Office of the Victorian Information Commissioner

t 1300 006 842
e enquiries@ovic.vic.gov.au
w ovic.vic.gov.au

PO Box 24274
Melbourne Victoria 3001

Our ref: D22/3048

10 February 2022

Electronic Surveillance Reform Branch
Department of Home Affairs

*Via online submission*

**Submission in response to the *Reform of Australia's electronic surveillance framework Discussion Paper***

Thank you for the opportunity to make a submission in response to the discussion paper 'Reform of Australia's electronic surveillance framework' (**discussion paper**).

My office, the Office of the Victorian Information Commissioner (**OVIC**), is the primary regulator for information privacy, information security and freedom of information in Victoria, administering both the *Privacy and Data Protection Act 2014* (Vic) (**PDP Act**) and the *Freedom of Information Act 1982* (Vic). The reform of Australia's electronic surveillance framework is of particular interest to my office, given the covert and intrusive nature of government surveillance powers, and their impacts on our individual and collective privacy.

As Information Commissioner, I appreciate the fundamental role that privacy plays in our society. It is an enabler of personal autonomy and a protector of imbalances in power between government and citizen. To ensure there is ongoing room for privacy to operate, any government surveillance must be limited by law to what is strictly necessary and proportionate in a democratic society. Surveillance that goes beyond this remit is not only an unjustified invasion of privacy, but a threat to the very foundations of our way of life.

OVIC is pleased to see a focus on privacy, necessity, and proportionality in the discussion paper and supports the following proposals for reform of the electronic surveillance framework:

- Removing the distinction between 'stored' and 'live' communications, in recognition that the privacy invasion is the same, whether the government is accessing stored communications or intercepting live communications.[1]

- Requiring warrants and authorisations to be targeted at the person under investigation in the first instance.[2] In OVIC's view, the present ability for ASIO and the AFP to obtain a computer access warrant, without needing to first establish that the use of the powers is directed at a particular person who is reasonably suspected of serious wrongdoing,[3] should not be retained in the new framework.

[1] Response to Discussion Paper, Questions 11 and 12.
[2] Response to Discussion Paper, Question 20.
[3] *Australian Security Intelligence Organisation Act 1979* (Cth), section 25A(2); *Surveillance Devices Act 2004* (Cth), section (1)(c).

- With respect to third party warrants, requiring agencies to satisfy the test for an ordinary warrant, *and* an additional threshold - that obtaining information directly from the person under investigation would be impractical or ineffective;[4] and

- Requiring an agency, in all cases, to satisfy an issuing authority that the use of a particular power would be necessary and proportionate before the warrant is issued.[5] In OVIC's view the matters to be considered by the issuing authority[6] should be set out in legislation. Further, the framework should be drafted such that the warrant can only be issued if the issuing authority is satisfied that the agency is requesting to collect the minimum information necessary, in the least invasive way, to achieve the stated objective.

The remainder of this submission raises issues of concern to OVIC, that may be of assistance in establishing the key principles which will guide the development of draft legislation. The submission responds in order of the content and questions in parts 1-5 and 7 of the discussion paper.

**Part 1: Who can access information under the new framework?**

**Response to question 1 – Do existing prohibitions against unlawful access to information and data adequately protect privacy in the modern day?**

1. In OVIC's view, the prohibitions in the *Telecommunications (Interception and Access) Act 1979* (Cth) (**TIA Act**),[7] *Telecommunications Act 1997* (Cth) (**Telecommunications Act**)[8] and *Criminal Code Act 1995* (Cth) (**Criminal Code**)[9] require amendment, to ensure that *all* private communications and *all* private information is adequately protected from unlawful access.

2. OVIC understands that under the current framework, content communicated using traditional SMS is protected from unlawful access while held by a carrier or carriage service provider.[10] Whereas, the same content communicated online using an over-the-top (**OTT**) service (such as Facebook Messenger or Apple iMessage) is not protected from unlawful access while held by the OTT service provider. According to the *Comprehensive Review of the Legal Framework of the National Intelligence Community* (**Comprehensive Review**), these OTT private communications are only protected from unlawful access while in transit over a telecommunications network, or if held in a computer.[11] OVIC also understands the prohibition in the Telecommunications Act on the use and disclosure of communications, metadata, and personal account information, only applies to traditional telephone calls and SMS, not communications made using OTT services.

