) accessing the Internet via a mobile phone.[47]

In addition to this, for the quarter ending June 2011, the total volume of data downloaded (via dial-up, fixed-line and wireless broadband Internet services) increased some 76 per cent on the same period in 2010.[48] Over the same timeframe, the amount of data downloaded to mobile handsets increased by 415 per cent.[49] The fact that there are nearly three times as many mobile phone services in operation as there are fixed-line telephone services, combined with the rapid growth in VoIP use and data downloaded to mobile handsets, highlights the trend towards communication technologies becoming increasingly internet-based and highly mobile, potentially making communication itself more integrated, immediate, and transient.

Furthermore, as the Discussion Paper points out, it is now quite common that 'in a single communications session, a person may access many application services such as a Google search engine portal, a webmail account, a Facebook account, and an online storage repository', all of which involves several different service providers under separate accounts and with individual subscriber identities.[50] The ability of people to effortlessly and quickly move between different modes of communication combined with increasing volumes of data makes it complex and costly for law enforcement agencies to reliably identify and access communications.[51]

41. Australian Government, *Communications report 2010–11*, Australian Communications and Media Authority, Canberra, October 2011, p. 25, viewed 18 September 2012, http://www.acma.gov.au/webwr/_assets/main/lib410148/communications_report_2010-11.pdf
42. Ibid.
43. Ibid. VoIP stands for 'Voice over Internet Protocol' and enables real-time voice conversations over the Internet.
44. Ibid.
45. Ibid., p. 153—applies to people aged 18 and over with a fixed-line telephone service at home.
46. Ibid.—applies to people aged 18 and over with a fixed-line telephone service at home.
47. Ibid.—in the month of June 2011.
48. Ibid., p. 26.
49. Ibid.
50. Australian Government, *Equipping Australia against emerging and evolving threats*, op. cit., p. 21.
51. Ibid., p. 22.

This rapid expansion in the range and uptake of communications technologies is being reflected in the exploitation of such technologies by criminals, as noted by both the AFP in its submission to the PJCIS inquiry:

> Targets of interest continue to utilise a wider range of the telecommunications services available, to communicate, and to coordinate, manage and commit crimes. This proliferation of new services and ways to communicate is impacting on agencies' opportunities to utilise telecommunications content. There are also ever-increasing levels of technology-enabled crime and cybercrime such as child exploitation and online fraud for which historical, internet based non-content telecommunications data is critical evidence.[52]

and the Queensland Crime and Misconduct Commission (CMC):

> Many of the CMC's targets utilise multiple communication devices or multiple internet connections. Trying to obtain a complete understanding of a target's communications framework can therefore be challenging. In particular, the use of data services over multiple devices and multiple points of connectivity (for example, 3G, 4G and public or private WIFI services) makes the task of law enforcement increasingly complex.[53]

However, because CSPs are not currently required to store communications data longer than they need to for their own business purposes, law enforcement and security agencies claim they cannot always access the data they need for investigations. Due to the increasing volume of data handled by CSPs and moves by the telecommunications sector to deliver services via IP-based networks rather than the traditional telephone network, the information upon which police have relied in the past is increasingly not being stored for long enough, if at all.[54] Vodafone, for example, is believed to delete most of its communications data after 24 hours.[55] As the commercial use by CSPs of communications data diminishes, so too does the ability of law enforcement agencies to access such data:

> As carriers' business models move to customer billing based on data volumes rather than communications events (for example number of phone calls made), the need to retain transactional data is diminishing. Some carriers have already ceased retaining such data

52. Australian Federal Police, submission to the Parliamentary Joint Committee on Intelligence and Security, op. cit., p. 7.
53. Queensland Crime and Misconduct Commission, submission to the Parliamentary Joint Committee on Intelligence and Security, *Inquiry into potential reforms of National Security Legislation*, submission no. 147, 2012, p. 6, viewed 18 September 2012, http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/subs.htm
54. According to the Attorney-General, 'the main drivers' behind data of use to agencies no longer being kept are the 'increased use of internet protocol technology and the trend to charge customers based on volume of data sent or received rather than by transaction (such as call by call or message by message)'— N Roxon (Attorney-General), letter to Anthony Byrne MP, Chair of the Parliamentary Joint Committee on Intelligence and Security, op. cit., p. 2; see also Australian Security Intelligence Organisation, submission to the Parliamentary Joint Committee on Intelligence and Security, op. cit., p. 4, for an almost identical statement.
55. B Grubb, 'New web spy powers: for and against', op. cit.

> for their business purposes and it is no longer available to agencies for their investigations.[56]

The situation is similar in the UK, where, in 2009, the Home Office noted:

> Companies may no longer need to keep as much information on the way customers use their services: not all providers of communications services will continue to keep communications data as we know it now—records on who contacted who, when, and where. By making it cheaper and easier to provide services, Internet Protocol means that many companies have started to offer cheap, packaged or even free services. Some companies may no longer have any business need to keep information on service use by an individual subscriber.[57]

The Home Office currently estimates that 'about 25 per cent of communications data that could be useful to operations is not available to the police and security agencies at required timeliness or quality'.[58] The UK Government claims that in 2006, agencies were estimated to have had access to 90 per cent of all communications data in the UK.[59]

Unfortunately in Australia, neither the Government nor any of the law enforcement and security agencies appear to have attempted to quantify the problem they claim exists (with the exception perhaps of the Queensland CMC which at least offers an estimate—see below). The unclassified ASIO submission to the PJCIS inquiry simply argues the Government's case, sounding much like an extension to the Discussion Paper (to the extent that each document contains an almost identical statement). It does not offer any real evidence to suggest that it has experienced any problems accessing communications data when it has needed to. Similarly, there does not appear to be any publicly available source in which the AFP outlines what proportion of its large number of requests for communications data was unsuccessful due to the data no longer being available from CSPs. Such information would go a long way to demonstrating the true nature and extent of the problem, and significantly bolster the Government's case that data retention is necessary and appropriate.

