18 February 2022

Electronic Surveillance Reform Branch
Department of Home Affairs
PO Box 25
Belconnen ACT 2616

Dear Secretary,

Thank you for the opportunity to provide a submission in response to the Department of Home Affairs' discussion paper on the *Reform of Australia's Electronic Surveillance Framework*.

Twitter is committed to working with the Australian Government, law enforcement bodies, our industry partners, academia, non-government organisations, and wider civil society to develop a new framework for electronic surveillance in Australia which enables law enforcement agencies to effectively address the threat of criminal activity and terrorism on the internet, while also protecting freedom of expression, whistle-blowers, and confidential sources.

It is clear that the electronic surveillance framework in Australia needs reform. The current patchwork of laws in this area is overly complex and outdated. Twitter supports the introduction of a new framework which is more streamlined and simplified, which ensures that surveillance intelligence and law enforcement agencies have surveillance powers only where there is a legitimate and demonstrated need and that the exercise of such powers does not unduly encroach upon the legitimate business activities of internet intermediaries and the privacy interests of their users.

We support smart regulation, and our focus is on working with governments to ensure that regulation of the digital industry is practical, effective, and feasible to implement while remaining inclusive and keeping core democratic values intact while promoting tech innovation, including Twitter's core commitment to an Open Internet worldwide.

We trust this written submission will be a useful input to the Department's consultation process. Our written submission also stands together with the joint industry submission from the Digital Industry Group Inc. (DIGI) and the Communications Alliance (Comms Alliance). Working with the broader community we will continue to collaborate to create a safe and secure digital ecosystem.

Thank you again for the opportunity to provide input as part of this important legislative reform process.

Kind regards,

Kara Hinesley
Director of Public Policy
Australia and New Zealand

Kathleen Reen
Senior Director of Public Policy
Asia Pacific

Overview

Twitter appreciates the opportunity to make a submission to the Department of Home Affairs (Department) in response to the *Reform of Australia's electronic surveillance framework* Discussion Paper (Discussion Paper).

Twitter shares the Australian Government's goal of disrupting bad actors and removing illegal content from the Internet. Consistent with the Department's Comprehensive Review, Twitter agrees that the current laws governing electronic surveillance in Australia are complex, inconsistent, outdated and inflexible.[1] Twitter supports the introduction of a modernised and streamlined framework for electronic surveillance that simplifies compliance obligations for internet service providers while also balancing the need to protect principles of free expression and privacy to prevent a chilling effect on robust and open public discourse and avoid unintended consequences.

Any new legal frameworks should be developed bearing in mind the public interest in freedom of expression, freedom of the press, open justice, and the protection of whistle-blowers and confidential sources. These frameworks should also contain appropriate thresholds and robust, effective, and consistent controls and oversight of the use of these intrusive powers by law enforcement agencies.

Key issues and concerns

Twitter's submission will focus on the key issues and concerns raised by the Discussion Paper as they pertain to Twitter operating in Australia, including that:

- Assessment criteria should be established and applied to agencies on an ongoing basis to ensure that the granting of electronic surveillance powers is necessary and proportionate.
- The agencies which are given electronic surveillance powers under the new framework should be set out in the legislation, and the functions for which they are permitted to use those powers should be specified, which will assist industry (including Twitter) in reviewing, interpreting and complying with warrants, access orders, and requests.
- The definition of 'communication' needs to be carefully revised, modernised, and made technology-neutral given that this definition will be used in the prohibitions and offences relating to the unlawful interception of or access to information by electronic means, and subcategories of information falling under the definition of 'communication' should be framed for the purposes of exceptions to those prohibitions.
- A clear and consistent definition of 'serious offence' should be adopted across the new framework and applied as the threshold for when electronic surveillance powers can be used by agencies.
- The new framework should consolidate, simplify, and streamline existing laws, and adopt an outcomes-based framework.
- The new framework should require in the legislation that for all warrant applications, an independent issuing authority must consider necessity and proportionality before authorising access to information (except in emergency situations).
- The new framework should implement the Parliamentary Joint Committee on Intelligence and Security (PJCIS) recommendations for improvement to the mandatory data retention framework and the PJCIS recommendations made in relation to the inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press.[2]
- The Journalist Information Warrant scheme and the role of the Public Interest Advocate should be extended beyond circumstances of professional journalism and should apply to others engaged in legitimate and good faith news breaking activities (including relevant Twitter users).
- Immunity from civil and criminal liability should be provided to communications providers where they act in good faith in responding to legal requests or warrants.
- Reporting requirements for agencies should be strengthened to provide the public and Parliament with more meaningful information to increase accountability and public confidence.

[1] https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/electronic-surveillance-reform
[2] https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/FreedomofthePress

- There is a need for robust and independent oversight of the new framework, and it should be reviewed two years after it comes into effect to ensure it contains appropriate protections for individual rights, remains proportionate to terrorism or national security threats, and is necessary.

We trust this written submission, together with the joint submission from DIGI and Comms Alliance, provides useful inputs for the Department's consideration. We urge and encourage the Department to ensure these issues are addressed in devising its recommendations for the new electronic surveillance framework in Australia.

