Telecommunications Data Retention: A Step in the Right Direction?

Lisa Hill and Jessica Childs take a brief look at Australia's potential telecommunications data retention laws, which may form part of the Government's next package of reform of national security legislation.

Australian carriage service providers (***CSPs***) are currently not required to retain metadata associated with telecommunications services generally, for law enforcement or national security purposes. While it is usual for such data to be routinely retained by a CSP for business purposes (for example, billing, marketing and network monitoring purposes), associated storage costs mean that it will be deleted if no longer required. However certain metadata, such as the details of Uniform Resource Locators (***URL***) visited, is not likely to be retained for business purposes and therefore would be deleted immediately.

The Government has raised the possibility of introducing a European Union (***EU***) style telecommunications data retention regime with, "tai lored 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"[1] (the ***data retention proposal***). Although the term "telecommunications data" is not defined in Australian legislation, the extrinsic materials suggest that it may mean the metadata associated with telecommunications services. Despite a lack of further detail on the Government's proposal – there is no draft legislation and no clear indication has been given as to the scope of the relevant data set - the issue has nevertheless ignited considerable debate on the merits and necessity of a data retention regime in Australia.

Inquiry by the Parliamentary Joint Committee on Intelligence and Security

In July 2012 the Government asked the Parliamentary Joint Committee on Intelligence and Security (***PJCIS***) to consider a package of potential reform of national security legislation. The Attorney General's Department released a discussion paper to accompany the relevant terms of reference and describe the reform proposals (the ***discussion paper***).[2] The discussion paper set out 18 proposals which were divided into 3 categories: those the Government wished to progress; those the Government is considering; and those on which the Government is seeking the views of the PJCIS.

The data retention proposal is included in the package of reform of the *Telecommunications (Interception and Access) Act 1979* (Cth) (the ***TIA Act***). At this stage the Government is only seeking the views of the PJCIS on the data retention proposal. Public submissions were sought by 20 August 2012. At the time of writing the PJCIS' report is yet to be tabled in Parliament.

Telecommunications data

Neither the discussion paper, nor any other documents available at the time of its release, provides adequate details and discussion of the nature of the data to be retained. As noted above, telecommunications data is not defined in either of the *Telecommunications Act 1997* (Cth) or the TIA Act, although the concept is relevant to these laws.

It is generally understood that telecommunications data refers to communications metadata; that is, information about a communication other than the content or substance of a communication, such as subscriber data (name and address) and traffic data (date, time, location and duration). However the scope of this information is not clear. In particular, it is not clear if, or to what extent, this information would include the URLs of websites visited by the customers of a CSP.

Statements made by the Attorney General, following the release of the discussion paper, have attempted to clarify the meaning of telecommunications data in the context of the data retention proposal. In a letter to the Chair of the PJCIS, the Attorney-General stated that the proposal does not include the retention of the content of a 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 communications, its duration, location and type of communication*".[3] The Attorney-General has further clarified that this type of data does not include the content of phone calls, emails, "tweets" or posts,[4] nor does it include records of website visits.[5]

So, will the details of URLs visited be considered 'telecommunications data' for the purposes of the data retention proposal? The Government has previously reported that the general practice under the TIA Act has been that URLs will be telecommunications data "*to the extent that they do not identify the content of a communication*".[6] This approach is consistent with that proposed in the UK and under the EU data retention provisions. However, at the Senate Estimates hearings in October 2012, the Attorney-General's Department stated that in the context of the data retention proposal, data would not include records of web browsing and would not include URLs.[7] There is some merit in this approach given the large volume of data that could be generated from the retention of such information (being data which would not usually be retained by CSPs) and the fact that it may be otherwise accessible via generally available analytics tools.

Data retention periods

It is critical to understand why the Government is considering a two year data retention period, and whether this is likely to be effective in ensuring that law enforcement agencies have adequate opportunity to protect Australians against future telecoms and online communications threats, in view of privacy concerns and the heavy compliance cost burden on CSPs.

---

1 Attorney-General's Department, Equipping Australia Against Emerging and Evolving Threats, July 2012, p. 10.

2 Ibid.

3 Attorney-General's letter to Anthony Byrne MP, Chair of the PJCIS, undated, received by the PJCIS on 19 September 2012, p. 1.

4 N Roxon, Letter to the editor—Herald Sun, media release, 7 September 2012, viewed 7 January 2013, http://www.attorneygeneral.gov.au/Media-releases/Pages/2012/Third%20Quarter/7-September-2012-Letter-to-the-editor-Herald-Sun.aspxhttp://www.attorneygeneral.gov.au/Media-releases/Pages/2012/Third%20Quarter/7-September-2012-Letter-to-the-editor-Herald-Sun.aspx

5 R Epstein, Transcript of interview on ABC 774 Melbourne with Rafael Epstein and Joe Hockey, transcript, ABC Radio, 5 September 2012, viewed 7 January 2013, http://www.attorneygeneral.gov.au/Transcripts/Pages/2012/Third%20Quarter/5September2012-TranscriptofinterviewonABC774MelbournewithRafaelEpsteinandJoeHockey.aspx

6 Attorney General's Department, Telecommunications (Interception and Access) Act 1979 – Annual Report for the year ending 30 June 2011, p. 6.