While the Attorney-General's Department's Discussion Paper does not provide any figures to substantiate the Government's claims that communications data is becoming increasingly less available, law enforcement agencies themselves at least have plenty of anecdotal evidence to offer. For example, the head of the NSW Police Fraud Squad, Detective Superintendent Colin Dyson, has been quoted saying:

56. Australian Government, *Equipping Australia against emerging and evolving threats,* op. cit., p. 21.
57. UK Government, *Protecting the public in a changing communications environment*, op. cit., p. 19.
58. UK Home Office, 'Communications data', UK Home Office website, op. cit.
59. R Syal and R Norton-Taylor, 'Theresa May and Kenneth Clarke urge Tories to back security plan', *Guardian*, 5 April 2012, viewed 13 September 2012, http://www.guardian.co.uk/politics/2012/apr/05/theresa-may-ken-clarke-security-plan

> … by the time we receive a report of a crime very often the information that we require to track the offender is no longer there … In some cases the data is lost within 24 hours.[60]

The Victoria Police reports experiencing similar problems:

> Often, the incoming data from calls/SMS are crucial to the investigation of crimes such as stalking and breaching family violence intervention orders. These investigations are being hampered, or in many cases are unable to progress at all, due to the purging of such information from carrier's *[sic]* systems at the earliest opportunity.
>
> Carriers do not keep cell tower information for long and again, it varies from carrier to carrier. It is not uncommon for investigators to have the need to establish whether a particular suspect was in a certain area at a certain period of time. This type of information is often necessary for reasons such as establishing whether they have identified a legitimate suspect and disproving alibis.[61]

In its submission to the PJCIS inquiry, the Queensland CMC alludes to the problems posed by some of the technical challenges involved in capturing and storing certain types of information of use to law enforcement agencies:

> In some cases Carriers are unable to provide law enforcement with information critically needed to progress investigations. For example, the 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. The CMC estimates that the inability to identify targets for this reason occurs in approximately 1 in every 5 investigations, and the rate at which this is occurring is increasing ... While recognising that telecommunications networks are very complex and contain vast volumes of data, CMC investigations in these types of areas can be frustrated because of a Carrier's or ISP's inability to retain certain types of information.[62]

Commenting specifically on the merits of data retention, the head of the Australian Federal Police High Tech Crime Operations, Assistant Commissioner Neil Gaughan, has been reported saying:

60. Cited in B Grubb, 'New web spy powers: for and against', op. cit.
61. Victoria Police, submission to the Parliamentary Joint Committee on Intelligence and Security, *Inquiry into potential reforms of National Security Legislation*, submission no. 200, 2012, p. 16, viewed 18 September 2012, http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/subs.htm
62. Queensland Crime and Misconduct Commission, submission to the Parliamentary Joint Committee on Intelligence and Security, op. cit., p. 8.

> If we don't have a data retention regime in place we will not be able to commence an investigation in the first place. And it's already getting increasingly difficult.[63]

and:

> Without data retention laws I can guarantee you that the AFP won't be able to investigate groups such as Anonymous over data breaches because we won't be able to enforce the law.[64]

In her letter to the PJCIS, the Attorney-General highlights an example in which the unavailability of communications data soon after the communication took place hindered a corruption investigation:

> A corruption investigation revealed evidence of SMS communications between a police member and a member of an organised criminal network. Despite knowledge of the communications occurring recently, no data relating to the communications was available. The inability to obtain relevant information about the communications led to the loss of evidence which could have supported the investigation into the corrupt links.[65]

In responding to questions in a media interview about the capacity of the police to investigate the use of text messages and social media to incite violent protests in Sydney in mid-September, the Attorney-General used the opportunity to allude to the need for reform:

> … we want our law enforcement agencies to be able to use different forms of communications if that helps them put together a case against someone who's been involved in a violent protest and committed a crime.
>
> So I do think there are a lot of different trends coming together here. I want to make sure our law enforcement agencies have the powers that they need and can keep up with the new technology.[66]

Due to the often protracted and complex nature of major investigations by law enforcement and security agencies, the suggested retention period of two years has been publicly endorsed by at least two agencies. The Western Australia Police has stated that 'due to the protracted nature of serious