ACRONYMS AND ABBREVIATIONS USED IN THESE SUBMISSIONS

Term	Meaning
AAT	Administrative Appeals Tribunal
AFP	Australian Federal Police
ASIO	Australian Security Intelligence Organisation
ASIO Act	*Australian Security Intelligence Organisation Act 1979* (Cth)
CLOUD Act	*Clarifying Lawful Overseas Use of Data Act* (US)
Comprehensive Review	Comprehensive Review of the Legal Framework of the National Intelligence Community, Mr Dennis Richardson AC, October 2020
Crimes Act	*Crimes Act 1914* (Cth)
Department	Department of Home Affairs
Discussion Paper	Department of Home Affairs, Reform of Australia's electronic surveillance framework Discussion Paper (2021)
DIGI	Digital Industry Group Inc.
IGIS	Inspector-General of Intelligence and Security
INSLM	Independent National Security Legislation Monitor
IP Act (UK)	*Investigatory Powers Act 2016* (UK)
JIW	Journalist Information Warrant
PJCIS	Parliamentary Joint Committee on Intelligence and Security
Press Freedom Inquiry	Parliamentary Joint Committee on Intelligence and Security, Inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press
Privacy Act	*Privacy Act 1988* (Cth)
SLAID Act	*Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* (Cth)
Surveillance Devices Act	*Surveillance Devices Act 2004* (Cth)
Telecommunications Act	*Telecommunications Act 1997* (Cth)
TIA Act	*Telecommunications (Interception and Access) Act 1979* (Cth)
TOLA Act	*Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth)
UK	United Kingdom

WHO CAN ACCESS INFORMATION UNDER THE NEW FRAMEWORK

Privacy provisions

While there is no clear gap in the existing prohibitions and offences against unlawful access to information and data, the legislative framework would benefit from reform, including to provide adequate privacy protections. At present, the framework consists of a number of legislative instruments which piece together a patchwork of protections, navigating this can become burdensome. Many of the laws are based on outdated concepts which have not kept pace with technological developments and, consequently gaps and loopholes have formed within the existing prohibitions.

A key example of this is s 280(1)(b) of the Telecommunications Act, which provides an exemption to the general prohibition on the use or disclosure of telecommunications information within ss 276, 277 and 278 of the Act and allows the use or disclosure of such information where it is "required or authorised by or under law." Requests under s 280(1)(b) are facilitated by industry obligations under s 313(3) of the Act, which requires service providers to give "such help as is reasonably necessary." Reliance on this exemption is not limited to security intelligence or law enforcement agencies, and we have seen that other bodies and agencies have regularly relied on powers in their own statutes to request information under this exemption.[3] In doing so, the bodies and agencies can avoid the requirement to assess whether disclosure is justifiable and proportionate.[4]

Relatedly, recommendation 15 of the PJCIS in its review of the mandatory data retention scheme recommends that s 280(1)(b) be immediately repealed,[5] as it goes beyond the intention of the Telecommunications Act. As detailed in previous industry submissions, including the statutory review of the Data Retention regime in 2020, s 280(1)(b) in combination with the requirement of s 313(3) of the Telecommunications Act to "give officers and authorities of the Commonwealth and of the States and Territories such help as is reasonably necessary"[6] have led to more than 80 agencies making requests for metadata, over and above the 22 Criminal Law Enforcement Agencies that were originally intended to be the only agencies vested with such powers.[7]

Twitter recommends that the new Act implement thresholds to ensure only a narrowly defined list of law enforcement agencies and ASIO be granted the powers to request access to metadata, and only through one specific legal mechanism.

The Discussion Paper also proposes considerations for determining whether additional agencies should be permitted to access peoples' information and data. The Discussion Paper specifically suggests giving consideration as to whether the "the agency typically deal[s] with the investigation, prevention or enforcement of crimes that merit access to such information."

As noted above, we believe that the recommendation by the PJCIS to limit the number of agencies that have access to metadata to those listed in section 110A of the TIA Act (and also those that have powers to intercept communications) ought to be implemented. If additional agencies must be added to the designated list in the future, we believe that the aforementioned criterion, in and of itself, is not sufficient, as it does not entail any threshold, nor include any form of proportionality test. In our view, there ought to be uniform and clearly defined thresholds for the crimes that warrant access to metadata.

Twitter also considers that the prohibitions and offences relating to the use of surveillance devices, which currently differ in each State and Territory, should be harmonised and made consistent to provide for equivalent privacy protection in each Australian jurisdiction. Twitter does not consider that this would substantially increase the complexity of the reform process.

Otherwise, any new prohibitions and/or offences need to be drafted and implemented in the new framework in terms which are coherent, accessible, and clear.

