



THE LAW SOCIETY
OF NEW SOUTH WALES

Our Ref: PDL: EEap1747772

27 June 2019

Mr Jonathan Smithers
Chief Executive Officer
Law Council of Australia
DX 5719 Canberra

By email: Christopher.brown@lawcouncil.asn.au

Dear Mr Smithers,

Parliamentary Joint Committee on Intelligence and Security: Review of the mandatory data retention regime under the *Telecommunications (Interception and Access) Act 1979*

Thank you for the opportunity to contribute to a submission on the Parliamentary Joint Committee on Intelligence and Security's ("PJCIS") Review of the mandatory data retention scheme under Part 5-1A of the *Telecommunications (Interception and Access) Act 1979* (Cth) ("TIA Act"). The Law Society's Privacy and Data Law Committee has contributed to this submission.

The Law Society supports the 2014 submission and supplementary submission of the Law Council of Australia in relation to the provisions and its policy position on a mandatory telecommunications data retention regime. Our general observations of the scheme are outlined below.

Privacy and security concerns

The *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* amended the TIA Act to require all telecommunications and internet service providers to store a mandatory set of telecommunications data ("metadata") for a period of two years for all users of their services. In progressing these amendments, the Australian Government recognised access to metadata as a "critical tool" for law enforcement and intelligence agencies' investigative and enforcement functions.¹

While we agree with the Law Council's position in recognising a legitimate need for law enforcement and intelligence agencies to have access to telecommunications data in relevant circumstances, we echo the concerns raised in relation to the scheme's structure and operation – in particular, the privacy and data security implications.

In the four years since the legislation passed, there have been significant technological developments. Today, more can be gleaned about an individual than ever before through metadata and the application of data analytics, which takes

¹Revised Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015* (Cth), 5.

advantage of real advances in artificial intelligence. Despite assurances that the scheme provides sufficient protections to the privacy of a communication by not permitting access to the content of communications,² we note significant research has established that a certain amount of metadata about an individual may provide sufficient information to construct a complete profile of that individual, particularly if it is matched with publicly available records.³ Indeed, the Court of Justice of the European Union held in *Tele2 Sverige AB v Post-Och Telestyrelsen* and *Secretary of State for the Home Department v Watson* (“Tele2”) that access to traffic and location data can “allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained”.⁴ The Court found that relevant data may provide a means “of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications”.⁵

The Law Society is concerned about the security of data collected and stored by service providers. We note hacking capabilities have become increasingly sophisticated and that many governments and large corporations have been unable to protect themselves against sophisticated attacks on their stored information.⁶ These attacks may be mounted by state actors or sophisticated criminal groups. We consider the dangers of maintaining such large datasets, even in encrypted format, are significant, and pose an attractive target to would-be attackers.

The legislation provides limited information and guidance to service providers about their storage and security requirements (apart from requiring that the information be encrypted and for organisations to comply with relevant privacy laws). While we note service providers may have stored metadata for years prior to the legislation’s passage,⁷ they are now required to do so by law. Given the mandatory nature of the scheme, which requires a significant amount of information to be stored for a two-year period, we consider that the TIA Act should prescribe a security framework for such storage. We also support the inclusion of a requirement that data be stored in Australia, which we consider is necessary from both a data sovereignty and data security perspective.

Appropriateness of retention period

The Commonwealth Government has only produced two annual reports outlining the extent to, and circumstances in, which government agencies have used the access powers available under the TIA Act since commencement of the scheme (for the

² Revised Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015* (Cth).

³ See eg, L Hardesty, ‘Privacy challenges, Analysis: It’s Surprisingly Easy to Identify Individuals from Credit-card Metadata’, *MIT News Office* (online, 29 January 2015) <<http://news.mit.edu/2015/identify-from-credit-card-metadata-0129>>; K Martineau, ‘Location Data on Two Apps Enough to Identify Someone, Says Study’, *Data Science Institute, Columbia University* (Web Page, 13 April 2016) <<https://datascience.columbia.edu/location-data-two-apps-enough-identify-someone-says-study>>.