The Attorney-General's Department's own advice on this issue was "*to limit the non-content data retention requirement to a short period (6 months) unless there is strong evidence relevant to Australia of the utility of a longer period*" before engaging in public consultation on a data retention proposal of up to two years. This recommendation is set out in a preliminary privacy impact assessment of the proposed reforms to the TIA Act that was conducted by Information Integrity Solutions and submitted to the department in December 2011.[8]

The Attorney-General's stated rationale for the data retention proposal (as part of a wider reform of national security legislation) is that the capabilities (systems, methods and tools) and powers of Australia's law enforcement and security agencies need to keep pace with cyber enabled crime and threats to national security.[9] Changing technology and business practices mean that less telecommunications data is now being retained by CSPs as a matter of usual business practice.[10] Accordingly, law enforcement and intelligence agencies claim that they cannot always access the data they need for investigations and that a longer retention period by CSPs would significantly increase their ability to operate in a digital environment as effectively as many criminals do now.[11]

Not surprisingly the data retention proposal has been met with significant resistance from CSPs. CSPs would ordinarily delete most communications data after they have completed their internal business processes, as such information is not currently required to be kept for law enforcement or national security purposes. Data storage costs and security concerns are their primary concerns. Similarly, consumer and user groups have also expressed privacy concerns, in relation to data security and privacy. For example, Electronic Frontiers Australia has expressed concerns about an "*unprecedented threat that [proposed data retention requirements] would represent to the right to privacy of all Australians*".[12] It is also not clear that any changes to the TIA Act in recent years have led to any great success measured in convictions per warrant issued.[13]

In relation to the length of the retention period, while the Government may have provided some rationale for data retention, to date there has been no discussion on whether a 2 year retention period would be appropriate for Australia. In relation to the issue of law enforcement's ability to access the data they need for investigations, there does not appear to be any publically available source in which, for example the Australian Federal Police, detail what proportion of their large number of requests for communications data were unsuccessful due to the data no longer being available from CSPs.[14] Understanding the scale of the issue for these agencies is difficult.

It would appear that the Government's justification for an Australian data retention regime relies heavily on the data retention directive for EU member states. The EU has had a data retention regime since 2006. Directive 2006/24 requires EU member states to oblige providers of publically available electronic communications services or of public communications networks to retain traffic and location data for between six months and two years, for the purpose of the investigation, detection and prosecution of serious crime.[15] However, it is questionable as to whether the EU regime has been successful in making the dent in serious or organised crime that the EU had intended.

In a 2011 review of Directive 2006/24 by the European Commission, the '*Evaluation report on the Data Retention Directive*' reported that quantitative evidence provided by EU member states regarding the age of retained data showed that around ninety percent of the data is six months old or less and around seventy percent three months old or less, when the initial request for access is made by law enforcement authorities.[16] Most of the EU member states who had transposed Directive 2006/24 into local law had opted for retention periods of less than 2 years (mainly 6 months to 1 year).[17] The report also found that the Romanian Constitutional Court in October 2009, the German Federal Constitutional Court in March 2010 and the Czech Constitutional Court in March 2011 annulled the laws transposing Directive 2006/24 into their respective jurisdictions, on the basis that they were unconstitutional.[18]

Despite a lack of further detail on the Government's proposal the issue has nevertheless ignited considerable debate on the merits and necessity of a data retention regime in Australia

The EU data retention experience raises serious questions as to whether Australia should be using principles from this EU regime, as an example of an effective method of data retention. The Government needs to analyse the effectiveness of both the EU regime and the proposed Australian regime, if the changes proposed are to be consistent with evidence-based policy approaches.

Next steps

With a federal election date of 14 September 2013 now locked in, there is no certainty that the PJCIS' report, including the Committee's views on the data retention proposal, will be tabled in Parliament this year. Given the Government's recent release of a new national security strategy package, it is also doubtful that any draft national security reform legislation could be published before the election. Therefore, national security reform legislation, with data retention provisions, is not likely to pass through the current Parliament.

With the Coalition unlikely to oppose the data retention proposal in principle, if such legislation enacted in a future Parliament then it would be more efficient for CSPs to pass on any associated costs of implementing the regime to the customer, rather than have the Government foot the bill. As a result, CSPs will need to consider how to manage their customer relationships when passing on such costs.

Lisa Hill is Special Counsel at Webb Henderson. Jessica Childs is Corporate Counsel at Optus. The authors would like to thank Dr Rob Nicholls of Webb Henderson for his assistance with this paper.

The views expressed in this article are the views of the authors only and do not represent the views of any organisation.

---

7 Senate Hansard, Legal and Constitutional Affairs Legislation committee, Estimates, 16 October 2012, p. 90

8 Information Integrity Solutions, Privacy Impact Assessment - Preliminary Report – Telecommunications (Interception and Access) Act 1979 Reform, December 2011, p. 12. Released publicly for the first time in August 2012 under freedom of information laws.

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

10 Attorney-General's letter to Anthony Byrne MP, Chair of the PJCIS, undated, received by the PJCIS on 19 September 2012, p. 2.

11 See for example, the Australian Federal Police submission to the PJCIS *Inquiry into potential reforms of National Security Legislation*, submission no. 163, p.15-18.

12 Electronic Frontiers Australia Inc, submission to the ,PJCIS' *Inquiry into potential reforms of National Security Legislation*, submission no. 121, 2012, p.5.

13 Nicholls, Rob "Right to Privacy: Telephone Interception and Access in Australia", Technology and Society, 31 4 Spring 2012.

14 Ibid at p. 14.

15 Available at ://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF

16 European Commission, Report from the Commission to the Council and the European Parliament – Evaluation report on the Data Retention Directive, 18 April 2011, p. 15, https://www.eff.org/sites/default/files/filenode/dataretention/20110418_data_retention_evaluation_en.pdf

17 Ibid at p. 14.

18 Ibid at p. 5.