Submission No 224

Inquiry into potential reforms of National Security Legislation

Organisation: **Law Council of Australia**

Law Council
OF AUSTRALIA

National Security Legislation Reform – Supplementary Submission

Parliamentary Joint Committee on Intelligence and Security

22 October 2012

GPO Box 1989, Canberra
ACT 2601, DX 5719 Canberra
19 Torrens St Braddon ACT 2612

Telephone **+61 2 6246 3788**
Facsimile +61 2 6248 0639

Law Council of Australia Limited
ABN 85 005 260 622
www.lawcouncil.asn.au

Table of Contents

Introduction

1. On 20 August 2012 the Law Council of Australia made a detailed written submission to the Parliamentary Joint Committee on Intelligence and Security (the PJCIS) in response to a range of proposed reforms to national security legislation outlined in a Discussion Paper entitled *Equipping Australia against emerging and evolving threats* (the Discussion Paper).

2. The Law Council's submission focused on reforms concerning the telecommunications interception and access regime under the *Telecommunications (Interception and Access) Act 1979* (Cth) (the TIA Act) and those reforms relating to the content, use and oversight of the special powers of the Australian Security Intelligence Organisation (ASIO).

3. On 14 September 2012 representatives of the Law Council, Mr Phillip Boulten SC and Ms Rosemary Budavari, appeared at a public hearing conducted by the PJCIS to outline the key points raised in the Law Council's written submission and to answer questions from the PJCIS.

4. At the hearing, the Law Council representatives agreed to take the following questions on notice:[1]

    - Whether the Law Council has developed some guidelines in relation to its proposed privacy impact test for warrants and authorisations issued under the TIA Act;

    - The Law Council's opinion on the European Union data retention directive.

5. This supplementary submission contains the Law Council's response to these questions.

Consistent Privacy Impact Test for Warrants and Authorisations under the TIA Act

6. In its submission of 20 August 2012 the Law Council submitted that one way to strengthen the existing protections in the TIA Act against unjustified intrusion into personal privacy is to ensure that privacy considerations are always taken into account before a warrant to intercept or access a telecommunication is granted or access to telecommunications data is authorised.

7. The Law Council noted that privacy considerations are currently taken into account in the issuing of certain TIA Act warrants, but not all. The Law Council recommended a consistent privacy test be applied in all warrant applications and in all authorisations to intercept, access or disclose telecommunications data.

8. During the public hearing of the PJCIS on 14 September, Senator Stephens asked the Law Council's representatives to take on notice the question of whether the Law

[1] Transcript of the public hearing of the Parliamentary Joint Committee on Intelligence and Security's inquiry into national security legislation reforms, 14 September 2012, Canberra, available at http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;db=COMMITTEES;id=committees%2Fcommjnt%2F8bfd904d-936a-4d84-986a-e60a9583b2a9%2F0002;query=Id%3A%22committees%2Fcommjnt%2F8bfd904d-936a-4d84-986a-e60a9583b2a9%2F0000%22

Council has developed some guidelines in relation to its proposed privacy impact test for warrants and authorisations issued under the TIA Act.

9. While the Law Council has not previously developed guidelines in relation to its proposed privacy impact test, the key features of the test proposed by the Law Council can be summarised as follows:

   Before authorising the use of an interception, access or disclosure power under the TIA Act the authorising officer must:

   - *consider whether the exercise of the interception, access or disclosure power would be likely to deliver a benefit to the investigation or inquiry; and*
   - *consider the extent to which the interception, access or disclosure is likely to interfere with the privacy of any person or persons; and*
   - *be satisfied on reasonable grounds that the benefit likely to be delivered to the investigation or inquiry substantially outweighs the extent to which the interception, access or disclosure is likely to interfere with the privacy of any person or persons.*

10. The Law Council has previously advocated for this type of test in the context of the proposed reforms to section 180 of the TIA Act relating to the authorisation of the disclosure of prospective telecommunications data.[2] In that context, the Law Council recommended that the following clause be introduced:

    "Before making an authorisation, the authorised officer must be satisfied on reasonable grounds that the likely benefit to the investigation which would result from the disclosure substantially outweighs the extent to which the disclosure is likely to interfere with the privacy of any person or persons."

11. The Law Council suggests that a similar provision should be included in the other sections of the TIA Act that currently provide for the use of telecommunications interception, access and disclosure powers.