3. In OVIC's view, this gap in the protection of online private communications is unacceptable in the modern day and should be remedied, given the growth in online private messaging and video-conferencing services in Australia, and parallel decline in the use of traditional SMS and telephone services.[12] OVIC notes that OTT communication services have already been recognised and included within the scope of protection in comparable international frameworks.[13]

[4] Response to Discussion Paper, Question 21.
[5] Response to Discussion Paper, Question 23.
[6] Listed on page 52 of the Discussion Paper.
[7] TIA Act, sections 7 and 108.
[8] Telecommunications Act, section 276.
[9] Criminal Code, Schedule 1, Parts 10.6 and 10.7.
[10] TIA Act, section 108.
[11] Dennis Richardson AC, *Comprehensive Review of the Legal Framework of the National Intelligence Community* (Volume 2, December 2019) [26.4] ('Comprehensive Review').
[12] For information on the prevalence of online private messaging and video-conferencing in Australia see ACCC, *Digital Platform Services Inquiry Interim report*, September 2020, 12.
[13] For example, Article 2 of the Directive (EU) 2018/1972 expanded the definition of 'electronic communications service' to include OTT communication services made available over the internet.

4. With respect to the protection of private information, such as personal documents and photographs, OVIC understands the Criminal Code currently protects private information on devices by including offences for unauthorised access or modification to data held in a computer and impairment of electronic communication to or from a computer.[14] These offences were introduced to the Criminal Code "to account for the change in the environment and to better reflect the community's dependence on telecommunications and the harm that can be done by misuse or disruption".[15]

5. The environment has shifted again since these offences were introduced, with the community becoming more reliant on cloud-based services and other OTT services, such as Dropbox, Apple iCloud and Google Photos, for the storage of private information, rather than storing information locally on a personal computer. OVIC queries whether the current prohibitions adequately protect private information held by these online service providers.

6. The harms caused by the intrusion of others into our private communications and private lives is the same, irrespective of whether the communication occurs over traditional telecommunications infrastructure, an OTT service, or some other method, and irrespective of where the information is stored and how it can be accessed. It is the private nature of the information or communication that is deserving of protection, not the method of its storage or transmission.[16]

7. The freedom to live one's life without being watched, or having the feeling of being watched, is essential to the development of personal autonomy and a hallmark of democratic society. In OVIC's view, the new framework should ensure that *all* electronic private communications and *all* private information is afforded equivalent levels of protection from unlawful access, irrespective of the device, technology or service used to store or transmit the information.

***Prohibitions must be supported by a culture of compliance and enforcement***

8. The ability to covertly access private information is a power given to law enforcement and the national intelligence community to engage in activities that would otherwise be unlawful. Contravention of a prohibition against unlawful access to, use and disclosure of information obtained through surveillance is a serious breach of public trust and a serious invasion of privacy. Penalties for breach of the law should reflect the seriousness of the crime and should be supported by a strong culture of compliance and enforcement. Weak compliance and enforcement offer silent consent to the erosion of our privacy and democratic values.

9. Similarly, the rigour with which agencies manage and oversee the tools and systems used to access surveillance information should reflect the public trust placed in agencies to act according to law. In OVIC's view, this should mean that deliberate misuse of an information system for unlawful purposes will result in workplace dismissal, not internal disciplinary action, or workplace guidance.

**Response to question 3 – Section 280(1)(b) of the Telecommunications Act 1997**

10. The discussion paper draws attention to the ability for organisations, other than law enforcement agencies, to obtain access to telecommunications data under sections 280(1)b) and 313(3) of the Telecommunications Act.[17] OVIC has previously raised concerns about legislation scope creep caused by these provisions,[18] and agrees with concerns raised in the discussion paper that these sections allow agencies to circumvent restrictions in the TIA Act and go beyond what was intended by Parliament.[19]

[14] Criminal Code Schedule 1, Parts 10.6 and 10.7.
[15] Explanatory Memorandum, *Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Bill (No. 2) 2004* (Cth) 4.
[16] This point was recognised when the prohibition on stored communications was first introduced into the TIA Act in 2006: See Explanatory Memorandum *Telecommunications (Interception) Amendment Bill 2006* (Cth) 10.
[17] Discussion paper, pages 16-17.
[18] OVIC submission to the Parliamentary Joint Committee on Intelligence and Security's Review of the mandatory data retention regime, 12 July 2019, https://ovic.vic.gov.au/wp-content/uploads/2019/08/OVIC-Submission-to-PJCIS-on-Review-of-the-mandatory-data-retention-regime.pdf.
[19] Discussion paper, pages 16-17.

