Office of the Victorian Information Commissioner

t 1300 00 6842
e enquiries@ovic.vic.gov.au
w ovic.vic.gov.au

PO Box 24274
Melbourne Victoria 3001

Our ref: D19/827

12 July 2019

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600

Dear Committee Secretary

Review of the mandatory data retention regime

Thank you for the opportunity to provide comment on the review of the mandatory data retention regime (**regime**). Under s 187N of the *Telecommunications (Interception and Access) Act 1979* (**TIA Act**), the Committee is required to review the mandatory data retention regime introduced by Part 5 – 1A of the TIA Act.

My office, the Office of the Victorian Information Commissioner (**OVIC**), has a unique regulatory focus, with combined oversight over privacy, information security and freedom of information in Victoria, administering both the *Privacy and Data Protection Act 2014* (**PDP Act**) and the *Freedom of Information Act 1982* (Vic).

Under the PDP Act, my office is responsible for setting standards for the security and integrity of law enforcement data systems and access to law enforcement and crime statistics data, as well as auditing such use under the Victorian Protective Data Security Framework. Further, I have an express function under the PDP Act to make public statements in relation to any matter affecting personal privacy or the privacy of any class of individual.[1] As such, the mandatory data retention regime has been of particular interest to my office for some time.

In 2015, my office's predecessor, the Office of the Commissioner for Privacy and Data Protection (**CPDP**), made a submission to the Committee's inquiry into the *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*.[2] My office shares many of the concerns raised by the former CPDP, particularly in relation to the following themes:

- the necessity and proportionality of the regime;
- the misconception that metadata about communications is inherently less privacy invasive than the content of communications;
- the information security concerns posed by the regime; and
- the overall lack of oversight, accountability and transparency of the regime.

As such, I have organised my comments under these above themes.

[1] Under s 8C(1)(f) of the PDP Act.
[2] Available on the Committee's website, here: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Data_Retention/Submissions.

The necessity and proportionality of the regime

In the context of this regime, metadata is information about communications, as distinct from the contents or substance of communications. However, metadata can reveal a wide range of personal and sensitive information about an individual,[3] in the case of this regime, painting a highly detailed picture of the private lives of Australians. The personal information contained in metadata, such as an individual's associations and patterns of communication, combined with its organised and standardised format, is precisely why it is so useful for the purposes contemplated under this regime.[4]

General concerns as to the necessity and proportionality of the regime

Under this regime, profoundly personal information belonging to almost all Australians, is being recorded and retained with what appears to be no corresponding requirement for people subject to this regime to be reasonably suspected of committing a crime or to be a person of interest. I question whether the mass intrusion on the privacy of millions of Australians brought on by this regime is proportionate to the benefits it brings to law enforcement and national security.

The datasets of personal information held by service providers under this regime are extraordinarily valuable; effectively creating a large number of 'honey pots' for malicious actors. When personal information such as this is the subject of a privacy or security breach, it may lead to real harm to affected individuals, such as identity theft, reputational damage, financial loss and even physical violence.[5] If even one of these datasets were to be compromised, it could cause serious harm to many Australians. I strongly encourage the Committee to take this into account when considering the proportionality of this regime.

The requirement that authorised officers must have regard for the seriousness of any offence in relation to an authorisation under Divisions 4 and 4A of Part 4 – 1, for the disclosure of metadata sought, is welcome.[6] However, I believe that merely having regard to the seriousness of offences is not sufficient to prevent this regime from being used disproportionately against a range of offences.

This regime excludes metadata from 'over the top' communications, such as WhatsApp, from being retained.[7] In practice, this suggests that malicious actors could take precautions to lawfully evade the regime, by using 'over the top' communications,[8] leaving unsuspecting Australians subject to pervasive monitoring. This further highlights my concerns as to the effectiveness of the regime, proportionate to its invasive nature.

Apparent interaction with the Telecommunications Act 1997

I am concerned about the potential for legislation scope creep, given the interaction between the regime and the *Telecommunications Act 1997* (**Telecommunication Act**), whether intended or not. I recommend the Committee consider the need for more guidance on the interaction between the TIA Act and the Telecommunications Act, and determine whether amendments need to be made to reduce the scope of

---

[3] See, for example, Jonathan Mayer, Patrick Mutchler, and John Mitchell, 'Evaluating the privacy properties of telephone metadata' (2016) 113 (20) *Proceedings of the National Academy of Sciences of the United States of America 5536*, available at https://www.pnas.org/content/113/20/5536; Will Ockenden, 'What reporter Will Ockenden's metadata reveals about his life', *Australian Broadcasting Corporation* (online, 24 Aug 2015) <https://www.abc.net.au/news/2015-08-24/metadata-what-you-found-will-ockenden/6703626>.