12. The "reasonable grounds" element of the test would ensure that the issue of privacy was more fully considered in the process. The Law Council also believes that such a test would reinforce the nature of the balancing process required when exercising powers under the TIA Act.

The European Data Retention Directive

13. In its written submission the Law Council expressed strong opposition to the proposed reform described in the Discussion Paper as "tailored data retention periods for up to two years for parts of a data set, with specific timeframes taking into account agency priorities, and privacy and cost impacts".[3]

---

[2] Law Council of Australia submission to Joint Select Committee on Cyber-Safety *Inquiry into the Cybercrime Legislation Amendment Bill 2011* (14 July 2011) available at http://www.lawcouncil.asn.au/shadomx/apps/fms/fmsdownload.cfm?file_uuid=69459E2B-C846-30EE-C1FD-17B77D7122E9&siteName=lca (the 2011 Cyber Crime Submission).

[3] Attorney General's Department, *Equipping Australia against emerging and evolving threats: A Discussion Paper to accompany consideration by the Parliamentary Joint Committee on Intelligence and Security of a package of national security ideas comprising proposals for telecommunications interception reform, telecommunications sector security reform and Australian intelligence community legislation reform* (July

14. This proposal is not outlined in any detail in the Discussion Paper, however, it is noted that:

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

15. Since the close of submissions to the inquiry on 20 August 2012, the data retention proposal has attracted significant media commentary. This commentary prompted the Attorney-General to appear in a YouTube video on 11 September 2012[4] and to write a letter to the PJCIS Chair on 19 September 2012. In the Attorney-General's letter to the PJCIS Chair she explains that this proposal does not include the retention of the content of the communication, but rather the "information about the process of a communication" such as:

> *"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." .*[5]

16. The Attorney's letter also stated that the ability to lawfully access telecommunications data enables investigators to identify and build a picture of a suspect, provides vital leads of inquiry and creates evidence for alibis and prosecutions.[6] Despite these comments, the Law Council remains concerned about this proposal.

17. When outlining its concerns in its written submission, the Law Council referred to the European Union (EU) Data Retention Directive 2006/24/EC (the Data Retention Directive). This requires EU Member States (Member States) to ensure that communications providers retain, for a period of between six months and two years, necessary data as specified in the Directive for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.

18. The Law Council noted that, since its introduction, serious concerns have been raised about the Data Retention Directive's compatibility with the rights to privacy and other rights protected under the European Convention on Human Rights (ECHR).[7]

2012) (the Discussion Paper) at p. 10 available at http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/index.htm

[4] On 19 September 2012, the Committee received a letter from the Attorney-General clarifying the data retention aspects of the terms of reference available at http://www.attorneygeneral.gov.au/Transcripts/Pages/2012/Third%20Quarter/11September2012TranscriptofYouTubevideobyNicolaRoxonMP.aspx

[5] Ibid

[6] Ibid.

[7] For example see Bignami, Francesca (2007), "Privacy and Law Enforcement in the European Union: The Data Retention Directive", *Chicago Journal of International Law* 8 (1): 233–256, Patrick Breyer, 'Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR" (2005) 11(3) *European Law Journal, ,* pp. 365–375.

19. During the public hearing of the PJCIS on 14 September 2012, Senator Stephens asked the Law Council representatives to provide the PJCIS with further information regarding the Law Council's opinion on the Data Retention Directive.

20. The Law Council is grateful for this opportunity to provide the PJCIS with the following further information regarding:

    - the content of the Data Retention Directive;
    - the key findings of the European Commission's 2011 evaluation of the Data Retention Directive; and
    - the implications that these findings, and other concerns raised during the public hearings of the PJCIS's inquiry, may have for an Australian data retention scheme based on the European experience.

The Content of the Data Retention Directive

21. The Data Retention Directive requires providers of publicly available electronic communications services and public communication networks to retain communications data for the investigation, detection and prosecution of serious crime as defined by each Member State.[8]

22. The Data Retention Directive does not permit the retention of data revealing the content of the communication. However it applies to a wide range of other telecommunications data, namely data necessary to:[9]

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

[8] European Union Data Retention Directive 2006/24/EC Article 3
[9] Ibid Article 5.

