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: D20/5512

26 March 2020

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

By email only to pjcis@aph.gov.au

Dear Committee Secretary

Review of the mandatory data retention regime – supplementary submission

Thank you for the opportunity to provide additional comment on the review of the mandatory data retention regime (**regime**) in the *Telecommunications (Interception and Access) Act 1979* (**TIA Act**). The particular focus for my comments is on access by agencies to retained telecommunications data under the *Telecommunications Act 1997* (**Telecommunications Act**), outside the TIA Act framework.[1]

My office, the Office of the Victorian Information Commissioner (**OVIC**), has 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. I also 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.[2] The regime therefore continues to be of particular interest to my office.

In 2015, my office's predecessor, the Office of the Commissioner for Privacy and Data Protection, made a submission to the Committee's inquiry into the *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*.[3]

In July 2019, my office made a submission to the Committee's review.[4] This submission touched on a range of topics relevant to the regime, including the necessity and proportionality of the regime, the significance of metadata, information security, and the lack of oversight, accountability and transparency of the regime.

I am pleased to provide this further supplementary submission to the Committee's review.

---

[1] This relates to the eighth dot point in the Committee's inquiry Terms of Reference (https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Dataretentionregime/Terms_of_Reference).
[2] Under s 8C(1)(f) of the PDP Act.
[3] Available on the Committee's website, here: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Data_Retention/Submissions.
[4] Available on the Committee's website here: https://www.aph.gov.au/DocumentStore.ashx?id=dce78942-662e-454d-a17c-e23cf7e5b934&subId=668111.

Interaction with section 280 of the Telecommunications Act

Legislation scope creep

An important limit on the regime in the TIA Act is the number and type of organisations who may receive and use metadata. Indeed, the regime was intended to strictly limit and reduce the range of enforcement agencies permitted to access metadata without a warrant.[5] This recognises the significance of access to metadata, and that only certain organisations should be able to see and use it, and for limited purposes.

However, submissions to the Committee's inquiry note that organisations who are not authorised under the TIA Act to access metadata,[6] may nonetheless be able to access that data through a combination of section 280(1)(b) of the Telecommunications Act and the organisation's authorising legislation.[7] This provision permits the disclosure or use of information if the disclosure or use is required or authorised by or under law. The Communications Alliance Ltd notes organisations such as local councils, the RSPCA, Environment Protection Authority, and State coroners have requested access to data for purposes ranging from managing traffic offences to the unlawful removal of trees.[8] This appears to go against the purpose and intent of restricting access to metadata under the regime.

In contrast, I note the joint submission of the Department of Home Affairs (**DHA**) and the Department of Infrastructure, Transport, Regional Development and Communications (**DITRDC**) states section 280(1)(b) of the Telecommunications Act is not a loophole to the regime in the TIA Act.[9] However, this submission also recognises the merit in further guidance for stakeholders on section 280 and other related elements in the Telecommunications Act,[10] given concerns raised by stakeholders about the operation of this section in previous submissions.

In my office's previous submission, I noted my concern regarding the potential for legislation scope creep given the interaction between the regime and the Telecommunications Act, whether intended or not.[11] In that submission, I suggested that the Committee consider, amongst other things, whether amendments need to be made to reduce the scope of the access to metadata to ensure that information retained under the TIA Act is only disclosed under the provisions in that Act, in so far as possible.

I acknowledge DHA and DITRDC's advice that they intend to prepare more guidance on the operation of section 280 of the Telecommunications. However, I do not believe guidance is sufficient to remedy current and future legislation scope creep. Instead, I confirm my previous recommendation that there be a legislative restriction to ensure that information retained under the TIA Act only be disclosed under provisions in the TIA Act, in so far as possible.

Necessity and proportionality

The mandatory retention of metadata by service providers relating to millions of Australians is significant and invasive. Not only does it create a mass intrusion into the private lives of Australians, but it does so in circumstances where it appears there is no requirement for people subject to this regime to be reasonably suspected of committing a crime or to be a person of interest. While there is a public interest in appropriate agencies having the capabilities to adequately investigate serious criminal investigations and

---

[5] Commonwealth, *Parliamentary Debates*, House of Representatives, 30 October 2014, 12560 (Malcolm Turnbull, Minister for Communications), available here: https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22chamber%2Fhansardr%2F4a3ea2e7-05f5-4423-88aa-f33e93256485%2F0010%22.

[6] Under section 110A of the TIA Act.

[7] See, for example, Communications Alliance, Submission No. 27 to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Mandatory Data Retention Regime* (12 July 2019).

[8] Communications Alliance, Submission No. 27 to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Mandatory Data Retention Regime* (12 July 2019).

[9] Department of Home Affairs and the Department of Infrastructure, Transport, Regional Development and Communications, Submission No. 21.2 to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Mandatory Data Retention Regime*, 23.

[10] Ibid, 22.

[11] Office of the Victorian Information Commissioner, Submission No. 23 to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Mandatory Data Retention Regime* (12 July 2019), 2.

matters of national security, allowing a broader range of agencies to access such data for much more minor matters would be disproportionate to the invasion of privacy that is involved.

Metadata can reveal a range of personal and sensitive information about an individual,[12] and paint a highly detailed picture of the private lives of Australians. For example, mobile phone metadata can be used to reveal an individual's age and gender,[13] religion and sexual preferences,[14] to predict an individual's personality,[15] or to predict the future location and activities of an individual's friends.[16] It can also reveal an individual's associations and patterns of communication, which can be incredibly useful for the purposes contemplated under the regime.[17]

If there is a privacy or security breach in relation to this kind of information, this may lead to real and serious harm to many Australians, such as identity theft, reputational damage, financial loss and physical violence.[18] This risk of harm is increased by the apparent broadening of access rights under the Telecommunications Act, meaning the more organisations that hold and store the data, the greater the opportunity for it to be misused, on-shared, or combined with other information an organisation holds about individuals to create a rich profile about their lives.

I strongly encourage the Committee to consider the nature of the metadata, the number of organisations who may access that information, and the necessity and proportionality of the regime in the way it interacts with section 280 of the Telecommunications Act. I also encourage the Committee to consider broader community expectations around the disclosure and use of their personal information – would a member of the public reasonably expect their mobile phone's metadata be disclosed to their local council for a parking offence? Probably not.

Thank you again for the opportunity to comment on the review. My office will continue to 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 Sarah Crossman, Senior Policy Officer, at sarah.crossman@ovic.vic.gov.au.

Yours sincerely,

Sven Bluemmel
Information Commissioner

---

[12] 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>.

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

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

[15] 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.

[16] 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.

[17] 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>.

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