63. Cited in D Welch and B Grubb, 'Roxon doubts over security plans to store web history', *Sydney Morning Herald*, 21 July 2012, viewed 10 August 2012, http://www.smh.com.au/technology/technology-news/roxon-doubts-over-security-plans-to-store-web-history-20120720-22fel.html
64. Cited in H Barwick, 'AFP assistant commissioner calls for data retention laws', *Computerworld*, 1 August 2012, viewed 17 September 2012, http://www.computerworld.com.au/article/432334/afp_assistant_commissioner_calls_data_retention_laws/
65. N Roxon (Attorney-General), letter to Anthony Byrne MP, Chair of the Parliamentary Joint Committee on Intelligence and Security, op. cit., p. 2.
66. W Aly, 'Transcript of interview on ABC Radio National with Waleed Aly', *RN Drive*, transcript, *ABC Radio National*, 17 September 2012, viewed 18 September 2012, http://www.attorneygeneral.gov.au/Transcripts/Pages/2012/Third%20Quarter/17-September-2012-Transcript-of-interview-on-ABC-Radio-National-with-Waleed-Aly.aspx

investigations, a minimum retention period of 2 years is considered appropriate'.[67] In addition, ASIO states:

> Given complex investigations are measured in years rather than months, access to CAD [Communication Assisted Data] for a minimum period of two years is proposed to ensure that agencies can undertake effective investigations in accordance with their functions. Shorter periods of access carry the risk that agencies may be less able to access the critical intelligence that they require to progress an investigation.[68]

Data retention in the UK

Data retention in the UK has a comparatively long history. The UK has had a Voluntary Code of Practice on the Retention of Communications Data since 2003 (under the terms of the *Anti-terrorism, Crime and Security Act 2001*) which encouraged telecommunications companies to voluntarily retain communications data for longer than they normally would for their own business purposes, up to a maximum of 12 months, for the specific purpose of safeguarding national security.[69] Companies were reimbursed for the additional costs involved.

In 2006, the EU Data Retention Directive (2006/24/EC) was adopted by the European Union and came into force as a set of regulations in the UK in October 2007—these regulations set a mandatory retention period in the UK of 12 months for data associated with traditional (landline and mobile) telephony.[70] The regulations were superseded in April 2009 by a new set of regulations which extended the mandatory 12 month data retention requirement in the UK to include Internet activity.[71] Internet monitoring covers websites accessed, but not the specific pages.[72] However, the data generated by Internet phone calls, instant messaging and social networking websites was not included.[73]

---

67. Western Australia Police, submission to the Parliamentary Joint Committee on Intelligence and Security, *Inquiry into potential reforms of National Security Legislation*, submission no. 203, 2012, p. 13, viewed 21 September 2012, http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/subs.htm
68. Australian Security Intelligence Organisation, submission to the Parliamentary Joint Committee on Intelligence and Security, op. cit., p. 5.
69. UK Government, *Protecting the public in a changing communications environment*, op. cit.; UK Government, *Retention of communications data under Part 11: Anti-terrorism, Crime and Security Act 2001—voluntary code of practice*, Home Office, UK, viewed 10 September 2012, http://www.opsi.gov.uk/si/si2003/draft/5b.pdf
70. It is worth noting here that in several countries the domestic legislation implementing the EU Directive has been struck down by the courts, including in Cyprus, Bulgaria, Lithuania and the Czech Republic (see, for example, Human Rights Law Centre, submission to the Parliamentary Joint Committee on Intelligence and Security, *Inquiry into potential reforms of National Security Legislation*, submission no. 140, 2012, viewed 15 October 2012, http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/subs.htm)
71. P Ward and A Horne, *Interception of communications*, Standard Note SN/HA/6332, House of Commons Library, London, 17 May 2012, viewed 5 September 2012, http://www.parliament.uk/briefing-papers/SN06332.pdf
72. UK Government, *Communications Data Bill*, op. cit.
73. P Ward, *Internet surveillance*, Standard Note SN/HA/6304, House of Commons Library, London, 18 May 2012, viewed 5 September 2012, http://www.parliament.uk/briefing-papers/SN06304.pdf

The UK Brown Government attempted to reform communications data retention as part of its 'Interception Modernisation Programme' in 2008, before essentially being forced to abandon the initiative in response to public and industry outcry over reported plans to create a government-controlled centralised national database of internet-generated communications data at an estimated development cost of up to £2 billion.[74]

In June 2012, the UK Cameron Government introduced the Draft Communications Data Bill to establish 'an updated framework for the collection and retention of communications data by communication service providers to ensure communications data remains available to law enforcement and other authorised public authorities'.[75] The current government has been keen to distance its proposals from the previous government's failed Interception Modernisation Programme—'we are not proposing a single Government database to store all communications data to which the police would then have access'.[76]

The current proposed legislation aims to address the problem of rapid technological change and the exploitation of emerging technologies by criminals by ensuring authorities have access to communications data arising from internet-based communications and phones in the event that they need it, by requiring service providers to retain a greater range of information. While CSPs are already required to retain data relating to phone calls and messages sent via their own networks for 12 months, this Bill will reportedly require them to also keep data related to websites visited, messages sent on social media, web-based email, voice calls over the Internet and online gaming.[77]

The cost of the scheme has been estimated to be £1.8 billion over 10 years, at no cost to the private sector—telecommunications companies will continue to be reimbursed by the Government for costs associated with the retention and provision of communications data—and 'compares with an annual cost for policing alone of £14 billion'.[78] The value of the scheme's benefits over the 10 years is expected to be in the range of £5.0–6.2 billion (excluding benefits that cannot be monetised, such as 'illicit drugs seized, successful murder convictions and the prevention of terrorism').[79]