23. Under the Data Retention Directive, Member States are required to implement measures to ensure this data is retained for periods between six months and two years from the date of the communication.[10]

24. The Data Retention Directive restricts access to this data to "the competent national authorities in specific cases and in accordance with national law". [11] It states that the procedures and conditions regulating access to retained data are to be developed in accordance with the principles of necessity and proportionality that are defined by each Member State in its national law, and must also be subject to the relevant provisions of EU law or public international law, and in particular the ECHR.[12]

25. The Data Retention Directive also outlines a list of minimum data security principles that apply to data retained in accordance with the Directive. Under these principles, data retained must be:

    - of the same quality and subject to the same security and protection as data on the public communications network;
    - subject to appropriate technical and organisational measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure;
    - subject to appropriate technical and organisational measures to ensure that it can be accessed by specially authorised personnel only; and
    - destroyed at the end of the period of retention.

26. It is also important to note that the Data Retention Directive exists alongside a number of other Directives that relate to electronic communications and privacy rights, including the Directive 2002/58/EC on privacy in electronic communications (the e-Privacy Directive),[13] which requires that traffic data generated by the use of electronic communications services must in principle be erased or made anonymous when such data is no longer needed for the transmission of a communication, except where, and only for so long as, it is needed for billing purposes, or where the consent of the subscriber or user has been obtained. The Data Retention Directive amends this e-Privacy Directive, to make an exception for data retained in accordance with its Articles.[14]

27. As at April 2011, 25 Member States had provided information to the European Commission (the EC) on the steps taken implement the Data Retention Directive into their national laws.[15] Austria and Sweden reported that draft legislation was under discussion. Although the Data Retention Directive was implemented into domestic law in the Czech Republic, Germany and Romania, this legislation was subsequently annulled by their respective constitutional courts.[16] These Member States therefore

[10] Ibid Article 6.
[11] Ibid, Article 4.
[12] Ibid, Article 4.
[13] Directive of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31/07/2002, p. 0037 – 0047).
[14] European Union Data Retention Directive 2006/24/EC Article 15
[15] The twenty-five Member States who have notified the Commission of transposition of the Directive are Belgium, Bulgaria, Czech Republic, Denmark, Germany, Greece, Estonia, Ireland, Spain, France, Italy, Cyprus, Latvia, Lithuania, Luxembourg, Hungary, Malta, Netherlands, Poland, Portugal, Romania, Slovenia, Slovakia, Finland and United Kingdom. Belgium informed the Commission that draft legislation completing transposition is still before Parliament.
[16] Decision no 1258 from 8 October 2009 of the Romanian Constitutional Court, Romanian Official Monitor No 789, 23 November 2009; judgement of the Bundesverfassungsgericht 1 BvR 256/08, of 2 March 2010; See

reported that they were considering how to re-implement the Data Retention Directive into their domestic laws.

Evaluation of the Data Retention Directive by the European Commission

28. The Data Retention Directive required the EC to undertake an evaluation of the application of the Directive by September 2010.[17] A report on this evaluation was provided by the EC to the European Council and Parliament in April 2011 (the Evaluation). The Law Council suggests that many of its findings are relevant when considering the appropriateness of the EU Directive as a model for Australia.[18]

29. The Evaluation considered the implementation of the Data Retention Directive by Member States and its impact on economic operators and consumers. It also examined the implications of the Data Retention Directive for fundamental human rights and whether measures are needed to address concerns associated with the use of new and emerging telecommunication technologies.

30. Although the EC concluded that data retention is a valuable tool for criminal justice systems and for law enforcement[19] it also noted that it had not resulted in harmonisation of approaches to data retention across Member States. For example, although the Data Retention Directive obliges Member States to adopt measures to ensure that data is retained and available for the purpose of investigating, detecting and prosecuting serious crime, important differences exist among Member States in relation to how this is expressed in national legislation. Some States limit data retention on the basis of a particular definition of 'serious crime', while other States allow data retention in relation to all criminal offences and for crime prevention, or on general grounds of national or state and/or public security.[20] Differences were also found to exist between the laws of the Member States in terms of which agencies can access the retained data, the periods for which data can be retained, and the standards of data protection and data security applied.[21]

31. The EC warned that these differences are likely to affect the volume and frequency of requests and in turn the costs incurred for compliance with the obligations in the Data Retention Directive. It also noted that this may make it difficult for an individual to anticipate the circumstances in which his or her data may be retained and accessed (known as 'foreseeability'), which is a requirement in any legislative measure which restricts the right the privacy under the EHCR.22 It was noted that the European Data Protection Supervisor has observed that this lack of harmonisation meant that the use of retained data had not been strictly limited to combatting serious crime,23 and called on the EU to adopt a comprehensive legislative framework which regulates how Member States use the data for law enforcement purposes, so as to create 'legal certainty for citizens'. The implications of this for an Australian data retention scheme based on the European Model are discussed below in paragraph 52 and following.