[4] See, for example, Australian Federal Police, Submission No 7 to Parliamentary Joint Committee on Intelligence and Security, *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* 7; Malcom Crompton, 'Privacy Unravelled: How much does the government know about us?', *Australian Broadcasting Corporation* (Radio, 29 May 2019) <https://www.abc.net.au/radio/programs/pm/how-much-does-the-government-know-about-us/11161460>.

[5] Office of the Victorian Information Commissioner, *Managing the privacy impacts of a data breach* (May 2019) page 3.

[6] Under s 180F(aa)(i) of the TIA Act.

[7] Under s 187A(4)(c) of the TIA Act.

[8] For example, a malicious actor could evade this regime by using a messaging application not operated by a service provider. See Commonwealth, *Parliamentary Debates*, Senate, 24 March 2015, 2132 (Sen Scott Ludlam); Daniel Hurst, '*Malcolm Turnbull explains how people can avoid having metadata collected*' (online, 25 March 2015) <https://www.theguardian.com/australia-news/2015/mar/25/malcolm-turnbull-explains-how-people-can-avoid-having-metadata-collected>.

access to metadata. Further, for clarity, I recommend that information retained under the TIA Act only be disclosed under provisions in the TIA Act, in so far as possible.

Data retention period

Under the regime, metadata is to be retained by service providers for two years,[9] a period of time longer than most other comparable regimes.[10] It appears that in the 2016/17 period, approximately 79 per cent of disclosures were for metadata less than three months old,[11] with just over six per cent of disclosures being for metadata older than 12 months.[12] I question the necessity of retaining this data for such a long period of time, especially considering the substantially negative impacts regimes like this can have on privacy. This retention period may create a 'chilling effect' – deterring people from exercising legal freedoms.[13]

The misconception that metadata about communications is inherently less privacy invasive than the content of communications

There is an idea that the metadata of communications is significantly less personal than the actual contents of communications. This is implied in the Explanatory Memorandum for the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014,[14] and is inferred by the TIA Act itself, in that it specifically excludes "the contents or substance of a communication".[15] However, it is widely acknowledged that metadata can be used to reveal extremely personal information,[16] and in fact can often be used as a proxy for content itself.[17] In many circumstances, the metadata of messages can reveal more information about a person than the contents of their messages.[18] For example, mobile phone metadata can be used to reveal an individual's age and gender,[19] religion and sexual preferences,[20] to predict an individual's personality,[21] or to predict the future location and activities of an individual's friends.[22] Former US National Security Agency (**NSA**) General Counsel, Stewart Baker, noted that "metadata absolutely tells you everything about somebody's life. If you have enough metadata, you don't really need content."[23]

I am firmly of the view that the metadata of communications can be just as personal as the contents of communications, and therefore equally privacy invasive in the hands of an unintended audience. I urge the Committee to take this into account when reviewing this regime.

---

[9] Under s 187C of the TIA Act.

[10] See, for example, 'Mandatory Data Retention around the World', *Privacy Sniffs* (Web Page) <https://privacysniffs.com/data-retention-law>.

[11] 230,176 (the number of authorisations for the disclosure of metadata between 0-3 months old) is 78.7% of 292,463 (the total number of authorisations). See Department of Home Affairs, *Telecommunications (Interception and Access) Act 1979 Annual Report 2016–17*, page 49, available at https://www.homeaffairs.gov.au/nat-security/files/telecommunications-interception-access-act-1979-annual-report-16-17.pdf.

[12] 18,009 is the total number of authorisations for the disclosure of metadata older than 12 months (5921 + 4091 + 2323 + 1138 + 4536), being 6.158% of 292,463 (the total number of authorisations) in the 2016/17 year. See Department of Home Affairs, *Telecommunications (Interception and Access) Act 1979 Annual Report 2016–17*, page 49, available at https://www.homeaffairs.gov.au/nat-security/files/telecommunications-interception-access-act-1979-annual-report-16-17.pdf>.

