Going against the flow: Australia enacts data retention law

Graham Greenleaf, Professor of Law & Information System, UNSW Australia

(2015) 134 *Privacy Laws & Business International Report*, 26-28

On 26 March 2015 Australia enacted the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* ('Data Retention Law').[1] The conservative Abbott government received bipartisan support from the Labor opposition, after it agreed to a few amendments, despite opposition from the cross-benches (Greens and others), and rejection by many sectors of civil society, industry and the media. Many critical submissions were received by the Senate committee that reported on the Bill.[2] However, opinion polls indicate majority public support for the legislation, though younger Australians are evenly divided.[3]

This is the end of the line for legal opposition to the law. Australia does not have a Bill of Rights or any other constitutional protections capable of invalidating an overly-broad or otherwise repressive data retention law.[4] Nor is Australia a party to any international convention or agreement which is likely to be able to used to invalidate such a law.[5] Nor will a change of government have any effect, given Labor's complicity in its enactment.

This situation in Australia is in stark contrast with Europe where, both before and after the 2014 decision of the EU Court of Justice in the *Digital Rights Ireland Case*[6] striking down the Data Retention Directive, data retention laws in many European countries have been declared invalid, or laws redrafted in an attempt to reconcile them with fundamental rights as identified by the Court.

Key features of the data retention law

Prior to this Act, law enforcement and intelligence agencies, and others, already had access to 'metadata' (as it is now called in Australia – previously 'call data' and similar terms) without a judicial warrant. However, ISPs and telcos (the two classes of 'service provider' entities affected by the Act) kept data at their discretion, there was no requirement for them to keep it for two years or any other period.

---

[1] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015 (as passed by both houses) <http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fbills%2Fr5375_aspassed%2F0000%22;rec=0 > ; see legislative history <http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r5375>

[2] See for example 'Australian Privacy Foundation Submission on the Data Retention Bill 2014' <http://ssrn.com/abstract=2553652>.

[3] Lowy Institute 'Data retention scheme has majority support from Australians' 27 March 2015 <http://www.lowyinterpreter.org/post/2015/03/27/Data-retention-scheme-has-majority-support-from-Australians.aspx>

[4] There is an implied right of political free speech according to High Court decisions, but it is not likely to be relevant here.

[5] Article 17 of the *International Covenant on Civil and Political Rights* (ICCPR) is the only relevant provision. It does not have any direct effect in Australian law, but breaches of it can found a complaint to the UN Human Rights Committee. A Committee decision has once previously found that Australia breached Article 17 (*Toonen v Australia*), and while of no legal effect within Australia, did lead to political steps to change the law concerned.

[6] *Digital Rights Ireland (Judgment of the Court)* [2014] EUECJ C-293/12 www.worldlii.org/ eu/cases/EUECJ/2014/C29312.html; see PL&B International, December 2014, pp. 23-27

'Metadata' is now defined – The government had refused to define in the Bill introduced to Parliament the information that ISPs etc would have to retain, preferring to state only that it must relate to one of seven very general categories of information (eg 'the source of a communication'). A concession to enable passage is that the Act now defines what is in each of the categories (eg for the sources category, 'Identifiers of a related account, service or device from which the communication has been sent by means of the relevant service.'). Examples are given of what is to be retained under each defined category (eg 'Cell towers, Wi-Fi hotspots' under the location of equipment category) (s187AA).

What's not metadata – The Act now contains provisions which appear to (as the Act says) 'put beyond doubt' that service providers are not required to keep 'information about telecommunications content' or 'information about subscribers' web browsing history', or communications that pass "over the top" of the underlying service the service provider provides, or location information which goes beyond what the service provider uses to provide the service (s187A).

Two year (or more) retention period – All data covered by the Act is required to be retained for two years (s187C). However, there is no requirement that data then be destroyed, and the Act explicitly states that it does not prevent a service provider from keeping the data longer.

Encryption, security and Privacy Act protections required – Service providers must both encrypt, and 'protect' against unauthorised access or disclosure the data they are required to keep (even if it is not 'personal information' with security obligations under the Privacy Act) (s187BA). The *Privacy Act* will apply to any metadata which relates to (a) an individual or (b) a communication to which the individual is a party, by making that data 'personal information', and irrespective of whether the service provider might be otherwise exempt from the *Privacy Act* (eg as a 'small business provider' (s187LA)).

Data retention implementation plans – There will be a Communications Access Co-ordinator who will supervise a complex scheme of approving data retention plans submitted by service providers, after they are considered by enforcement and security agencies. The government 'may make a grant of financial assistance to a service provider' to assist them to comply with the legislation (s187KB). The high costs of compliance with the Act's obligations are likely to ensure that service providers do the government's bidding in order to obtain these discretionary funds. Uncertainty concerning the costs of the scheme, or who will bear it, has been one of the continuing controversies concerning the Bill, with many referring to it as 'the Internet tax'.

Access without warrant allowed to 20 organisations or classes of organisations – Intelligence agencies plus fourteen 'criminal law enforcement agencies' will not require a warrant to access such metadata (but will still require a warrant to access 'content' – 'stored communications'). They include the Australian Taxation Office (ATO), Australian Securities and Investment Commission (ASIC) and the Australian Competition and Consumer Commission (ACCC). The Minister can also declare additional authorities to be a 'criminal law enforcement agency', but such a declaration will lapse 40 days after Parliament next sits.

