



THE LAW SOCIETY
OF NEW SOUTH WALES

Our ref: HumanRightsJEvk:939104

3 March 2015

Senator the Hon Eric Abetz
Leader of the Government in the Senate
PO Box 6100
Senate
Parliament House
Canberra ACT 2600

By email: senator.abetz@aph.gov.au

Dear Senator Abetz,

Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014

I am writing on behalf of the Human Rights Committee of the Law Society of NSW ("Committee").¹

The Committee is deeply concerned about the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 ("Bill") and its effect on individuals and businesses in Australia, and writes to you to oppose the Bill in its present form.²

If this Bill is to pass, the Committee strongly urges that it be amended to require that:

- judicial warrants be obtained for accessing metadata;
- access to the metadata be restricted to criminal law enforcement agencies for preventing, detecting or prosecuting serious crimes; and
- the Bill be subject to sunset provisions.

The Committee notes the recommendations of the Parliamentary Joint Committee on Intelligence and Security in its advisory report on the Bill,³ and submits these recommendations do not adequately address the serious privacy concerns raised by the Bill.

¹ The Committee is responsible for considering and monitoring Australia's obligations under international law in respect of human rights; considering reform proposals and draft legislation with respect to issues of human rights; and advising the Law Society accordingly.

² The Committee has previously made submissions to the Attorney General on 10 April 2014 expressing its concerns about a mandatory metadata collection and retention scheme.

³ Parliamentary Joint Committee on Intelligence and Security, *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, 27 February 2015, available online: http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Data_Retention/Report (accessed 3 March 2015).

Given the highly sensitive nature of metadata, and evidence that its collection and retention has little to no effect on crime clearance rates,⁴ the Committee respectfully submits that the Government has not adequately justified the proposed intrusion on the right to privacy.

The Committee sets out its views in more detail below.

1. The nature of metadata

Accessing an individual's metadata can be as intrusive, if not more telling,⁵ as accessing the content of that individual's communications, as it can reveal that person's associations and movements,⁶ sensitive personal information, including health information and even a person's sexual orientation.⁷

The Committee notes the submission of internet service provider iiNet to the Senate Inquiry on the Comprehensive Revision of the Telecommunications (Interception and Access) Act 1979 (Cth) which stated that:

Contrary to the Attorney-General Department's submission to this Committee, access to telecommunications data is not necessarily less privately [sic] intrusive than access to the content of a communication. We draw the Committee's attention to recent research from Stanford University which should put to bed the fallacy that the community should only be concerned about access to telecommunications content and not "metadata" or telecommunications data. Telecommunications data when accessed and analysed may create a profile of a person's life including medical conditions, political and religious views and associations:

The researchers initially shared the same hypothesis as their computer science colleagues, Mayer said. They did not anticipate finding much evidence one way or the other.

"We were wrong. Phone metadata is unambiguously sensitive, even over a small sample and short time window. We were able to infer medical conditions, firearm ownership and more, using solely phone metadata," he said.⁸

⁴ "Impossible to Ensure Legality of EU Communications Data Retention Directive Says German Parliament" (26 April 2011), available online: <http://www.vorratsdatenspeicherung.de/content/view/446/79/lang,en/> (accessed 3 March 2015).

⁵ The Committee notes this report in the *New York Magazine*:

"When you take all those records of who's communicating with who, you can build social networks and communities for everyone in the world," mathematician and NSA whistle-blower William Binney — "one of the best analysts in history," who left the agency in 2001 amid privacy concerns — told Daily Intelligence. "And when you marry it up with the content," which he is convinced the NSA is collecting as well, "you have leverage against everybody in the country." [emphasis in the original]

See Joe Coscarelli, "Metadata Can Be More Revealing Than Your Actual Conversations", *New York Magazine*, 7 June 2013, available online: <http://nymag.com/daily/intelligencer/2013/06/metadata-whats-in-your-phone-records.html> (accessed 3 March 2015).

⁶ Malte Spitz, "Germans loved Obama. Now we don't trust him," *New York Times*, 29 June 2013, available online: http://www.nytimes.com/2013/06/30/opinion/sunday/germans-loved-obama-now-we-dont-trust-him.html?_r=1 (accessed 3 March 2015)

⁷ Matthew Moore, "Gay men 'can be identified by their Facebook friends'," *The Telegraph*, 21 September 2009, available online: <http://www.telegraph.co.uk/technology/facebook/6213590/Gay-men-can-be-identified-by-their-Facebook-friends.html> (accessed 3 March 2015)

⁸ Clifton B. Parker, "Stanford students show that phone record surveillance can yield vast amounts of information", *Stanford Report*, March 12, 2014, available online: <http://news.stanford.edu/news/2014/march/nsa-phone-surveillance-031214.html> (accessed 7 April 2014)



It's not at all clear that this increased surveillance and fundamental privacy risk, together with the significant cost, is either necessary or proportionate. We've not seen solid evidence that justifies surveilling minors and citizens on the chance that two years later some evidence might help an investigation.⁹

2. Right to privacy

As a signatory to the International Covenant on Civil and Political Rights ("ICCPR"), the Committee notes that state intrusions on the right to privacy must be necessary and proportionate. Article 17 of the ICCPR sets out as follows:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.

