The Costs of Data Retention

Nikki Macor considers the implications of proposals for wide-sweeping data retention laws on carriers.

The *Cybercrime Legislation Amendment Act 2011* (Cth) amended Australia's telecommunications legislation to facilitate Australia's accession to the Council of Europe Convention on Cybercrime, by enabling certain domestic agencies and the AFP to require that carriers preserve certain stored communications. This data preservation regime is relatively limited, requiring that agencies issue a preservation notice only where, among other requirements, access is intended to be obtained by a warrant. Communications are only required to be preserved for a maximum of 90 days or over a month-long period. The main impact on carriers, aside from a limited increase in storage requirements, is likely to be the need to ensure routine data destruction procedures allow for data subject to a preservation notice to be retained for the requisite period.

However, the government does not intend to stop at a limited data preservation regime. As outlined in the article 'Telecommunications data retention: a step in the right direction?' in this issue, the government is considering the introduction of a much broader communications data retention regime, which could require retention of data for up to 2 years.

The fundamental public policy behind both the data preservation regime and the proposed data retention regime is focused on ensuring Australian law enforcement and intelligence capabilities are adequate to deal with the ever-increasing threat posed by cybercrime.

But how will these requirements affect stakeholders? The submissions to the Parliamentary Joint Committee on Intelligence and Security inquiry (***Inquiry***) provide valuable insights into the industry's concerns.

Cost

One of the most vexing issues for industry stakeholders is the cost of establishing infrastructure to meet proposed data retention requirements.

iiNet's Chief Regulatory Officer made a statement to the Inquiry quoting a rough calculation of $60 million for start up costs for two years data storage, which would equate to approximately $400 million for the whole industry, if source and destination IP addresses are included in the scope of data required to be stored.[1] He also noted the industry's understanding that the government intends to reimburse only the actual cost of the data requested from time to time. Invariably the additional costs will be passed on to consumers, at a rate estimated by iiNet to be around $5 per month.

The Australian Mobile Telecommunications Association and Communication Alliance (the ***Associations***) cited set up costs of $500 million to $700 million and noted that any additional data element could add tens of millions of dollars to set up costs.[2] It observed that in some European countries where data retention regimes are in place, capital and operational costs incurred in compliance are reimbursed by the government, and called for the same to occur in Australia.[3]

Processing burden

Many submissions raised concerns about the onerous processing activities required to store and manage specific data sets in large volumes.

Telstra's concerns were focused on the burden of processing and managing large data sets.[4] In its view, the requirements would involve the inspection, identification and extraction of required communications data, and that this would expand its role inappropriately into communications interception.

The fundamental public policy behind both the data preservation regime and the proposed data retention regime is focused on ensuring Australian law enforcement and intelligence capabilities are adequate to deal with the ever-increasing threat posed by cybercrime

Optus, among others, raised the impracticality of effectively searching records to locate information sought by law enforcement agencies, given the sheer volume of data to be retained.[5] The Internet Society of Australia[6] also noted the additional labour force requirements that feed into the cost implications discussed above.

Security

Data security is an increasingly sensitive issue and the damage caused by breaches is constantly growing as more information is stored and transmitted electronically, and accordingly security was one of the other main issues raised by stakeholders.

Tim Berners-Lee, who is generally recognised as one of the founders of the internet, has described the data that would be stored under the proposed data retention regime as 'dynamite'.[7] He expressed doubts as to the ability of the government to keep the information secure and described what would be available to hackers as 'dossiers' of information on individuals. This highlights the importance of ensuring rigorous security over the data retained, which will amount to two years' worth of information about the communications of the nation.

---

1 S Dalby, Commonwealth Parliamentary Joint Committee on Intelligence and Security, 27 September 2012.

2 The Australian Mobile Telecommunications Association and Communication Alliance, Submission No. 114, Parliamentary Joint Committee on Intelligence and Security, [3.47].

3 The Australian Mobile Telecommunications Association and Communication Alliance, Submission No. 114, Parliamentary Joint Committee on Intelligence and Security, [3.45].