---

also Report from the Commission to the Council and the European Parliament, *Evaluation report on the Data Retention Directive (Directive 2006/24/EC)* (18 April 2011)available at http://eur-lex.europa.eu/COMByRange.do?year=2011&min=201&max=225 p. 6.

[17] European Union Data Retention Directive 2006/24/EC Article 14.

[18] Report from the Commission to the Council and the European Parliament, *Evaluation report on the Data Retention Directive (Directive 2006/24/EC)* (18 April 2011) a copy of this report is available at http://eur-lex.europa.eu/COMByRange.do?year=2011&min=201&max=225).

[19] Ibid Chapter 5.

[20] Ibid p. 6, see also Table 1.

[21] Ibi pp. 8-18, see also Tables 2-4.

[22] Ibid pp.8-9.

[23] Speech by Peter Hustinx at the conference 'Taking on the Data Retention Directive', 3 December 2010.

32. When evaluating the impact of the Data Retention Directive on the right to privacy and the protection of personal data, the EC had regard to the following matters:[24]

- The right to private life and the protection of personal data are fundamental rights in the EU[25] and any limitation of these rights must be: provided for by law and respect the essence of those rights; subject to the principle of proportionality; and justified as necessary and meeting the objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others.[26]

- Article 8(2) of the EHCR recognises that interference by a public authority with a person's right to privacy may be justified as necessary in the interests of national security, public safety or the prevention of crime. Article 15(1) of the e-Privacy Directive and the preamble to the Data Retention Directive reiterate these principles underpinning the EU's approach to data retention.

- The relevant case law of the European Court of Justice and the European Court of Human Rights suggests that any limitations on the right to privacy must be: precise, necessary and proportionate.Such limitations should enable 'foreseeability' and minimum safeguards should be included.

The implications of this for an Australian data retention scheme based on the European Model are discussed below in paragraph 46 and following.

33. The EC also considered the nature of the constitutional challenges to the implementation of the Directive into domestic law in Romania, Germany and the Czech Republic. It summarised the nature of these challenges as follows: [27]

- The Romanian Court[28] accepted that interference with fundamental rights may be permitted where it respects certain rules and where adequate and sufficient safeguards are provided to protect against potential arbitrary state action. However, the Court found the transposing law to be ambiguous in its scope and purpose with insufficient safeguards. The Court held that a 'continuous legal obligation' to retain all traffic data for six months was incompatible with the rights to privacy and freedom of expression in Article 8 of the ECHR.

- The German Constitutional Court[29] said that data retention generated a perception of surveillance which could impair the free exercise of fundamental rights. It explicitly acknowledged that data retention for strictly limited uses along with sufficiently high security of data would not necessarily violate the German Basic Law. However, the Court stressed that the retention of such data constituted a serious restriction of the right to privacy and therefore should only be admissible under particularly limited circumstances, and that a retention period of six months was at the upper limit of what could be considered proportionate. The Court further held that data should only be

[24] Report from the Commission to the Council and the European Parliament, *Evaluation report on the Data Retention Directive (Directive 2006/24/EC)* (18 April 2011) pp. 28-30.
[25]Article 7 and Article 8 of the Charter of Fundamental Rights of the European Union guarantees everyone's right to the "protection of personal data concerning him or her." Article 16 of the Treaty on the Functioning of the European Union also enshrines everyone's right to the "protection of personal data concerning them."
[26]See the Commission's Fundamental Rights Check-List for all legislative proposals in Commission Communication COM (2010) 573/4, 'Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union'.
[27] Report from the Commission to the Council and the European Parliament, *Evaluation report on the Data Retention Directive (Directive 2006/24/EC)* (18 April 2011) p. 28
[28] Decision no 1258 from 8 October 2009 of the Romanian Constitutional Court.
[29] Bundesverfassungsgericht, 1 BvR 256/08, para 1 – 345.

requested where there was already a suspicion of a serious criminal offence or evidence of a danger to public security, and that data retrieval should be prohibited for certain privileged communications which rely on confidentiality.