In a speech on 25 June 2012, the Director-General of the UK's Security Service (MI5), Jonathan Evans, made the following comments in support of the Bill:

---

74. Ibid.
75. UK Government, *The Queen's Speech 2012—briefing notes*, UK Cabinet Office, London, 9 May 2012, pp. 44–45, viewed 26 June 2012, http://www.cabinetoffice.gov.uk/sites/default/files/resources/Queens-Speech-2012-briefing-notes.pdf . According to the UK Parliament's website, 'a Draft Bill is published to enable consultation and pre-legislative scrutiny. After consultation and pre-legislative scrutiny has taken place, the Draft Bill may be introduced formally in [the] House of Commons or the House of Lords', *Draft Bills before Parliament* webpage, viewed 13 September 2012, http://www.parliament.uk/business/bills-and-legislation/draft-bills/
76. UK Government, *Communications Data Bill*, op. cit., p. 13.
77. 'Theresa May sets out plans to monitor internet use in the UK', *BBC News* online, 14 June 2012, viewed 27 June 2012, http://www.bbc.co.uk/news/uk-politics-18434112
78. UK Government, *Communications data legislation impact assessment*, UK Home Office, 11 May 2012, pp. 8–9 & 12, viewed 12 September 2012, http://www.homeoffice.gov.uk/publications/counter-terrorism/comms-data-bill/communications-data-ia?view=Binary
79. Ibid.

> ...the proposed legislation to ensure that communications data continues to be available to the police and security agencies in the future, as it has in the past, is in my view a necessary and proportionate measure to ensure that crimes, including terrorist crimes, can be prevented, detected and punished. It would be extraordinary and self-defeating if terrorists and criminals were able to adopt new technologies in order to facilitate their activities while the law enforcement and security agencies were not permitted to keep pace with those same technological changes.[80]

Cybercrime Legislation Amendment Act 2012

On 22 August 2012, the Australian Parliament passed the Cybercrime Legislation Amendment Bill 2012, which is primarily for the purposes of implementing the Council of Europe Convention on Cybercrime. Amongst other things, it enables Australian agencies to provide foreign law enforcement agencies with existing and prospective telecommunications data held/generated in Australia, provided certain conditions are met.

Stored communications

Communications such as email and text messages stored on a CSP's server after they have been sent (and any associated data) can currently be accessed by law enforcement agencies and ASIO under warrant. Although different from communications data, which is the focus of this paper and the subject of the current data retention proposals, it is worth noting the expanded powers the *Cybercrime Legislation Amendment Act 2012* grants to law enforcement and security agencies in relation to stored communications.

The Act requires CSPs to preserve stored communications at the request of certain domestic agencies, or the Australian Federal Police acting on behalf of certain foreign countries, in advance of a warrant to access the information being issued.

These so-called 'preservation notices' are designed to prevent communications such as emails and text messages from being destroyed before they can be accessed under a warrant, which takes time to organise. In its submission to the PJCIS inquiry, the Victoria Police notes in relation to stored communications that 'the opportunity to obtain crucial evidence is often lost in a short period of time', and outlines the sort of situation in which preservation notices may be useful:

> Victoria Police investigators were investigating the stabbing murder of a male. Call records showed recent contact between the deceased and telecommunications services utilised by two males. Further records obtained showed that on the night of the murder there were several text messages between these two males. Investigators seized a SIM card belonging to one of the males which contained a text message that appeared to implicate both in the murder. All other text messages between the two had been deleted.

80. *The Olympics and beyond*, Address at the Lord Mayor's Annual Defence and Security Lecture by the Director General of the Security Service, Jonathan Evans, Mansion House, City of London, 25 June 2012, viewed 13 September 2012, https://www.mi5.gov.uk/home/about-us/who-we-are/staff-and-management/director-general/speeches-by-the-director-general/the-olympics-and-beyond.html

> A stored communications warrant was unable to be applied for due to the unavailability of the content from the carrier. One of the males assisted investigators and became a witness against the other male who was charged with murder. The accused claimed it was the witness' idea to carry out the murder but the witness disputed this. Having access to all of the text messages between the two may have confirmed either person's story. The accused was subsequently acquitted at trial.[81]

There are two types of preservation notices—domestic ('which cover stored communications that might relate either to a contravention of certain Australian laws or to security') and foreign ('which cover stored communications that might relate to a contravention of certain foreign laws').[82] In turn, there are two types of domestic preservation notices—historic ('which cover stored communications held by the carrier on a particular day') and ongoing ('which cover stored communications held by the carrier in a particular 30-day period').[83] A foreign preservation notice only covers stored communications held by the carrier on a particular day. The Ombudsman and the Inspector-General of Intelligence and Security will have oversight in relation to preservation notices.

A similar system operates in the United States, for example, where the law as it applies to 'the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system' states that 'a provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process'. Records must be preserved for a period of 90 days, renewable for another 90 day period.[84]

The *Cybercrime Legislation Amendment Act 2012* is otherwise unrelated to the data retention proposals put forward in the recent Discussion Paper.