4 Telstra, Submission No. 189, Parliamentary Joint Committee on Intelligence and Security, p11.

5 Optus, Submission No. 206, Parliamentary Joint Committee on Intelligence and Security, p3.

6 Internet Society of Australia, Submission No. 145, Parliamentary Joint Committee on Intelligence and Security, p3.

7 Lateline, 29 January 2013, (available at: http://www.abc.net.au/lateline/content/2013/s3679053.htm).

As the government will not be storing the majority of the data, the standards by which carriers and carriage service providers will store and recover data will be critical to maintaining the security of the treasure trove of information. As noted by the Internet Industry Association, it is not yet clear what standards will be imposed,[8] but what is clear is that higher standards will lead to higher costs.

Competitiveness

Submissions identified potential issues for competitiveness at both domestic and international levels.

The Internet Industry Association explained that increased costs imposed on Australian services may result in them suffering a competitive disadvantage against offshore 'over-the-top' services such as Gmail.[9] Offshore providers are already dominant, and any reduction in the competitiveness of the Australian industry would merely reinforce and exacerbate this situation.

The Internet Society of Australia also pointed out that domestic competition may be hampered by higher barriers to entry, given the additional costs and infrastructure requirements associated with meeting proposed data retention requirements.[10]

Privacy

The retention and availability of vast stores of personal information poses an obvious threat to privacy that was recognised in a number of submissions.

In its written submission, iiNet concluded that data retention requirements would effectively create a statutory exemption to National Privacy Principle 1.1 under the *Privacy Act 1988* (Cth), which requires that an organization not collect personal information unless the information is necessary for one or more of its functions or activities.[11]

iiNet's statement to the Inquiry raised the likelihood that the proposed data retention requirements will be extended to other fields in due course, such as transport, utilities and retailers. The Associations pointed out that the inclusion of location data of mobile telephone users could result in continuous tracking and surveillance of all mobile customers.[12]

Given the volume of information that will be collected under the data retention proposal, this could have a significant impact on privacy protections for all Australians.

Conclusion

With the recent retirement of Nicola Roxon as Attorney General, there may be some doubt as to the future of the data retention proposal. Roxon's incoming replacement Mark Dreyfus has been reported as being sympathetic to privacy concerns and it is not yet clear whether he will support and prioritise the proposal as strongly as Roxon.[13] However, as the submissions to the Inquiry indicate, if the government does proceed with the proposal, there will be significant issues to be overcome by the industry.

Nikki Macor is a lawyer at Allens. The views expressed in this article are the views of the author only and do not represent the views of any organisation.

---

8 Internet Industry Association, Submission No. 187, Parliamentary Joint Committee on Intelligence and Security, p8.

9 Internet Industry Association, Submission No. 187, Parliamentary Joint Committee on Intelligence and Security, p8.

10 Internet Society of Australia, Submission No. 145, Parliamentary Joint Committee on Intelligence and Security, p3.

11 iiNet, Submission No. 108, Parliamentary Joint Committee on Intelligence and Security, p12.

12 The Australian Mobile Telecommunications Association and Communication Alliance, Submission No. 114, Parliamentary Joint Committee on Intelligence and Security, [3.48].

13 C Porter, news.com.au, 4 February 2013 (available at: http://www.news.com.au/technology/mark-dreyfus-not-ruling-out-data-retention-spy-plan/story-e6frfro0-1226570198350); J Gliddon, itnews, 4 February 2013 (available at: http://www.itnews.com.au/News/331094,data-retention-stalls-at-committee-level.aspx).

Contributions & Comments

Contibutions and Comments are sought from the members and non-members of CAMLA, including features, articles, and case notes. Suggestions and comments on the content and format of the Communications Law Bulletin are also welcomed.

Contributions in hard copy and electronic format and comments should be forwarded to the editors of the Communications Law Bulletin at editor@camla.org.au or to

Valeska Bloch or Victoria Wark

C/- Allens
Deutsche Bank Place
Corner Hunter & Philip Streets
SYDNEY NSW 2000

Tel: +612 9230 4000
Fax: +612 9230 5333

Please note the change to CAMLA contact details:

Email: camla@tpg.com.au
Phone: 02 9399 5595
Mail: PO Box 237,
KINGSFORD NSW 2032