- The Czech Constitutional Court[30] annulled the transposing legislation on the basis that it was insufficiently precise and clear in its formulation. The Court held that the definition of authorities competent to access and use retained data and the procedures for such access and use were not sufficiently clear in the transposing legislation to ensure the integrity and the confidentiality of the data. Because of this, the individual citizen had insufficient guarantees and safeguards against possible abuses of power by public authorities. In *obiter dictum* the Court also expressed doubt as to the necessity, efficiency and appropriateness of the retention of traffic data given the emergence of new methods of criminality such as through the use of anonymous SIM cards.

34. It was also noted that cases challenging the constitutional validity of national data retention systems implemented to give effect to the Data Retention Directive had been heard in Bulgaria, Cyprus, and Hungary[31] and that a case had been commenced in Ireland by a civil rights group, which has subsequently been referred to the European Court of Justice.[32]

35. The EC also considered the impact of data retention on operators and consumers including the costs incurred by industry participants and governments in each Member State.[33]

36. The EC recommended that the EU continue to support and regulate data retention as a security measure, but that harmonised rules should be developed to ensure that data retention is an effective tool in combatting crime; that industry has legal certainty in a smoothly functioning internal market; and that high levels of respect for privacy and the protection of personal data are applied consistently throughout the EU.[34] The EC explained that this should involve further examination of matters including:[35]

    - limiting the purpose of data retention and the types of crime for which retained data may be accessed and used for investigative purposes;
    - harmonising and possibly shortening the periods of mandatory data retention;ensuring independent supervision of requests for access and of the overall data retention and access regime applied in all Member States;
    - limiting the authorities authorised to access the data; and
    - reducing the data categories to be retained.

37. The EC also concluded that the Data Retention Directive had not fully harmonised the approach to data retention and had not created a level-playing field for operators.[36] It

[30] Judgment of the Czech Constitutional Court of 22 March on Act No. 127/2005 and Decree No 485/2005; see in particular paragraphs 45-48, 50-51 and 56..
[31]Bulgarian Supreme Administrative Court, decision no. 13627, 11 December 2008; Supreme Court of Cyprus Appeal Case Nos. 65/2009, 78/2009, 82/2009 and 15/2010-22/2010, 1 February 2011; the Hungarian constitutional complaint was filed by the Hungarian Civil Liberties Union on 2 June 2008.
[32]On 5 May 2010 the Irish High Court granted Digital Rights Ireland Limited the motion for a reference to the European Court of Justice under Article 267 of the Treaty on the Functioning of the European Union.
[33] Report from the Commission to the Council and the European Parliament, *Evaluation report on the Data Retention Directive (Directive 2006/24/EC)* (18 April 2011) Chapter 6, see also Table 6.
[34] Ibid p. 31.
[35] Ibid p. 32.
[36] Ibid p. 31.

also recommended that operators should be consistently reimbursed for the costs they incur.[37]

Implications for an Australian data retention scheme based on the European Model

38. It appears that the Government is considering the Data Retention Directive as a possible model for an Australian data retention scheme. For example, the Data Retention Directive was described in some detail in the Attorney-General's recent letter to the Chair of the PJCIS, and identified as an example of a response to the challenges arising from changes in technology that have affected the behaviour of criminal and national security suspects.[38]

39. The Law Council would be concerned by any efforts to utilise the Data Retention Directive as a model for an Australian data retention scheme.

40. As noted in the Law Council's written and oral submissions to the PJCIS, the Law Council opposes the implementation of a data retention scheme on the grounds that it has not been shown to be necessary for the purpose of the investigation of criminal activity or for national security. It also opposes the proposal due to its potentially intrusive impact on the privacy rights of large sectors of the community regardless of whether they are suspected of engaging in any criminal conduct or other wrongdoing.

41. Despite the provision of further material by the Attorney-General and her Department, the Law Council is not satisfied that the Government has demonstrated that the range of powers currently available to law enforcement officers to access and disclose telecommunications data is insufficient for them to investigate and prosecute serious criminal activity, even in the face of emerging telecommunications technologies. For example, evidence provided to the PJCIS by representatives from Telstra suggests that Australian law enforcement agencies may not "always [be] well informed about what they can actually get now by way of information" and may benefit from the opportunity to liaise more closely with technical and industry experts to "make better value of the current arrangements" before further data retention options are pursued.[39]

42. It is also not clear that a data retention scheme would effectively resolve any current operational difficulties faced by law enforcement officers as a result of rapid changes to telecommunications technology. For example, when giving evidence to a public hearing of the PJCIS, representatives from Telstra said that:

> *The simple evolution of technology would mean that [under the proposed data retention scheme] we could not capture or provide any metadata or any content around something like Gmail, because it is Google owned, it is offshore and it is*

[37] Ibid p. 31.