Concerns and objections

The data retention proposal (and the Discussion Paper) has attracted strong criticism on privacy and civil liberties grounds, with several submissions to the inquiry describing it as the most controversial of all the proposed reforms.[85] The main complaint with the Discussion Paper is that it lacks detail,

---

81. Victoria Police, submission to the Parliamentary Joint Committee on Intelligence and Security, op. cit., p. 18.
82. *Cybercrime Legislation Amendment Act 2012*, section 107G, p. 7—as the Act was not yet published at the time of writing, the page reference refers to the Bill as passed by both Houses, viewed 13 September 2012, http://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r4575_aspassed/toc_pdf/11114b01.pdf;fileType=application%2Fpdf
83. Ibid., pp. 7–8.
84. United States Code, Title 18, section 2703(f)(1), viewed 7 September 2012, http://uscode.house.gov/download/pls/18C121.txt
85. See, for example, Office of the Victorian Privacy Commissioner, submission to the Parliamentary Joint Committee on Intelligence and Security, *Inquiry into potential reforms of National Security Legislation*, submission no. 109, 2012, p. 7, viewed 15 October 2012, http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/subs.htm, and NSW Council for Civil Liberties, submission to the Parliamentary Joint Committee on Intelligence and Security, *Inquiry into potential reforms of National Security Legislation*, submission no. 175, 2012, p. 5, viewed

making it difficult to provide meaningful feedback, which therefore prevents proper scrutiny of the proposal:

> … the data retention proposal, which merits a single sentence in the Terms of Reference and is effectively completely absent from the Discussion Paper. This proposal is arguably the most egregious of the proposed new powers that the Committee has been asked to consider, and it is therefore difficult not to conclude that the absence of any detail in relation to this proposal represents a deliberate attempt on the part of the Attorney-General's Department to reduce the degree of public scrutiny to which this proposal would otherwise be subjected.[86]

The Gilbert + Tobin Centre of Public Law believes that the Discussion Paper 'fails to give enough attention to civil liberties' and states that 'it is vital that civil liberties are front and centre' of the debate.[87]

A number of submissions to the PJCIS inquiry also expressed some concern and surprise that the Discussion Paper did not even acknowledge the findings and recommendations of the April 2011 report of the inquiry into *The adequacy of protections for the privacy of Australians online* by the Senate Standing Committees on Environment and Communication, let alone address them.[88] Chapter Four of this report deals with the issue of data retention based on reports from June 2010 that the Government was seeking to introduce a mandatory data retention framework.

The Senate Committee expressed concern at the time about the 'very real possibilities' that a data retention scheme is 'unnecessary, will not provide sufficient benefit to law enforcement agencies, and is disproportionate to the end sought to be achieved'.[89] The report also recommended 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;

---

15 October 2012, http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/subs.htm

86. Electronic Frontiers Australia Inc, submission to the Parliamentary Joint Committee on Intelligence and Security, op. cit., pp.2–3. See also, for example, Human Rights Law Centre, submission to the Parliamentary Joint Committee on Intelligence and Security, op. cit., p. 7.
87. J Goh and N McGarrity, 'Just the beginning of a national security debate', *Inside Story*, Swinburne Institute, Swinburne University of Technology, 2 August 2012, viewed 3 August 2012, http://inside.org.au/just-the-beginning-of-a-national-security-debate/
88. See, for example, iiNet, submission to the Parliamentary Joint Committee on Intelligence and Security, *Inquiry into potential reforms of National Security Legislation*, submission no. 108, 2012, p.13, viewed 15 October 2012, http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/subs.htm, and Electronic Frontiers Australia Inc, submission to the Parliamentary Joint Committee on Intelligence and Security, op. cit., p. 8.
89. Senate Standing Committees on Environment and Communication, op. cit., p. 68.

- 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'.[90]

The above issues again featured strongly in many of the submissions to the current PJCIS inquiry, suggesting that consultation with stakeholders has not advanced much and that the Government has done little to address any of these recommendations before further embarking on its attempt to introduce a data retention scheme. The current opposition to data retention seems to revolve around three key objections:

- it amounts to mass blanket surveillance which targets everyone, and therefore lacks proportionality
- the case for data retention has (so far) not sufficiently been made, meaning the proposal has not been shown to be necessary, and
- it is vulnerable to 'function creep' in that the process and the information it collects could potentially be put to a range of uses in the future that are not intended now.

Each of these broad objections is discussed below in more detail.

Blanket surveillance

The Australian Greens Senator, Scott Ludlam, has stated that the data retention proposal is 'premised on the unjustified paranoia that all Australians are potential criminal suspects'.[91] Similarly, Electronic Frontiers Australia Inc stated in its submission to the current PJCIS inquiry that it 'does not believe that crime "prevention" can be used to justify a system that would collect data on the entire population, regardless of whether they are suspected of a crime or not'.[92] Similar objections have been raised in the UK, with the group Big Brother Watch claiming 'we are all suspects now'.[93]

The Office of the Victorian Privacy Commissioner has taken this concern further to argue that data retention is:

> …characteristic of a police state. It is premised on the assumption that all citizens should be monitored. Not only does this completely remove the presumption of innocence which