11. In its review of the Mandatory Data Retention Regime (**MDRR**), the Parliamentary Joint Committee on Intelligence and Security (**PJCIS**) cited at least 87 non-law enforcement agencies gaining access to telecommunications data under section 280(1)(b), including local councils, and state and Commonwealth government agencies,[20] without effective oversight.[21] The PJCIS recommended that section 280(1)(b) of the Telecommunications Act be repealed and that access to telecommunications data be restricted only to the law enforcement agencies listed in section 110A of the TIA Act.[22] OVIC supports this recommendation.

**Response to question 4 – proposed considerations for determining whether additional agencies should be permitted to access peoples' information and data**

12. In OVIC's view the decision to grant an agency with power to access private information and communications, including telecommunications data, should be made by the Parliament, not the Executive. Ensuring these decisions are made by Parliament, and not the Executive, places certain safeguards on inappropriate expansion of powers, if (for example) the Executive were to act beyond the expectations of the community.

13. The list of permitted agencies and the extent of each agency's powers should be subject to periodic and public review, to ensure that electronic surveillance powers are removed or scaled down when no longer necessary and proportionate.

14. OVIC agrees with the considerations listed on page 18 of the discussion paper. Any additional considerations should align with international best practice principles.[23]

**Part 2 – What information can be accessed?**

**Response to question 5 – Are there other kinds of information that should be captured by the new definition of 'communication'? If so, what are they?**

15. OVIC believes the list of information proposed to be captured by the new definition of 'communication' is sufficient to protect the public against unauthorised access.[24] We also support the inclusion of information related to machine learning and emphasise that inferred information deserves equal protection. However, we question how a bill might be expected to extend to quantum computing given the uncertain state of data held in a quantum computer. Perhaps this might be better considered in terms of the outputs or inputs into a quantum computer rather than the information processed within the computer itself.

16. In addition, OVIC considers non-content information (also referred to as metadata, telecommunications data or technical information) should be given the same legal protection. Non-content information is discussed further below, in response to questions 8 and 18 of the discussion paper.

**Response to question 8 – What kinds of information should be defined as 'content' information? What kinds of information should be defined as 'non-content' information?**

17. OVIC does not agree with the premise of the discussion paper's distinction between content and non-content information. It is well-known and accepted internationally that non-content information is no less private, or deserving of protection, than content information.[25] According to former US National

[20] Parliamentary Joint Committee on Intelligence and Security, *Review of the mandatory data retention regime* (Final Report, October 2020) [5.94].
[21] Ibid, 74.
[22] Ibid, Recommendation 15, [5.100].
[23] For example, Necessary & Proportionate, *International Principles on the application of Human Rights to Communications Surveillance* (2014) https://necessaryandproportionate.org/.
[24] Discussion paper, page 22.
[25] Necessary & Proportionate, *International Principles on the Application of Human Rights to Communications Surveillance* (2014).

Security Agency General Counsel, Stewart Baker, "metadata absolutely tells you everything about somebody's life. If you have enough metadata, you don't really need content."[26]

18. OVIC and its predecessor, the Office of the Commissioner for Privacy and Data Protection, have regularly raised concerns regarding the misconception that metadata related to communications is inherently less privacy sensitive than the content of communications.[27] Numerous submissions by academics, integrity bodies and civil society groups have raised similar concerns in response to the PJCIS review of the MDRR and the Attorney General's Privacy Act Review Issues Paper.[28]

19. The International Principles on the Application of Human Rights to Communications Surveillance have included non-content information in the definition of 'communications' and 'communications surveillance' since 2014.[29] The Principles state that non-content information should be given the highest protection in law on the basis that:

> "It is clear that other information arising from communications – metadata and other forms of non-content data – may reveal even more about an individual than the content itself, and thus deserves equivalent protection. Today, each of these types of information might, taken alone or analysed collectively, reveal a person's identity, behaviour, associations, physical or medical conditions, race, colour, sexual orientation, national origins, or viewpoints; or enable the mapping of the person's location, movements or interactions over time, or of all people in a given location, including around a public demonstration or other political event."[30]