[13] See, for example, Elizabeth Stoycheff, 'Under surveillance: Examining Facebook's spiral of silence effects in the wake of NSA internet monitoring' (2016) 93.2 *Journalism & Mass Communication Quarterly* 296.

[14] See Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, 10.

[15] See, for example, TIA Act s 187A(4)(a).

[16] Above n 3; Rachel Adler, 'What Metadata Reveals About You', *The Century Foundation* (Web Page, 21 July 2016) <https://tcf.org/content/facts/what-metadata-reveals-about-you>.

[17] See, for example, Declaration of Professor Edward W. Felten, in *American Civil Liberties Union v Clapper* 27, Case No. 13-cv-03994, 39, available at https://www.clearinghouse.net/detailDocument.php?id=76786.

[18] See, for example, Commonwealth, *Parliamentary Debates*, Senate, 29 July 2014, page 20 (Mr Dalby, Chief Regulatory Officer, iiNet Limited).

[19] Bjarke Felbo et al, 'Using deep learning to predict demographics from mobile phone metadata' (2016), available at https://openreview.net/forum?id=91EEnoZX0HkRlNvXUKLA.

[20] See, for example, *Klayman v Obama,* 957 F. Supp. 2d 1 35, 36 (D.D.C. 2013).

[21] Yves-Alexandre de Montjoye et al, 'Predicting Personality Using Novel Mobile Phone-Based Metrics' (2013) *Proceedings of the 6th international conference on Social Computing, Behavioral-Cultural Modeling and Predictions,* 48.

[22] Eunjoon Cho, Seth Myers and Jure Leskovec, 'Friendship and Mobility: User Movement In Location-Based Social Networks', (2011) *Proceedings of the 17th ACM SIGKDD international conference on Knowledge discovery and data mining* 1082.

[23] As stated in a discussion with Alan Rusbridger: 'The Snowden Leaks and the Public' (2013) 60(18) *The New York Review of Books*.

The information security concerns posed by the regime

Encryption of retained metadata

The TIA Act expressly requires that information retained under this regime be encrypted.[24] It is positive to see requisite security measures included in legislation. However, due to the evolving nature of security threats, encrypting the information may not always be sufficiently effective in ensuring the confidentiality of information alone – other measures may also be required. While I note that the requirement to encrypt information is complemented by a secondary requirement to protect the information from unauthorised interference or access,[25] as well as similar requirements under Australian Privacy Principle 11 of the *Privacy Act 1988* (**Privacy Act**), I recommend amending the prescriptive requirement to encrypt information, and instead requiring that reasonable steps be taken to secure the information that are proportionate to the security risks associated with the information. Such a requirement could still be complemented by the secondary requirement to protect the information from unauthorised interference or access, and I expect would be more applicable in a changing risk environment and amenable to further definition in guidance, that can be more easily updated than legislation.

Destruction of retained metadata

There appears to be no express requirement under the TIA Act that metadata be destroyed after a period of time.[26] The destruction of personal information no longer needed for an identifiable purpose is a common requirement under privacy law.[27] Not destroying data retained under the regime when it is no longer required for an identifiable purpose significantly increases privacy and information security risks. For example, this could increase the amount of personal information that needs to have protections applied to it, increase the potential harm that could be caused should the information be subject to a privacy or security breach, and increase the probability that large quantities of personal information will be retained for no legitimate purpose.

Further, the absence of an express requirement introduces uncertainty as to the retention period of the data (taking into account obligations under the Telecommunications Act and the Privacy Act). I suggest introducing an express requirement that metadata retained by service providers under this regime, that is older than two years and is not needed for any lawful purpose, be permanently destroyed.

In addition, there is no requirement that enforcement agencies who access metadata destroy it once they no longer need it. I would also recommend including a requirement that enforcement agencies destroy any copies of metadata they have accessed under this regime once it is no longer needed for the purpose for which it was disclosed.