⁴ Court of Justice of the European Union, C-203/15; C-698/15, ECLI:EU:C:2016:970, 21 December 2016 [99].

⁵ *Ibid.*

⁶ See eg, N McKenzie and A Grigg, ‘Australia’s Defence Department was Badly Exposed to China’s Hackers’, *Sydney Morning Herald* (online, 29 November 2018) <<https://www.smh.com.au/politics/federal/australia-s-defence-department-was-badly-exposed-to-china-s-hackers-20181129-p50j48.html>>.

⁷ Revised Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015* Cth.

reporting years 2015-2016 and 2016-2017).⁸ The most recent report provides a breakdown of the age of data accessed under the scheme over the 2016-2017 reporting year. We note approximately 94 per cent of access to retained data was to data less than 12 months old, less than 5 per cent was for data between 12 months and 2 years old, and 1.5 per cent was for data more than 2 years old. Seventy-nine per cent of data access was for data 0-3 months old.⁹

Noting the vast majority of data access requests are made within the first 12 months of storage (based on statistics presently available), we query whether retention for a two-year period is necessary or whether a reduced mandatory retention period may be more appropriate, particularly noting the security concerns raised above.

Costs of the scheme

While the two annual reports produced since commencement of the scheme illustrate the successful use of data in the prosecution and conviction of various offences, they also demonstrate the significant costs associated with the scheme.

The Annual Report for 2015-2016 indicates the estimated capital costs to industry for implementing data retention obligations were \$198,527,354 as of 30 June 2016.¹⁰ The industry capital costs of compliance with the mandatory data retention scheme in the period 2016-2017 were \$119,793,739.83.¹¹ The Commonwealth Government provided \$134,593,265.57 of public funding through the single-round Data Retention Industry Grants Programs to 174 recipients to comply with the scheme over the 2016-2017 reporting period.¹²

Noting the significant expenses associated with the scheme's operation, both to industry and to the Australian community, we recommend careful consideration be given to whether these costs are reasonable, necessary and proportionate to meeting the scheme's stated purposes. We also recommend careful consideration be given to whether less expensive and less intrusive alternatives are available.

Appropriateness of oversight and approval mechanisms

Under section 110A of the TIA Act, 20 law enforcement agencies at both the state and federal level are able to lawfully access retained metadata when investigating relevant offences. The Act also enables the Minister to make a declaration to prescribe an agency as a "criminal law-enforcement agency" for the purpose of lawful access to this data.¹³ Any of the prescribed agencies may internally authorise access to this data. Agencies are only required to apply for a warrant if seeking to access metadata that would identify a journalist's information source.

⁸ Attorney-General's Department (Cth), *Telecommunications (Interception and Access) Act 1979 – Annual Report 2015-2016* (Report, 2016) <<https://www.homeaffairs.gov.au/nat-security/files/telecommunications-interception-access-act-1979-annual-report-15-16.pdf>>, Department of Home Affairs, *Telecommunications (Interception and Access) Act 1979 – Annual Report 2016-2017* (Report, 2017) <<https://www.homeaffairs.gov.au/nat-security/files/telecommunications-interception-access-act-1979-annual-report-16-17.pdf>>.

⁹ Department of Home Affairs, *Telecommunications (Interception and Access) Act 1979 – Annual Report 2016-2017*, Table 38.

¹⁰ Attorney-General's Department, *Telecommunications (Interception and Access) Act 1979 – Annual Report 2015-2016*, 58.

¹¹ Department of Home Affairs, *Telecommunications (Interception and Access) Act 1979 – Annual Report 2016-2017*, Table 40.

¹² Department of Home Affairs, *Telecommunications (Interception and Access) Act 1979 – Annual Report 2016-2017*, 31.

¹³ *Telecommunications (Interception and Access) Act 1979*, sub-s 110A(m).