20. The value and sensitivity of non-content information is acknowledged by the Attorney-General's Department in its recent Privacy Act Review Discussion Paper, with one of the proposals being to update the definition of 'personal information' in the *Privacy Act 1988* (**Privacy Act**) to include technical and inferred information. The examples of technical and inferred information intended to be covered by the new protections in the Privacy Act include location data, online identifiers and one or more factors specific to the physical, physiological, genetic, mental, behavioural (including predictions of behaviours or preferences), economic, cultural or social identity or characteristics of a person.[31] As mentioned earlier, inferred information becomes a particularly important factor when considering the operation of machine learning systems and artificial intelligence.

21. Given the clear recognition in Australia and abroad that metadata can be just as, if not more, privacy sensitive than content information, OVIC strongly urges the principles and policy underlying this aspect of the proposed framework be reconsidered.

**Part 3 – How can information be accessed?**

**Response to question 15 – Proposal to simplify warrant framework**

22. The discussion paper proposes a new outcome-based electronic surveillance framework that would grant warrants to access certain types of information, such as one warrant for access to electronic communications and one warrant for access to surveillance information. The proposed approach departs from the current method-based framework that grants a warrant to use a particular method to

---

[26] As stated in a discussion with Alan Rusbridger: 'The Snowden Leaks and the Public' (2013) 60(18) *The New York Review of Books*.
[27] CPDP submission 39 to the PJCIS inquiry into the *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (January 2015) https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Data_Retention/Submissions; OVIC's *submission in response to the PJCIS review of the mandatory data retention regime* (July 2019) https://ovic.vic.gov.au/wp-content/uploads/2019/08/OVIC-Submission-to-PJCIS-on-Review-of-the-mandatory-data-retention-regime.pdf.
[28] See Submissions 4, 10, 19 and 28 to the PJCIS review of the mandatory data retention regime, available at https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Dataretentionregime/Submissions; See comments in Attorney-General's Department, *Privacy Act Review Discussion Paper* (October 2021) 22-23 https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/user_uploads/privacy-act-review-discussion-paper.pdf.
[29] Necessary & Proportionate, *International Principles on the Application of Human Rights to Communications Surveillance* (2014).
[30] Ibid, 4-5.
[31] Attorney-General's Department, *Privacy Act Review Discussion Paper* (October 2021) 26 – 28 https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/user_uploads/privacy-act-review-discussion-paper.pdf.

access information (for example, intercepting live communications, accessing stored communications or using a listening, visual, or data surveillance device).[32] The discussion paper states that under an outcome-based framework, the emphasis would be on the type and volume of information the agency wants to collect, the intrusiveness, and the matter being investigated, instead of the current focus on how the agency intends to collect the information.[33]

23. OVIC understands the potential benefits in moving to a technology neutral framework and commends the discussion paper's intention to bring a stronger focus to the privacy impact of obtaining access to information when determining if a warrant should be issued. However, OVIC shares the concerns raised by the Australian Human Rights Commission during the Comprehensive Review, that any reform of the electronic surveillance framework must not result in an increase in agency powers for the sake of consistency or administrative efficiency.[34]

24. OVIC is concerned about the potential for scope creep in the implementation of the proposed outcome-based framework if the methods of access are not made transparent, and agencies are only accountable to the issuing authority, rather than to Parliament, for the methods in which they choose to intrude into the private lives of the community. The new framework must be transparent and will need to be robust to ensure that access is only permitted where strictly necessary and proportionate, using the least intrusive means, and only collecting data that is necessary to achieve a legitimate aim.

25. OVIC notes that the Comprehensive Review did not recommend the framework proposed in the discussion paper.[35] Instead, the Comprehensive Review recommended the new framework continue to categorise and define warrants based on method of access. In reaching its conclusion, the Comprehensive Review considered a proposal put forward by ASIO that is somewhat similar in nature to the proposed outcome-based framework in the discussion paper. ASIO proposed to shift the legislation's emphasis to the effects sought, rather than the tools used, by allowing one single warrant to authorise access to information that may intrude into an individual's privacy, irrespective of the particular methods applied. The Comprehensive Review rejected the proposal on the basis it failed the transparency test.[36]