90. Ibid., p. 69.
91. Senator Scott Ludlam (Australian Greens Communications Spokesperson), *Data retention scheme a lunge for vast surveillance powers*, media release, 4 September 2012, viewed 15 October 2012, http://scott-ludlam.greensmps.org.au/content/media-releases/data-retention-scheme-lunge-vast-surveillance-powers
92. Electronic Frontiers Australia Inc, submission to the Parliamentary Joint Committee on Intelligence and Security, op. cit., p. 4.
93. Big Brother Watch, 'The Communications Data Bill: we are all suspects now' webpage, viewed 15 October 2012, http://www.bigbrotherwatch.org.uk/home/2012/06/communications-data-bill-misdirection.html

> all persons are afforded, it goes against one of the essential dimensions of human rights and privacy law: freedom from surveillance and arbitrary intrusions into a person's life.[94]

The Human Rights Law Centre has expressed concern that the large repository of private data which a data retention scheme would generate will risk creating a situation in which police and security agencies might trawl through private data 'in search of suspicion, not on the basis of it'.[95]

Data retention has attracted similar criticism in the UK, where the current UK proposal has been dubbed a 'snooper's charter'. The human rights group Liberty is running a 'No Snoopers' Charter' campaign and describes the proposals as:

> ... a shift from targeted monitoring of future communications on the basis of individual suspicion to the indiscriminate stockpiling of private data to be used by public agencies for a future unspecified purpose.[96]

In questioning the relative value of data retention as an investigative tool, several of the submissions to the PJCIS inquiry suggest that data retention represents a major erosion of privacy which does not justify what they believe to be relatively minor benefits. For example, the Office of the Victorian Privacy Commissioner has stated:

> This proposal would invade the privacy of every Australian citizen, erode democratic freedoms in Australia, and remove protections ensconced in human rights law, in the name of identifying and capturing a relatively small number of people.[97]

Electronic Frontiers Australia makes a similar point in stating that if implemented in full, the raft of proposals 'would amount to an unprecedented programme of mass surveillance that would invade the privacy of all Australians in the name of catching a tiny minority of serious wrong-doers'.[98]

In commenting generally on the range of proposed reforms, the Attorney-General has stated 'I think we should always taken credibly *(sic)* seriously any request made from law enforcement agencies, but they also need to be balanced with what is appropriate'.[99]

---

94. Office of the Victorian Privacy Commissioner, submission to the Parliamentary Joint Committee on Intelligence and Security, op. cit., p. 7.
95. Human Rights Law Centre, submission to the Parliamentary Joint Committee on Intelligence and Security, op. cit., p. 11.
96. Liberty, 'No snoopers' charter' webpage, viewed 27 June 2012, http://www.liberty-human-rights.org.uk/campaigns/no-snoopers-charter/no-snoopers-charter.php
97. Office of the Victorian Privacy Commissioner, submission to the Parliamentary Joint Committee on Intelligence and Security, op. cit., p. 11.
98. Electronic Frontiers Australia Inc, submission to the Parliamentary Joint Committee on Intelligence and Security, op. cit., p. 2.
99. 'Anonymous attack protests web laws, catches innocents', *7.30*, transcript, Australian Broadcasting Corporation (ABC TV), 1 August 2012, viewed 4 September 2012, http://www.abc.net.au/7.30/content/2012/s3558603.htm

Case not made

Several of the submissions to the PJCIS inquiry claim the Government has not provided sufficient evidence of the problem for law enforcement that it claims exists or adequately demonstrated that data retention is necessary to address the issue. For example, in its submission to the inquiry, iiNet notes:

> … there is no 'hard evidence' referred to in the Discussion Paper to support the assertion that changes in technology and the practices of C/CSPs [carriers/carriage service providers] are causing serious problems for law enforcement agencies. For example, no statistics have been provided on the number of attempts made by law enforcement agencies to obtain data from C/CSPs that were unsuccessful due to the C/CSP not having retained or collected the data that the law enforcement agency required.[100]

The Human Rights Law Centre agrees:

> … the Government has not provided any significant information to show that there is an overriding public interest in implementing a data-retention system.[101]

Given that, as one of its main concerns, the previous Senate Committee inquiry questioned the necessity of a data retention scheme, it is surprising the Government did not do more this time in its Discussion Paper to provide statistical 'hard evidence' of the nature and extent of the problem facing law enforcement, or to demonstrate that data retention is the answer.

'Function creep'

There is also significant concern amongst some submissions to the inquiry that if it goes ahead, a data retention scheme may be used for purposes in the future that are not envisaged or intended now. Even if, for example, website visits are excluded for now from any data retention scheme, they might be included in future revisions, as happened in the UK. As Electronic Frontiers Australia notes:

> EFA is also concerned that should such a system be put in place, the scope of acceptable uses would be too broad or would be broadened in response to political pressure. This could lead to retained data being used for unfocused 'fishing expeditions' by law enforcement, or for it to be made available for use in civil proceedings relating to alleged copyright infringement, or other matters.[102]

100. iiNet, submission to the Parliamentary Joint Committee on Intelligence and Security, op. cit., p. 9.
101. Human Rights Law Centre, submission to the Parliamentary Joint Committee on Intelligence and Security, op. cit., p. 7.
102. Electronic Frontiers Australia Inc, submission to the Parliamentary Joint Committee on Intelligence and Security, op. cit., p. 7.