Given the highly sensitive nature of metadata, the Committee submits that the Government has not adequately justified how its collection and retention in the way proposed by the Bill is necessary and proportionate. The Committee notes that the experience of other jurisdictions has been that that data retention had no impact on either the effectiveness of criminal investigations or the crime rate.¹⁰ For example, a February 2011 opinion published by the Legal Services of the German Parliament cited data suggesting only a marginal increase in crime clearance rates:

This marginal increase in the clearance rate by 0.006% could raise doubts about whether the provisions in their current form would stand their ground under a proportionality review. In any case, the relationship between ends and means is disproportionate.¹¹

3. Committee's submissions

3.1. The Bill should be opposed in its present form

The Committee respectfully submits that the Bill should not be passed in its present form.

The Committee's view is that it is strongly arguable that such intrusion on individuals' privacy is neither necessary nor proportionate as required by Article 17 of the ICCPR. The Committee therefore opposes the collection and mandatory retention of metadata in the way proposed by the Bill.

3.2. Judicial warrants for access

If the Bill is to pass, the Committee remains concerned about the lack of legal oversight over the proposed collection of, and access to, metadata. Given its highly sensitive nature, the Committee's view is that if metadata is to be

⁹ Senate Standing Committees on Legal and Constitutional Affairs, *Comprehensive revision of Telecommunications (Interception and Access) Act 1979*, submission no. 38 made by iiNet, available online: http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Legal_and_Constitutional_Affairs/Comprehensive_revision_of_TIA_Act/Submissions (accessed 3 March 2015)

¹⁰ Katie Miller, "Ditch the data retention bill," *Australian Financial Review – technology section* 3 March 2015 at 25 citing evidence from Germany, Britain and USA.

¹¹ See note 4 which provides the English translation.



mandatorily collected, access to metadata should only be permitted under a judicial warrant.

3.3. Access be restricted to criminal law enforcement agencies

The Committee is also concerned about the potential for an increasing number of people and organisations permitted to access collected metadata. The Committee submits that access to metadata should be restricted to criminal law enforcement agencies in respect of serious crimes. The Bill currently provides the Attorney-General discretion to allow the use of metadata in civil proceedings,¹² and submits that this provision should be removed.

3.4. Sunset provisions

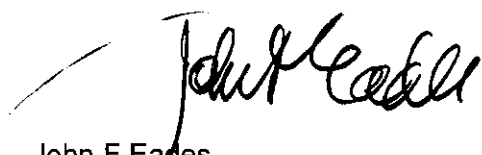
Finally, the Committee has serious concerns about the permanence of what is essentially a mass surveillance scheme, in the context of increasing legislative intrusion on the rights and liberties of individuals in the name of national security.

For example, the Committee notes that the *Counter-Terrorism Legislation Amendment (Foreign Fighters) Act 2014* further extends the sunset provisions in respect of control orders, preventative detention orders, anti-terrorism stop, search and seizure powers, and ASIO's questioning and detention powers.

The Committee acknowledges that the proposed legislation is subject to a review within four years of its introduction. However, given its extraordinary nature, the Committee submits that the scheme should also be subject to a sunset provision.

Thank you for considering this submission. If you have any questions, please contact Vicky Kuek, policy lawyer for the Committee, on victoria.kuek@lawsociety.com.au or (02) 9926 0354.

Yours sincerely,



John F Eades
President

¹² Proposed section 176A(4)(f) of the Bill allows the Minister to declare any authority or body an enforcement agency where the Minister considers it may be relevant. The Law Council of Australia has argued in its submission to the Parliamentary Joint Committee on Intelligence and Security dated 20 January 2015 that this could include local councils, organisations responsible for enforcing copyright infringement and gambling authorities. Available online: [http://www.lawcouncil.asn.au/lawcouncil/images/2923 - Telecommunications Interception and Access Amendment Data Retention Bill 2014.pdf](http://www.lawcouncil.asn.au/lawcouncil/images/2923_-_Telecommunications_Interception_and_Access_Amendment_Data_Retention_Bill_2014.pdf) (accessed 3 March 2015).