26. OVIC is similarly concerned that the proposed outcome-based framework will fail the transparency test unless the methods of access are listed in and limited by legislation. OVIC agrees with the statements made by the Comprehensive Review that:

> "Describing the tools agencies use to collect information provides the public with a degree of visibility and foreseeability about agency powers. A warrant regime that does away with the tools agencies may use to achieve its purposes also does away with the specificity that helps people to understand agency powers."[37]

27. OVIC is concerned that if the methods of access are not prescribed in legislation, the proposed framework will place too much responsibility on the issuing authority to ensure the use of agency powers is proportionate. The public is not privy to a warrant application or the reasons for issuing a warrant. Instead, the public must place its trust in the legislative framework and the competence of the issuing authority to only authorise surveillance where necessary and proportionate to achieving a legitimate aim. The issuing authority may struggle to determine if the proposed surveillance is proportionate, if the methods agencies are using to access information are not publicly known and have therefore not been the subject of public debate. As stated by the Comprehensive Review:

[32] Discussion paper, pages 33-36.
[33] Ibid.
[34] Comprehensive Review, Volume 2, 269.
[35] Comprehensive Review, Volume 2, 271-3.
[36] Ibid, 272.
[37] Ibid.

> "…changes in technology often lead to changes in how society views that technology, privacy and surveillance. There is value in a legislative framework that requires the public – through the Parliament – to revisit agencies' surveillance powers, and the limits, controls and safeguards on them, on a reasonably regular basis, to ensure that they remain consistent with societal expectations and values".[38]

28. OVIC is pleased to see the acknowledgement in the discussion paper that the method of access will still be a key consideration for the issuing authority when assessing the privacy impact of the warrant and its necessity and proportionality.[39] To further improve oversight and accountability, OVIC recommends the new framework include a legislative requirement for the agency to specify the proposed methods of access in the warrant application and a legislative requirement for the issuing authority to only grant access to information if the proposed methods are the least intrusive to achieving the legitimate aim of the warrant, and for the methods to be specified in the warrant as the only authorised methods of access.

29. If the methods of access are not made transparent and properly accounted for in the legislation, OVIC is concerned the proposed framework may result in increased covert and intrusive surveillance, over and above what is permitted under the existing framework. This issue becomes particularly important where the thresholds for approving surveillance allow it to occur for the prevention or prosecution of less serious offences. Such an outcome would be detrimental to public trust in government, and risks the creation of a surveillance framework, over and above that which is necessary in a democratic society.

**Part 4 – When will information be accessed?**

**Response to question 17 – Is it appropriate to harmonise legislative thresholds (as outlined in the discussion paper) for covert access to private communications, content data and surveillance information where existing warrants are functionally equivalent?**

30. In OVIC's view, warrant thresholds must be based on demonstrable (evidence-based) need and must be proportionate. That is, surveillance should only be conducted when it is the only effective means of achieving a legitimate aim, or, when there are multiple effective means, it is the means least likely to be privacy invasive and infringe upon human rights. The government bears the onus of justifying that surveillance is necessary and proportionate, and the legislation should only permit surveillance powers to be used when their use has been properly justified.

31. OVIC queries whether there is a proper justification for the current legislative thresholds, which enable the application of surveillance powers to all offences carrying a particular maximum penalty, irrespective of the subject matter or nature of the crime. The offences caught by current legislative thresholds, such as tax evasion and trademark infringement, do not appear to match the public statement of the Secretary of the Department of Home Affairs that electronic surveillance powers are only intended to be used for "the worst offences such as terrorism, child exploitation and organised crime".[40]

32. OVIC strongly recommends a review of the crimes covered by the current legislative thresholds, with a view to constraining and restricting the use of surveillance powers to only those crimes where it is demonstrably necessary and proportionate, when weighed against the infringement of rights caused by the intrusion into the private lives of the community, and the chilling effects on perceptions of individual freedom. Legislative thresholds based on demonstrable need improve clarity and

[38] Ibid.
[39] Discussion paper, 35.
[40] Rebecca Le May, '*Privacy fears swirl around surveillance law overhaul but top bureaucrat instead warns of capitalist data trawling*' (The Australian, 20/01/22), https://www.theaustralian.com.au/breaking-news/privacy-fears-swirl-around-surveillance-law-overhaul-but-top-bureaucrat-instead-warns-of-capitalist-data-trawling/news-story/cf3021270450a117155b8ad34244f973?btr=92e86e67f8dd1756ffaa67b7959f4733.

transparency, by enabling people to foresee and understand when these extraordinary powers can be used.