The Office of the Victorian Privacy Commissioner agrees, suggesting that if a data retention scheme is introduced, the offences for which the data collected can be used should be 'defined in legislation', otherwise 'the potential for "function creep" is too great'.[103]

Electronic Frontiers Australia takes its argument a step further, warning that because under a data retention scheme, it will be known that communications data is kept for a defined period of time, 'the existence of retained data could potentially make that data accessible to third parties through court orders and other legal proceedings'.[104] For this reason, Electronic Frontiers Australia recommends that the use of retained data for civil purposes be expressly prohibited. Both Electronic Frontiers Australia and the Queensland Council for Civil Liberties have suggested that communications data should only be accessible via a warrant or judicial order. ASIO has rejected this idea, warning that 'if you have to get a warrant every time you need to access call-associated data, the whole system would get gummed up and come to a stop'.[105] The AFP too rejects this suggestion for similar reasons:

> So if you were wanting to grind the AFP to a halt, then you should implement a warrant scheme to actually do non-content data application—because 23,000 of these would require 23,000 judges to consider affidavits for those to be prepared and for those to be granted. It is an unrealistic expectation.[106]

At least part of the concern about 'function creep' stems from the fact that it is claimed patterns can be determined from the analysis of communications data over time which could be used to make assessments about a person's life and lifestyle. As noted by Electronic Frontiers Australia, this was one of the concerns raised by Germany's Federal Constitutional Court in striking down Germany's data retention laws:

> Even though the storage does not extend to the contents of the communications, these data may be used to draw content-related conclusions that extend into the users' private sphere... The observation over time of recipient data, dates, times and the place of phone conversations, it continued, "permit detailed information to be obtained on social or political affiliations and on personal preferences, inclinations and weaknesses".[107]

Furthermore, the crude nature of this information would be likely to result in a greater likelihood that such an assessment is wrong or misleading. Related to this is the possibility raised by Electronic Frontiers Australia, referred to earlier, that information which amounts to communication content, such as email subject lines, may get caught up with non-content communications data like email

103. Office of the Victorian Privacy Commissioner, submission to the Parliamentary Joint Committee on Intelligence and Security, op. cit., p. 9.
104. Electronic Frontiers Australia Inc, submission to the Parliamentary Joint Committee on Intelligence and Security, op. cit., p. 6.
105. David Irvine, cited in Legal and Constitutional Affairs Legislation Committee, op. cit., p. 105.
106. Tony Negus, AFP Commissioner, cited in ibid., p. 60.
107. Cited in Electronic Frontiers Australia Inc, submission to the Parliamentary Joint Committee on Intelligence and Security, op. cit., p. 6.

header information.[108] This suggests a possible technical difficulty in separating content from non-content data and raises the question of how this might be handled at a practical level when access to content and non-content information is governed by entirely different processes.

Overall, Senator Ludlam suggests that 'the Committee should reject the data retention proposal outright as impractical, dangerous, and a serious erosion of the legal and human rights of Australians'.[109]

Cost and other challenges

A number of CSPs and their representative bodies have raised concerns about the cost and technical challenges involved in implementing a data retention scheme, with some noting the lack, so far, of any cost-benefit analysis.[110] For example, in its submission to the PJCIS inquiry, Telstra states:

> 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.[111]

In a joint submission to the PJCIS inquiry, the Australian Mobile Telecommunications Association and the Communications Alliance report that basic set-up costs for 'capture and retention' are likely to be around $100 million.[112] They estimate that if 'source and destination IP addresses' were to be included, the cost would more likely be in the range of $500–700 million, and that the addition of a 'single additional data element' would increase the overall cost by tens of millions of dollars.[113]

---

108. Ibid., p. 5.
109. Senator Scott Ludlam, submission to the Parliamentary Joint Committee on Intelligence and Security, *Inquiry into potential reforms of National Security Legislation*, submission no. 146, 2012, p.7, viewed 15 October 2012, http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/subs.htm
110. On the issue of cost-benefit analysis, see, for example, Internet Industry Association, submission to the Parliamentary Joint Committee on Intelligence and Security, *Inquiry into potential reforms of National Security Legislation*, submission no. 187, 2012, viewed 20 September 2012, http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/subs.htm, and Electronic Frontiers Australia Inc, submission to the Parliamentary Joint Committee on Intelligence and Security, op. cit., p. 4.
111. Telstra, submission to the Parliamentary Joint Committee on Intelligence and Security, *Inquiry into potential reforms of National Security Legislation*, submission no. 189, 2012, p.11, viewed 18 September 2012, http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/subs.htm
112. Australian Mobile Telecommunications Association and the Communications Alliance, submission to the Parliamentary Joint Committee on Intelligence and Security, *Inquiry into potential reforms of National Security Legislation*, submission no. 114, 2012, p.14, viewed 19 September 2012, http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/subs.htm
113. Ibid.

Macquarie Telecom Pty Ltd notes that 'as the volume of data being created increases there is a significant and increasing cost in data storage and retrieval which *prima facie* would be borne by industry' and states its concern about 'any data retention regime which would impose a significant additional cost to industry'.[114] Similarly, the Internet Society of Australia predicts 'an increase in capital and operational cost with attendant labour force requirements' and that 'even with some cost recovery from the Commonwealth, and in turn, the taxpayer, much of this cost will be passed on to Internet users'.[115]

However, the Attorney-General has already indicated that she does not believe consumers would have to bear the costs, describing the increased costs instead as 'something that's now part of doing business in a changing technological world'.[116]

Technical challenges highlighted in a number of submissions to the PJCIS include the capacity to collect, collate and store the huge amounts of data generated, and the need to ensure the data is stored securely. Alluding to the fact that personal information has become a valuable commodity, the Office of the Victorian Privacy Commissioner believes:

> 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.[117]

The Australian Mobile Telecommunications Association and the Communications Alliance also believe that the retained data will itself become 'a target for unlawful access' and maintains that 'the Government should accept full responsibility and liability, including costs, for storage of the retained data'.[118] They suggest that the cost in particular should be borne in full by the Government, as is the case in the UK.