[38] More recently, in response to questions from Senator Ludlam during a Senate Estimates Hearing on 17 October 2012, the Attorney-General's Department provided some further information about the definition of 'telecommunications data' that would form part of the data retention proposal. This definition aligns broadly with the EU data retention directive, and does not include the content of telecommunications, but rather covers information that allows a communication to occur (such as the identifier assigned to the internet user by the internet provider or the number called or texted by mobile phone) and information about the parties to the communication (such as the name and contact details of the person who owns the service).

[39] Evidence from Mr Kane, Telstra Corporation Ltd to Parliamentary Joint Committee on Intelligence and Security Joint Committee Inquiry into Potential reforms of national security legislation, Thursday, 27 September 2012, Sydney copy available at http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;db=COMMITTEES;id=committees%2Fcommjnt%2F4df3cb6c-f4d2-40db-a27b-3c13628da892%2F0001;query=Id%3A%22committees%2Fcommjnt%2F4df3cb6c-f4d2-40db-a27b-3c13628da892%2F0000%22

over the top on our network. The real value of what we might have in our data-retention scheme would be greatly diminished as soon as the good, organised criminals and potential terrorist cells knew that we were not capturing that data.[40]

43. The Law Council is also of the view that if the Data Retention Directive is being considered as a model for an Australian data retention scheme, the concerns outlined above by the EC following its evaluation of the Directive must be addressed in the Australian context. These include:

Questions regarding the effectiveness of data retention as a tool for law enforcement agencies

44. A number of bodies that have provided submissions to the PJCIS opposing the data retention proposal have cited studies that question the effectiveness of the Data Retention Directive as a method used by law enforcement.[41] For example, a number of organisations have referred to a study of Germany's Data Retention Directive that found it had no impact on either the effectiveness of criminal investigations or the crime rate, and that it may even have a detrimental impact on the investigation of criminal activity as it provides an incentive for organised criminal groups to develop more sophisticated electronic communication techniques or use more technologically advanced encryption.[42]

45. The Law Council notes that while the EC expressed the view that the Data Retention Directive was generally having a positive impact on the investigation and prosecution of serious criminal activity, it also acknowledged that there were gaps in coverage of the Directive particularly in relation to new and emerging technologies that were providing sophisticated criminal organisations with options to avoid the reach of the Data Retention Directive. This was having an impact on the Directive's effectiveness as a tool for law enforcement agencies. A similar issue was raised by representatives from Telstra when questioned on the coverage of the proposed Australian data retention scheme, where it was noted that there was a range of metadata that might not be covered such as data relating to communications made using Skype, YouTube or Google applications.[43]

---

[40] Evidence from Mr Kane, Telstra Corporation Ltd to Parliamentary Joint Committee on Intelligence and Security Joint Committee Inquiry into Potential reforms of national security legislation, Thursday, 27 September 2012, Sydney copy available at http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;db=COMMITTEES;id=committees%2Fcommjnt%2F4df3cb6c-f4d2-40db-a27b-3c13628da892%2F0001;query=Id%3A%22committees%2Fcommjnt%2F4df3cb6c-f4d2-40db-a27b-3c13628da892%2F0000%22

[41] See for example, submissions to the Parliamentary Joint Committee on Intelligence and Security Joint committee Inquiry into Potential reforms of national security legislation by Blueprint for Free Speech, Institute of Public Affairs and Pirate Party of Australia, available at http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/subs.htm

[42] Arbeitskreis Vorratsdatenspeicherung, *Serious criminal offences, as defined in sect. 100a StPO, in Germany according to police crime statistics*, http://www.vorratsdatenspeicherung.de/images/data_retention_effectiveness_report_2011- 01-26.pdf.,

43 Evidence from Mr Kane, Telstra Corporation Ltd to Parliamentary Joint Committee on Intelligence and Security Joint Committee Inquiry into Potential reforms of national security legislation, Thursday, 27 September 2012, Sydney copy available at http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;db=COMMITTEES;id=committees%2Fcommjnt%2F4df3cb6c-f4d2-40db-a27b-c13628da892%2F0001;query=Id%3A%22committees%2Fcommjnt%2F4df3cb6c-f4d2-40db-a27b-3c13628da892%2F0000%22