We note there are vast differences in the experience, capabilities and resources of law enforcement agencies authorised to access data under the scheme, and in their capacity to comply with their requirements under the TIA Act. Indeed, the Commonwealth Ombudsman, which is authorised to assess agency compliance with obligations under the TIA Act, has identified various discrepancies between the processes and systems each agency has in place and their overall compliance with the scheme. In its report on the monitoring of agency access to stored communications and telecommunications data for the period 2015-2016, the Ombudsman found that while agencies at that time were generally attempting to become compliant with the scheme, the (then) Department of Immigration and Border Protection (DIBP) was non-compliant and did not have sufficient processes in place for the Ombudsman to determine whether the Department was lawfully dealing with stored data.¹⁴ In its report on the monitoring of agency access to stored communications and telecommunications data for the period 2016-2017, the Ombudsman noted DIBP had not implemented the Ombudsman's previous recommendation for a centralised record keeping system and advised that the risks previously identified in relation to DIBP's record keeping practices had not been addressed.¹⁵ In that report, the Ombudsman made two formal recommendations to the Department of Home Affairs (which replaced DIBP), for improved storage practices and processes, and for accurate accounting of authorisations made.

While we note the Ombudsman provides a level of oversight over law enforcement agencies' use of the scheme, its approach is retrospective – it assesses compliance once agencies have used their relevant access powers. The Ombudsman has recognised that a “person who has been subject to the powers will not be aware of the fact, and therefore, will not be in a position to make a complaint”.¹⁶ The covert nature of agencies' access powers tends to corrode a person's right to obtain a remedy, noting they are almost always unaware any intrusion has occurred.

In our view, the oversight mechanisms contained in the scheme are inadequate. We consider an external oversight and approval regime for agencies' original data access requests, in addition to a post-access compliance oversight regime, would be more appropriate.

We note in the Tele2 decision,¹⁷ the Court of Justice of the European Union held that it is “essential” that access to retained data should, except in cases of clear urgency, be subject to prior review by either a court or an independent body. In the recent

¹⁴ Commonwealth Ombudsman, *A Report on the Commonwealth Ombudsman's Monitoring of Agency Access to Stored Communications and Telecommunications Data under Chapters 3 and 4 of the Telecommunications (Interception and Access) Act 1979: For the Period 1 July 2015 to 30 June 2016* (Report, March 2017), 30
<https://www.ombudsman.gov.au/data/assets/pdf_file/0018/45423/TIA-Act-Annual-Report-2015-16.pdf>.

¹⁵ Commonwealth Ombudsman, *A Report on the Commonwealth Ombudsman's Monitoring of Agency Access to Stored Communications and Telecommunications Data under Chapters 3 and 4 of the Telecommunications (Interception and Access) Act 1979: For the Period 1 July 2016 to 30 June 2017* (Report, November 2018), 33
<https://www.ombudsman.gov.au/data/assets/pdf_file/0033/96747/201617-Chapter-4A-Annual-Report.pdf>.

¹⁶ Commonwealth Ombudsman, *A Report on the Commonwealth Ombudsman's Monitoring of Agency Access to Stored Communications and Telecommunications Data under Chapters 3 and 4 of the Telecommunications (Interception and Access) Act 1979: For the Period 1 July 2015 to 30 June 2016* (Report, March 2017), 1.

¹⁷ *Tele2* (Court of Justice of the European Union, C-203/15; C-698/15, ECLI:EU:C:2016:970, 21 December 2016) [108].

case of *Big Brother Watch v The United Kingdom*,¹⁸ the European Court of Human Rights (ECHR) found that “since the individual will necessarily be prevented from seeking an effective remedy of his or her own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding his or her own rights”. The Court ultimately held the United Kingdom’s bulk interception of communications violated the European Convention on Human Rights, including due to the “absence of robust independent oversight”.¹⁹

Over ten European countries have a judicial oversight regime for access to retained data. We strongly encourage implementation of an independent access approval mechanism in Australia, for example by requiring judicial review of access requests or by referring authorisation functions to an independent, external body.