The Internet Industry Association makes a similar point about the challenges associated with securing the data—'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'.[119] Telstra too, believes that retaining large data sets means that 'an effective and fair data

---

114. Macquarie Telecom Pty Ltd, submission to the Parliamentary Joint Committee on Intelligence and Security, *Inquiry into potential reforms of National Security Legislation*, submission no. 115, 2012, p.4, viewed 20 September 2012, http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/subs.htm
115. Internet Society of Australia, submission to the Parliamentary Joint Committee on Intelligence and Security, *Inquiry into potential reforms of National Security Legislation*, submission no. 145, 2012, [p. 3], viewed 19 September 2012, http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/subs.htm
116. N Roxon (Attorney-General), 'Transcript of doorstop—Canberra', 4 September 2012, op. cit.
117. Office of the Victorian Privacy Commissioner, submission to the Parliamentary Joint Committee on Intelligence and Security, op. cit., p. 7.
118. Australian Mobile Telecommunications Association and the Communications Alliance, submission to the Parliamentary Joint Committee on Intelligence and Security, op. cit.
119. Internet Industry Association, submission to the Parliamentary Joint Committee on Intelligence and Security, op. cit., p. 7.

retention regime must recognise there is an increased risk to privacy that C/CSPs will need to manage, and the regime should provide indemnity or relief to C/CSPs if such data is compromised despite the best efforts by C/CSPs to avoid that happening'.[120]

Similar concerns have arisen in the UK, where the Internet Service Providers Association (ISPA) reportedly told the BBC that 'the technological challenge of collating and storing such vast levels of communication would be vast' and that while it is all 'do-able', it would potentially involve 'network redesigns' and systems would need to be capable of storing 'multiple petabits of data' (a single petabit is defined as the equivalent of 'around 130 000 gigabytes').[121] The ISPA has also raised the prospect that 'the government's desire to gather data could in fact have the unintended side-effect of encouraging more and more people to mask their online activity completely'.[122] Electronic Frontiers Australia agrees, noting that 'determined criminals will have little difficulty disguising or anonymising their communications'.[123]

Conclusion

Unless deliberate attempts are made to disguise or hide activity online or one's communications by phone, using the Internet or a phone unavoidably creates a record of its use. A loss of some privacy might have become a consequence of an increasingly electronically-connected world, but that only makes protecting our personal information and regulating access to it all the more important.

However, law enforcement and security agencies need to be able to operate in the digital environment as effectively as many criminals now do. As Telstra has noted, 'regrettably, not all the intelligence rests on the good side of the equation. There are some smart people out there who want to do bad things and they will, invariably, find ways to utilise technology for their benefit'.[124]

Contrary to the impression created by much of the media coverage and public commentary on the issue, as it currently stands the proposal to introduce a data retention scheme does not provide law enforcement agencies (or ASIO) with any new or additional powers. Police and other agencies have for many years been able to request communications data from CSPs under certain conditions (and currently have access to stored communications, such as text message and emails that have already been sent, under warrant).

In its current form, the data retention proposal only suggests stipulating a minimum period for which CSPs will be required to keep communications data, in an effort to address the apparently growing

120. Telstra, submission to the Parliamentary Joint Committee on Intelligence and Security, op. cit.
121. D Lee, 'Analysis: will the government's web "snoop" plans work?', *BBC News* online, 2 April 2012, viewed 19 September 2012, http://www.bbc.com/news/technology-17582974
122. Ibid.
123. Electronic Frontiers Australia Inc, submission to the Parliamentary Joint Committee on Intelligence and Security, op. cit., p. 4.
124. James Shaw, Director Government Relations, Telstra, cited in S McDonald, 'Data retention: the case against', *Computerworld*, 12 October 2012, viewed 12 October 2012, http://www.computerworld.com.au/article/438816/data_retention_case_against/?pp=2

problem that by the time police mount an investigation and need access to historical communications data, it is often no longer available. The proposed measures aim to ensure police continue to have access to such data for investigative purposes when it might otherwise have been deleted soon after it was generated. However, while it is clear how such a problem has arisen, there is very little statistical evidence available publicly to indicate the true extent of the problem or to demonstrate that data retention is the most appropriate solution.

While on the face of it data retention might sound like a sensible solution, there are a number of important issues (notably the cost and data security) which have been raised in submissions to the PJCIS inquiry relating to how a data retention scheme would work in practice that are as yet unaddressed. Evidence to the 2010 Senate inquiry and the nature of the concerns outlined in many of the submissions to the current PJCIS inquiry would suggest that Government consultation with industry in particular has so far been limited and patchy. It will be critical to the implementation and proper operation of any data retention scheme that these issues are properly considered and resolved prior to its commencement.