***Proposal to expand ASIO powers to retain information for the purposes of training an AI model to use for compliance purposes***

33. In Part 4, the discussion paper states that "[i]n line with the Comprehensive Review's recommendations, the Government will consider expanding the scope of agency powers to access, use and retain information for the purpose of developing, testing, maintaining and evaluating electronic surveillance and cyber capabilities and technologies."[41]

34. OVIC understands that one of the Comprehensive Review's recommendations was for ASIO to retain information that has been lawfully collected for a different purpose (including non-compliant information) and retain this information for a potentially extended period of time for the purpose of developing AI for compliance purposes.[42] This is an extraordinary use of surveillance information that should only be permitted where it is demonstrably necessary and is the only means by which the most serious offences can be prosecuted. Developing AI with surveillance powers to collect and analyse compliant and non-compliant information is an extreme solution and should be subject to the highest scrutiny possible.

35. OVIC queries whether necessity has been established, given that the use of synthetic data to train AI models does not appear to have been explored by the Comprehensive Review. In OVIC's view, the government should fully explore the use of synthetic data and defer to its use to the greatest extent possible in the new electronic surveillance framework. Synthetic data has the potential to offer the most privacy protective option, and its use could save the Government the time and costs that would have been involved in collecting, labelling and securing real-world data.

36. Should the Government decide to permit ASIO to collect and retain real-world data to train an AI for compliance purposes, strong information security practices must be ensured. At an absolute minimum:

    - the personnel with access to the data must be completely independent of investigation and intelligence teams and ideally should be siloed from all other personnel within the agency. This could be achieved through the use of third-party contractors with appropriate clearances engaged exclusively for the purposes of training the AI model; and

    - the data used to train the AI model should be stored completely separately from all other data held by the agency.

**Response to question 18 – Are there any other changes that should be made to the framework for accessing telecommunications data?**

37. As outlined above in response to questions 7 and 8, OVIC's view is that non-content information should be treated the same as content information in the new framework. Telecommunications data should only be accessible under warrant and should be given the same protections from unlawful access as content information.

38. OVIC's concerns about the MDRR are documented in previous submissions to the PJCIS, such as the necessity and proportionality of the regime, the information security concerns posed by the regime,

[41] Discussion paper, 39.
[42] Comprehensive Review, Volume 2, Recommendation 108.

and the overall lack of oversight, accountability and transparency of the regime.[43] These concerns have also been raised by others.[44]

39. The regime itself is out of step with international best practice principles on the integrity of communications and systems, which state that:

> "In order to ensure the integrity, security and privacy of communications systems, and in recognition of the fact that compromising security for State purposes almost always compromises security more generally, States should not compel service providers or hardware or software vendors to build surveillance or monitoring capability into their systems, or to collect or retain particular information purely for State Communications Surveillance purposes. A priori data retention or collection should never be required of service providers."[45]

40. In OVIC's view, the MDRR should not form part of a new electronic surveillance framework in Australia.

**Response to question 19 – What are your views on the proposed thresholds in relation to access to information about a person's location or movements**

41. OVIC disagrees with the assertion in the discussion paper that a person's movements are less private in nature. As set out in response to question 8 above, location data is personal information, and can infer highly sensitive information about a person's life.

42. OVIC also disagrees with the assertion in the discussion paper that location tracking and access to location metadata is the same as a person being "typically observable to others".[46] The long-term monitoring of a person through the use of surveillance tools clearly reveals types of information that are not revealed through the short term monitoring of a person's movements on public streets.[47] Government surveillance of a person's location or movements through access to metadata or the use of a tracking device is more akin to stalking, which is a criminal offence in Australia. As stated by the US District of Columbia Circuit Court:

> "Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story. A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups – and not just one such fact about a person, but all such facts."[48]

**Response to question 22 – Is the proposed additional threshold for group warrants appropriate?**

43. OVIC is concerned about how persons will be determined to form part of a group and the proportionality of the proposed warrant.