Client legal privilege in the age of data retention

Client legal privilege protects the communications which clients have with their lawyers. It is a privilege that has been honoured since Elizabethan times. In *Baker v Campbell*,²⁰ Murphy J emphasised the importance of protecting a client’s privacy from the intrusion of the state, noting, “the client’s legal privilege is essential for the orderly and dignified conduct of individual affairs in a social atmosphere which is being poisoned by official and unofficial eavesdropping and other invasions of privacy”.

We note that when the PJCIS sought submissions in relation to the proposed data retention laws in 2014, the Law Council expressed concerns that while telecommunications data may not reveal the content of the communications, it would reveal who a lawyer has contacted, the identity and location of the lawyer, and the identity and location of witnesses. This may reveal a litigation or defence strategy.

Measures that can be taken to protect lawyer-client communications rely on encryption. However, in December 2018, the Federal Government passed the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* to enable Australian law enforcement agencies to access the content of end-to-end encrypted information. Internet companies are now obliged to assist law enforcement agencies with accessing information, in compliance with an appropriate warrant or court order. The legislation also imposes an obligation on device manufacturers and service providers to assist intelligence and law enforcement agencies with a warrant to access encrypted information.

By contrast, the 2015 United Nations Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, stated that states should promote strong encryption and anonymity, and national laws should recognise that individuals are free to protect the privacy of their digital communications by using encryption technology and tools that allow anonymity online.²¹

¹⁸ European Court of Human Rights, Chamber, Application Nos 58170/13, 6322/14 and 24960/15, 13 September 2018 [309].

¹⁹ *Ibid* [347].

²⁰ (1983) 153 CLR 52, 85, 116–7 (Murphy J).

²¹ David Kaye, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HCR/29/32 (22 May 2015) <https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx>.

We recommend the Review carefully consider the interaction between the data retention scheme and new encryption legislation, and the effects on lawyers' ability to protect their confidential client communications as a result.

International developments

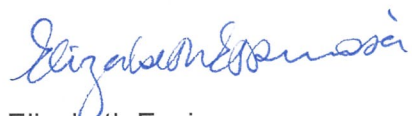
Due to developments in technology that enable the cost-effective storage and processing of large datasets, the broad, state-based surveillance of members of a population has increased globally. The trend toward mass, indiscriminate surveillance has, however, been met with increasing opposition.

In particular, we draw attention to the Court of Justice of the European Union's 2016 *Tele2* decision²² which found that, to be consistent with privacy rights, any law concerning metadata retention must limit the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted. Following this decision, the Irish Government commissioned the former Chief Justice of Ireland, John Murray, to review its current data retention legislation. That report was released on 4 October 2017, finding that the Irish data retention regime breached European law and amounted to mass surveillance of the entire population of the Irish State. The scheme in Ireland, much like in Australia, enabled police and other state authorities to access metadata with a disclosure request and without judicial oversight. The report stated the statutory framework was indiscriminate in application and scope and was being implemented without the consent of those affected. A draft bill accompanying the report proposed the data retention scheme be modified to require greater judicial oversight and a requirement that a High Court judge approve access to journalists' metadata.

We also note the recent case of *Big Brother Watch v The United Kingdom*,²³ in which the ECHR considered a challenge to three different systems of mass surveillance adopted by the United Kingdom's intelligence services. Relevantly, the ECHR found the regime for obtaining communications data from communications service providers was not limited to combatting "serious crime", was not subject to prior review by a national authority and did not sufficiently protect journalists' confidential communications. The Court held the regime was therefore in breach of the European Convention on Human Rights.

Thank you again for seeking our input on this important topic. Should you have any questions in relation to this submission, please contact Adi Prigan, Policy Lawyer, on (02) 9926 0285 or email Adi.Prigan@lawsociety.com.au.

Yours sincerely,



Elizabeth Espinosa
President

²² *Tele2* (Court of Justice of the European Union, C-203/15; C-698/15, ECLI:EU:C:2016:970, 21 December 2016) [108].

²³ *Big Brother Watch v The United Kingdom* (European Court of Human Rights, Chamber, Application Nos 58170/13, 6322/14 and 24960/15, 13 September 2018).