The overall lack of oversight, accountability and transparency of the regime

Transfer of metadata outside Australia

Aside from potential for harm caused to individuals should a dataset retained under the regime be compromised, these datasets likely contain official information, such as information regarding the communications and movements of members of Parliament or heads of intelligence agencies, which would undoubtedly be of interest to foreign states. The TIA Act currently appears to have no express restrictions on this data being transferred outside of Australia. While the operation of s 187LA of the TIA Act provides clarity on the privacy obligations, under the Privacy Act, of service providers in relation to data held under

[24] Under s 187BA(a) of the TIA Act.
[25] Under s 187BA(b)
[26] See s 187C(3) of the TIA Act.
[27] See, for example, Australian Privacy Principle 11 – Security of personal information under the Privacy Act; Information Privacy Principle 4 – Data Security under the PDP Act.

the regime, I recommend the Committee consider the need for express restrictions on transborder data flows under the TIA Act.

Secondary uses of metadata accessed under the regime

Although there are some restrictions on the circumstances in which metadata can be disclosed to enforcement agencies,[28] there appears to be no express restrictions on how enforcement agencies can use or disclose metadata once they have accessed it. This opens up the possibility of enforcement agencies using or disclosing metadata for unknown and opaque purposes that cannot be predicted by the public, or for purposes which had not been envisaged by Parliament when the legislation was passed. I recommend expressly restricting the use and disclosure of metadata by law enforcement agencies to the purpose for which it was originally disclosed to those agencies.

While I acknowledge that some of the above issues may be covered by other legislation, such as the Privacy Act, I believe that due to the volume and nature of information retained under the regime, these issues should be explicitly addressed in the TIA Act to avoid doubt.

Expansion of the regime via subordinate instruments

The TIA Act allows the Minister to declare an authority or body to be an enforcement agency,[29] allowing them to authorise the disclosure of metadata retained under this regime to that authority or body. The Minister may also declare modifications to the kinds of information to be kept by service providers.[30] This executive ability to expand the scope of what kinds of metadata are retained, and who can access it, has the potential to drastically change the nature of this regime without sufficient transparency, parliamentary scrutiny and public debate, especially considering the sheer number of agencies who are seeking to be declared enforcement agencies.[31] I recommend that changes to the agencies that are considered enforcement agencies, and the kinds of information to be kept under this regime, be allowed by legislative amendment only.

While the Commonwealth Ombudsman has oversight of the mandatory data retention regime,[32] that oversight only applies to enforcement agencies. Service providers, on the other hand, are subject to the Privacy Act, administered by the Office of the Australian Information Commissioner (**OAIC**), to the extent that their activities relate to data retained under this regime.[33] Considering the number of service providers, the number of datasets held by service providers, and the volume of highly personal information within each dataset, I suggest ensuring the OAIC is appropriately resourced to oversee the privacy and information security practices of service providers under the regime.

Annual reporting requirements

The Minister is required to report annually on authorisations made by enforcement agencies under the regime.[34] I recommend expanding the reporting requirements to include information regarding the effectiveness of this regime, such as the number of arrests, proceedings and convictions that were based on evidence obtained from metadata. Such a quantitative assessment would provide greater transparency as to the effectiveness of the regime.

---

[28] For example, under s 178(3) of the TIA Act.
[29] Under s 176A(3) of the TIA Act.
[30] Under ss 187A(3A), 187AA(2) of the TIA Act.
[31] A Freedom of Information Request in 2016 revealed 61 agencies that have requested to be declared an enforcement agency under s 176A(2), available at https://www.righttoknow.org.au/request/requests_for_access_to_telecommu#incoming-4557. However, the Minister did not declare any agencies to be enforcement agencies in the 2015/16 period or in the 2016/17 period, see Department of Home Affairs, *Telecommunications (Interception and Access) Act 1979 Annual Report 2015–16,* page VIII; Department of Home Affairs, *Telecommunications (Interception and Access) Act 1979 Annual Report 2016–17*, page VII.
[32] Under Chapter 4A of the TIA.
[33] Under s 187LA of the TIA Act.
[34] Under s 186 of the TIA Act.

I thank you again for the opportunity to comment on the review. My office will watch the progress of the Committee's inquiry on the mandatory data retention regime with interest.

I have no objection to this letter being published by the Committee without further reference to me. I also propose to publish a copy of this letter on the OVIC website but would be happy to adjust the timing of this to allow the Committee to collate and publish submissions proactively.

If you have any questions regarding any of the above, please don't hesitate to contact me or my colleague Asher Gibson, Policy Officer, at asher.gibson@ovic.vic.gov.au.

Yours sincerely,

Sven Bluemmel
Information Commissioner