44. The discussion paper states that the group will be identified by reference to 'members shared characteristics and group activities'. OVIC would be concerned about a warrant that identified persons based only on shared characteristics. Surveillance must not be applied in a blanket way, or in a manner

[43] CPDP submission 39 to the PJCIS inquiry into the *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (January 2015) https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Data_Retention/Submissions; OVIC's *submission in response to the PJCIS review of the mandatory data retention regime* (July 2019) https://ovic.vic.gov.au/wp-content/uploads/2019/08/OVIC-Submission-to-PJCIS-on-Review-of-the-mandatory-data-retention-regime.pdf.
[44] See PJCIS, *Review of the mandatory data retention regime* (Final Report, October 2020) [2.44].
[45] Necessary & Proportionate, *International Principles on the Application of Human Rights to Communications Surveillance* (2014).
[46] Discussion paper, page 57.
[47] "Short-term monitoring of a person's movements on public streets accords with expectations of privacy but the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy": *United States v. Jones*, 565 U.S., 132 S. Ct. 945, 964 (2012).
[48] *U.S. v. Maynard*, 615 F.3d 544 (U.S., D.C. Circ., C.A.) 562.

that discriminates on the basis of race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

45. OVIC also questions the proportionality of the example use case provided in the discussion paper, which would enable an agency to obtain a group warrant to access the communications of all users of an encrypted messaging platform similar to the AN0M app, "where all users of the platform use it for criminal purposes". In OVIC's view, a group warrant should only be issued where there is a reasonable suspicion of a *common* criminal purpose amongst all members of the group,[49] not criminal purposes generally. The criminal activity should also be sufficiently serious to justify the need for surveillance. OVIC is concerned about the risks of over-collection of information if a group warrant were to enable surveillance of *all* users of a publicly available communications app.

**Response to question 24 – Should magistrates, judges and/or AAT members continue to issue warrants for law enforcement agencies seeking access to this information?**

46. In OVIC's view, the complex judgements of fact and law that are required to be made by an issuing authority and the serious consequences that flow from the misuse of these covert and intrusive powers mean that warrants should only be authorised by a superior court judge, whether sitting on the bench of a superior court or as an AAT member.[50]

47. OVIC further notes that AAT members are appointed for five-year terms, at the discretion of the Government of the day. By contrast, superior court judges are effectively appointed for life, until retirement at age 70. In OVIC's view, this gives superior court judges a greater measure of independence from the Executive, adding further weight to their suitability as an issuing authority.

**Response to question 25 – What are your thoughts on the proposed principles-based, tiered approach to use and disclosure?**

48. At a conceptual level, OVIC supports the proposal to shift to a principles-based approach to use and disclosure of information obtained through surveillance. As a regulator of a principles-based framework, OVIC understands its benefits, in allowing for a degree of flexibility in how privacy is best protected in varying contexts.

49. However, the success of a principles-based framework will depend on the strength of its administering body and the willingness of agencies to comply with the principles. It is imperative that agencies respect and understand the 'why?' behind the limitations placed on the use and disclosure of information, for a principles-based framework to be effective.

50. Comments made by the Comprehensive Review regarding agency culture suggest there is potential for misuse of the principles if there is insufficient education and oversight of the framework and a corresponding improvement in the internal culture within intelligence and law enforcement agencies. For example, the Comprehensive Review cited one intelligence agency who saw legal requirements as a hindrance to data and information sharing, rather than understanding the law's important role in safeguarding and protecting individual rights, and numerous agencies who viewed legal requirements as an administrative burden rather than as necessary in a liberal democracy.[51]

51. Similarly, in Victoria, IBAC's Operation Dawson reported that "some police personnel continue to disregard their obligations around information use" and that "Victoria Police needs to continue to improve employees' understanding of the seriousness of this conduct."[52] Operation Dawson is not the

[49] This view was put forward by the Law Council in its submission to the Parliamentary Joint Committee on Intelligence and Security *Advisory report on the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020*, [4.25]-[4.26].
[50] This is supported by the Parliamentary Joint Committee on Intelligence and Security, *Advisory report on the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020*, recommendation 9.
[51] Comprehensive Review, 34.
[52] IBAC, *Operation Dawson special report,* 16 December 2021, https://www.ibac.vic.gov.au/publications-and-resources/article/operation-dawson-special-report-december-2021.

only investigation by an integrity agency to demonstrate the need for strong education against misuse of information in a law enforcement context.