The impact of the Data Retention Directive model on the privacy rights of individuals

46. It is important to note that the Data Retention Directive operates within a legal framework that includes an enforceable right to privacy and a range of legal protections for personal information, such as those contained in Article 8 of the ECHR and the e-Privacy Directive described above. The relationship between the Data Retention Directive and these protections is complex and has given rise to constitutional issues in some Member States. As noted above, domestic legislation implementing the Directive has been found to be so broadly expressed as to fall outside the permitted limitations on the right to privacy, or has been found to be insufficiently precise to enable individuals to foresee the circumstances in which their privacy rights will be breached. It has also been found that domestic legislation contained insufficient safeguards to protect against overuse or misuse by law enforcement agencies.

47. This has led the EC to recommend that the EU reconsider a range of key features of the Directive, such as:

    - the purpose of data retention and the types of crime for which retained data may be accessed and used for investigative purposes;
    - the need for independent supervision of requests for access and of the overall data retention and access regime applied in all Member States;
    - the limitation of authorities authorised to access the data; and
    - the reduction of data categories for retention.

48. These matters must be carefully considered before Australia seeks to replicate such a scheme. Unlike the EU, Australia lacks any specific legislation at the federal level that replicates the protections found in the ECHR, which in many respects, makes the privacy of Australians more vulnerable to unjustified interference by state agencies than that of Europeans.

49. The absence of an enforceable right to privacy such as that contained in Article 8 of the ECHR does not absolve Australia of its responsibilities to protect individual privacy. Australia has assumed obligations under the international conventions to which it is a party, such as the International Covenant on Civil and Political Rights which protects the right to privacy, which could be seriously undermined by the adoption of a data retention scheme based on the Data Retention Directive model.

The maximum period for which data should be retained

50. As noted above, under the Data Retention Directive, Member States have the flexibility to implement domestic data retention schemes that permit data to be retained for periods between six months and two years. The EC Evaluation of the implementation of the Directive found that different time periods were being applied across Member States and within Member States, depending on the category of data. The EC stated that, to meet the proportionality principle required in relation to laws that infringe protected rights, such as the right to privacy, and in the light of the information provided by Member States, it would consider applying different periods for different categories of data, for different categories of serious crimes or for a combination of the two.[44] It also noted that evidence provided by Member States regarding the age of retained data suggests that around ninety percent of the data is

[44] Report from the Commission to the Council and the European Parliament, *Evaluation report on the Data Retention Directive (Directive 2006/24/EC)* (18 April 2011) p. 15.

six months old or less and around seventy percent is three months old or less when the (initial) request for access is made by law enforcement authorities. [45]

51. This raises serious questions about the appropriateness of the outer limit of two years for the retention of data under any Australian model based on the Data Retention Directive.

The need to guarantee the security of the data retained

52. As described above, the Data Retention Directive outlines a range of minimum standards that should be observed when implementing data retention systems in Member States,[46] however the EC found that the implementation of these standards differ across Member States, raising questions about whether these issues have been satisfactorily addressed in the Directive itself.[47] As the EC observed:

> *Retained data is potentially of a highly personal and sensitive nature and high standards of data protection and data security need to be applied throughout the process, for storage, retrieval and use, and consistently and visibly in order to minimise the risk of breaches of privacy and to maintain confidence of citizens. The Commission will consider options for strengthening data security and data protection standards, including introducing privacy-by-design solutions to ensure these standards are met as part of both storage and transmission.* [48]

53. Until such options have been identified and implemented, the Data Retention Directive should not be considered as representing world's best practice in terms of data protection and data security. The risks associated with storing this data securely should also be considered when evaluating whether such a system would be a proportionate response to the needs identified by law enforcement agencies that have been cited by the Government as justifying the data retention proposal in Australia.