Supposed civil litigation exemption – A new provision, recommended by the PJCIS, aims to exempt from access metadata kept 'solely for the purpose of complying' with this Act, 'in connection with a civil proceeding' authorised by a court process (s280(1A)). The word 'solely' will make it very difficult to prove that this provision applies. Anyway, exceptions (function creep) can be made by regulations. There is a widespread belief that one of the main purposes of this legislation will be that it will be used to pursue copyright infringements by ensuring that ISPs keep the data desired by media owners. Now that an Australian court

has decided that ISPs can be required to hand over identification of users of peer-to-peer networks,[7] if ISPs attempt to refuse to hand over metadata of file-sharers based on this provision, intense pressure from content owners to create an exception by regulation is likely to follow. It is unlikely that either side of politics will resist such well-financed persuasion.

Some extra protection for journalists – A warrant will be required to access the metadata of professional journalists if and when the security or enforcement personnel 'reasonably believes' this is for the purpose of identifying a source used by the journalist (eg has a journalist contacted a particular public servant). The head of ASIO may request the Attorney-General to issue a 'journalist information warrant' specifying the public interest grounds on which such disclosure considered is necessary (s180J). Enforcement agencies can obtain a warrant from a prescribed magistrate or administrative tribunal member. High level judicial supervision is therefore not required. Other professions whose communications are normally privileged, such as lawyers and doctors, will not obtain any similar protection, in contrast with UK government policy.

Independent Senator Nick Xenophon summed up the law's effect as 'Metadata is all the information that defines your presence on line, taken and stored from your digital devices such as your phone, tablet and computer. So the Government can now, without a warrant, find out where your devices have been, who you've been emailing or phoning and the duration and location of those contacts.'[8]

Promised trade-off: mandatory data breach reporting

As part of the deal with Labor to get the Bill through, the government accepted a recommendation by the PJCIS to introduce a mandatory data breach reporting (MDB) scheme by the end of 2015. However, the PJCIS did not specify details, so it is unknown whether the new MDB Bill will resemble the previous Labor government's unsuccessful 2013 Bill.[9] It is assumed that such an obligation will be imposed not only on ISPs but on all parties (public or private sector), and would apply to all metadata (whether or not it is 'personal data').

At the moment, the MBN scheme is little more than an IOU to the Australian public, from a government that could not keep world leaders' passport and visa data safe, but didn't bother telling them until they read about it in the newspapers.[10] If Canberra doesn't think that Vladimir Putin or Barack Obama needs data breach notification, what they have in mind for ordinary Australian citizens might not be worth much.

Conclusions

Australia's Minister for Communications, partly responsibility for defending the Bill, has (among others) advised the public on how to legally avoid its effects:[11] use Gmail or some other web-based mail service located outside of Australia (and enjoy content surveillance by Google instead); use some organisation's Wi-Fi service that does not require registration; use

---

[7] Dallas Buyers Club LLC v iiNet Limited [2015] FCA 317 (7 April 2015) < http://www.austlii.edu.au/au/cases/cth/FCA/2015/317.html>

[8] Nick Xenophon blog 'Senate update' 1 April 2015 < http://www.nickxenophon.com.au/blog/senate-update/>

[9] See Mary-Anne Nielsen (Australian) Parliamentary Library *Bills Digest: Privacy Amendment (Privacy Alerts) Bill 2013*, BILLS DIGEST No. 146, 2012–13, 19 June 2013; Graham Greenleaf 'Privacy enforcement in Australia is strengthened: gaps remain' (2014) 128 *Privacy Laws & Business International Report* 1-5

[10] Scott Ludlam 'The Australian government can't safeguard Putin's data. That means yours isn't safe, either' *Guardian Australia*, 31 March 2015 <http://gu.com/p/4756j/sbl>

[11] Philllip Branch "Is it possible to circumvent metadata retention and retain your privacy?" *The Conversation*, 31 March 2015 <http://theconversation.com/is-it-possible-to-circumvent-metadata-retention-and-retain-your-privacy-39429>

a VPN located outside Australia or another '5 Eyes' country; or use TOR; and so on. Will those who really are carrying out illegal activities be unaware of these side-steps? And how will the 'intelligence and law enforcement community' react to this? This legislation gives the impression of being only a first step, not the last word. There are many aspects of the Bill where Ministerial declarations can be used to expand its scope, able to be used in response to alleged emergencies, which will lapse after 40 days only if the Labor opposition has the spine to refuse to enact legislation making them permanent. This is a recipe ripe for government exploitation by national security and law-and-order campaigns.

This article's brief analysis identifies only a selection of the criticisms of the Act made by ISPs, the legal profession, civil libertarians and others, which have been well-analysed elsewhere.[12] Australia's legislation, and its subsequent history, may provide valuable lessons for countries that have not yet enacted such laws, including those in Europe.

[12] Many other objections are conveniently analysed in the Parliamentary Library 'Bills Digest' report on the Bill, referred to above.