52. Statutory bodies will need to be tasked with administering the framework at the commonwealth level and state level to cover both commonwealth intelligence and law enforcement agencies and state law enforcement and integrity bodies. These statutory bodies must be able to effectively explain the principles and educate agency's on how to use them in practice. There will also need to be effective oversight of agencies use and disclosure of information in practice, to ensure adherence to the principles. These are significant tasks and will need to be well resourced if the reforms envisaged in the discussion paper are to be effectively introduced and maintained.

53. In OVIC's view, given the sensitivity of the information and the need to retain public trust in the surveillance framework, a principles-based framework must also be supported by prescriptive legislation specifying clear 'no-go' zones for the use and disclosure of surveillance information and offence provisions for unauthorised use and disclosure of information obtained through surveillance.

**Response to question 26 – When should agencies be required to destroy information obtained under a warrant?**

54. In OVIC's view, information obtained under a warrant should be permanently destroyed as soon as reasonably practicable after it is no longer needed for any lawful purpose. This requirement should also be supported by a legislated time limit, after which the information must be destroyed. Legislative time periods for the destruction of data are an important safeguard and control against the indefinite retention of surveillance information.

55. If information is required to be held for the purposes of enabling a regulatory body to perform its oversight functions, and is otherwise no longer required by the agency, the information should be quarantined for access by the oversight body and destroyed once that purpose has been fulfilled.

56. Agencies should be legislatively required to keep auditable records of the destruction process.

**Part 5 – Safeguards and oversight**

**Response to question 33 – Are there any additional reporting or record-keeping requirements agencies should have to improve transparency, accountability and oversight?**

57. OVIC supports the strengthening of reporting and record-keeping requirements as a means of improving public trust in the use of extraordinary powers. Providing meaningful information to the public is an important and necessary component of a strong accountability and oversight framework.

58. In the interests of public trust, OVIC considers that legislative annual reporting requirements should include information about:

    - when and where electronic surveillance information is used – including the specific type of offence being investigated or prosecuted, whether the information was used in evidence in the prosecution, and whether information has also been used in the hearings and reports of agencies;

    - the extent of the use of electronic surveillance powers – including the number of people who have been the subject of electronic surveillance, not just the number and type of warrant issued;

    - the role of the issuing authority – including the number of times an issuing authority has a warrant application granted or rejected, and/or requested further information in support of a warrant application.

- the effectiveness of the use of electronic surveillance powers – including the number of arrests, proceedings and convictions that were based on evidence obtained through the use of electronic surveillance powers, whether or not it was the person the subject of the surveillance that was charged, prosecuted or convicted or someone else, and whether or not the information was used to rule someone out of an investigation;

- the broad types or categories of information obtained through electronic surveillance powers and the methods of access used to obtain the information; and

- the instances where surveillance information has been disclosed to third parties, including the type of third party, the nature of the information and the reasons for its disclosure.

**Part 7 – Interaction with existing and recent legislation and reviews**

**Response to question 37(a) - What data generated by 'Internet of Things' and other devices should or should not be retained by providers?**

59. OVIC queries why the retention of IoT data is being explored, given that the PJCIS recommendation was to amend the TIA Act to clarify that service providers are *not* required to store information generated by IoT devices.[53] The PJCIS specifically noted that "there has been no case put forward by the Government and considered by the Parliament for requiring information generated by Internet of Things devices to be retained… the Committee therefore recommends that such information be excluded from the data retention regime".[54]

60. In OVIC's view it is never justifiable in a democratic society to indiscriminately retain information about the private lives of citizens if no demonstrable need for the information has been established. Even if a justification were put forward, OVIC questions whether the mass intrusion on the privacy of millions of Australians that would be caused by the retention of IoT data would be proportionate to any stated benefits to law enforcement and national security.

Thank you again for the opportunity to make a submission in relation to reforming Australia's electronic surveillance framework. I have no objection to this submission being published without further reference to me. I also propose to publish a copy of this submission on the OVIC website.

If you would like to discuss this submission, please do not hesitate to contact my colleague Emma Stephens, Senior Policy Officer, at Emma.Stephens@ovic.vic.gov.au.

Yours sincerely

Sven Bluemmel
**Information Commissioner**

[53] PJCIS, Review of the Mandatory Data Retention Regime, Recommendation 5.
[54] Parliamentary Joint Committee on Intelligence and Security, *Review of the mandatory data retention regime* (Final Report, October 2020) [5.28].