The costs of implementing a data retention scheme

54. The Evaluation of the Data Retention Directive suggests that it is difficult to predict the total costs of implementing and maintaining a data retention system, and that further research is required to determine the real costs of such a system from both the perspectives of the service operators and consumers.[49]

55. The Law Council notes that representatives from Telstra provided some insights into the range of costs that industry participants may need to absorb if such a system was implemented in Australia. For example, Telstra representatives explained that:

> *"The storage of data is one of the lesser elements of the cost, although it does give rise, as I have said, to the privacy and security risks to protect that data and, not least, to protect its integrity also. But, certainly, the costs—for the system to retrieve it and to then create a way of retaining it and then making it accessible and then on the other side, the agency side, creating the ability for them to access, understand and use it—would be substantial, in our view."*[50]

[45] Ibid p. 15.
[46] European Union Data Retention Directive 2006/24/EC Article 7.
[47] Ibid p. 18 see also Table 4.
[48] Ibid.
[49] Ibid p. 28.
[50] Evidence from Ms Van Beelan, Telstra Corporation Ltd to Parliamentary Joint Committee on Intelligence and Security Joint Committee Inquiry into Potential reforms of national security legislation, Thursday, 27 September 2012, Sydney copy available at

56. The Law Council is of the view that this full range of costs needs to be carefully considered before Australia adopts a data retention system based on the Data Retention Directive model.

Conclusion

57. The Law Council is not in a position to express a conclusive view on the effectiveness of the Data Retention Directive as a tool to fight serious crime or threats to national security. However, it is clear from the European experience that serious concerns have arisen in a number of Member States about the constitutional validity of data retention schemes based on this model, in light of their disproportionate impact on the privacy rights of individuals. A number of other serious concerns have been raised in relation to the Data Retention Directive, such as those relating to its ability to keep pace with rapid technological changes and those relating to the costs of implementing and maintaining such systems.

58. The Law Council is not satisfied that the range of issues identified in the EC's 2011 Evaluation of the Data Retention Directive have been addressed in the information provided by the Government relating to its data retention proposal. Nor has sufficient information been provided to justify the implementation of a similar scheme in the Australian context.

59. The European experience suggests that the Data Retention Directive has the potential to lead to the retention of data that: can be of a highly personal nature; is available for a wide range of purposes; and is accessible by a wide range of agencies, regardless of whether it relates to an individual who has been suspected of any criminal conduct or wrongdoing. It should not be considered a model for Australia, particularly when it remains unclear whether such a system is necessary or whether it will address the types of operational difficulties faced by law enforcement agencies.

http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;db=COMMITTEES;id=committees%2Fcommjnt%2F4df3cb6c-f4d2-40db-a27b-c13628da892%2F0001;query=Id%3A%22committees%2Fcommjnt%2F4df3cb6c-f4d2-40db-a27b-3c13628da892%2F0000%22

Attachment A: Profile of the Law Council of Australia

The Law Council of Australia exists to represent the legal profession at the national level, to speak on behalf of its constituent bodies on national issues, and to promote the administration of justice, access to justice and general improvement of the law.

The Law Council advises governments, courts and federal agencies on ways in which the law and the justice system can be improved for the benefit of the community. The Law Council also represents the Australian legal profession overseas, and maintains close relationships with legal professional bodies throughout the world.

The Law Council was established in 1933, and represents 16 Australian State and Territory law societies and bar associations and the Large Law Firm Group, which are known collectively as the Council's constituent bodies. The Law Council's constituent bodies are:

- Australian Capital Bar Association
- Australian Capital Territory Law Society
- Bar Association of Queensland Inc
- Law Institute of Victoria
- Law Society of New South Wales
- Law Society of South Australia
- Law Society of Tasmania
- Law Society Northern Territory
- Law Society of Western Australia
- New South Wales Bar Association
- Northern Territory Bar Association
- Queensland Law Society
- South Australian Bar Association
- Tasmanian Independent Bar
- The Large Law Firm Group (LLFG)
- The Victorian Bar Inc
- Western Australian Bar Association

Through this representation, the Law Council effectively acts on behalf of approximately 56,000 lawyers across Australia.

The Law Council is governed by a board of 17 Directors – one from each of the constituent bodies and six elected Executives. The Directors meet quarterly to set objectives, policy and priorities for the Law Council. Between the meetings of Directors, policies and governance responsibility for the Law Council is exercised by the elected Executive, led by the President who serves a 12 month term. The Council's six Executive are nominated and elected by the board of Directors. Members of the 2012 Executive are:

- Ms Catherine Gale, President
- Mr Joe Catanzariti, President-Elect
- Mr Michael Colbran QC, Treasurer
- Mr Duncan McConnel, Executive Member
- Ms Leanne Topfer, Executive Member
- Mr Stuart Westgarth, Executive Member

The Secretariat serves the Law Council nationally and is based in Canberra.