---

[3] Submission by the Communications Alliance to the PJCIS *Review of the mandatory data retention scheme*, p 4.
[4] Submission by Telstra to the PJCIS *Review of the mandatory data retention scheme*, p 3.
[5] PJCIS *Review of the Mandatory Data Retention Regime* (Final Report, October 2020) at [5.100].
[6] http://www5.austlii.edu.au/au/legis/cth/consol_act/ta1997214/s313.html
[7] https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Dataretentionregime/Report

Where the offences listed in the Discussion Paper are global issues (cyber security of networks, online safety or scam protection/reduction), they largely cannot be addressed under national legislation. To the extent that a cyberattack or online scam is perpetrated by someone within Australia, the existing prohibitions and offences are sufficient to enable these people to be prosecuted under local laws where they are identified. However, where the bad actor is overseas, detection and prosecution may not be possible.

Twitter is of the view that if increased electronic surveillance powers were granted in relation to these other objectives, they may be out of proportion with countervailing privacy interests and other freedoms, and may generate public perception of undue intrusion.

Agencies authorised to access information

Twitter does not have specific comment on additional agencies that should or should not be granted access to electronic surveillance powers, however, we support a strict assessment of the functions and powers of each agency being undertaken prior to granting access, as well as robust oversight mechanisms for all agencies accessing information under the framework. This position is discussed further throughout this submission.

Twitter actively upholds and protects its users' right to privately interact on its platform. Interference with such a right should only occur in the most limited of circumstances and only once an extensive and independent consideration of all the relevant factors has been undertaken. Twitter objects to the grant of any legislative power to an agency which does not, at a minimum, meet designated assessment criteria. To grant power in the absence of such an assessment would risk platforms such as Twitter becoming government instruments of surveillance rather than public platforms designed to promote positive interactions and free communication.

In determining whether to grant electronic surveillance powers to an agency, consideration must be given to the core functions and objectives of the agency. If the agency is capable of performing these objectives and functions in the absence of access to private documents, information, and metadata, the default position should be to deny access. Only in circumstances where the core functions and objectives of an agency cannot be reasonably undertaken without access to such information and data should access be granted.

In addition to this threshold requirement, Twitter submits further assessments should be undertaken to ensure the agency is capable of adequately storing, protecting, and disposing of information received through electronic surveillance. The assessment criteria should include, *inter alia,* whether the collection, use, and disposal of electronic surveillance material:

(a) can be facilitated quickly, efficiently and securely;

(b) can be properly monitored to ensure compliance with legislative requirements; and

(c) is in the public interest, when balanced against the potential consequences should access not be granted.

Page 18 of the Discussion Paper sets out a list of proposed assessment questions to be considered when determining whether additional agencies should have access to particular powers in the new framework. Twitter considers that these assessment questions are appropriate. In relation to the question 'does the agency typically deal with the investigation, prevention or enforcement of crimes that merit access to such information,' Twitter submits that a well-defined and uniform threshold for what crimes warrant access via electronic surveillance would further assist with the efficient and effective application of the legislation. Intruding on an individual's privacy should only occur in circumstances where such intrusion is necessary. As such, Twitter submits only 'serious offences' (as discussed further in response to Questions 6 and 17) should warrant access via electronic surveillance.

Once an agency is deemed to have satisfied the relevant assessments, Twitter considers that the agency should be expressly named within the relevant legislation and the specific functions of the agency for which electronic surveillance powers may be used should be expressly stated in the legislation. Twitter

submits that the disclosure of this information in legislation is important for maintaining agency accountability, providing clarity for industry, and increasing public trust and transparency. Twitter notes the widespread support for such an approach in the Comprehensive Review.[8] In particular, setting out the agencies' functions in legislation is of particular relevance where it serves a legislative purpose, that is, there are particular rights, immunities, or restrictions which attach to the particular functions.

Such transparency would assist service providers like Twitter in complying with warrants, access orders, and legal requests. At present, service providers are required to undertake their own analysis of each request for information in order to determine whether or not an agency is empowered to access electronic surveillance material. Not only is this process draining on resources for service providers, but it also has the potential to lead to erroneous legislative interpretation and subsequently increase the possibility of material being mishandled.

Information accessed

Twitter considers that it is fundamental that the term 'communication' is carefully defined and modernised for the new framework, given that this is the term that will be used in the prohibitions and offences relating to the unlawful interception of or access to information by electronic means. The definition should be sufficiently broad and technology-neutral to capture all information and data transmitted electronically that needs to be protected under the new framework.

The definition of 'communication' should make clear that it captures the categories of information set out on page 22 of the Discussion Paper, including technical information "such as machine-to-machine signalling".[9] Twitter considers that the broad definition of 'communication' should be modelled on either the United Kingdom's definition of 'communication' in s 261(2) of the IP Act (UK) or New Zealand's definition of 'communication' in s 47 of the *Intelligence and Security Act 2017* (NZ).

However, Twitter considers that agencies should not necessarily be able to access all categories of information falling within the definition of 'communication.' The types of information which agencies should be permitted to access under a warrant or authorisation should be limited to the information that is necessary to enable the agencies to perform their functions.

Twitter therefore submits that the concept of 'protection' of information included in the definition of 'communication' should be decoupled from the concept of 'access' to that information. Under this approach, a broader definition of 'communication' would be appropriate for use in relation to prohibitions and offences on the basis that proportionality would be embedded at the access stage by reference to subcategories of information that can be obtained by agencies via electronic surveillance on a case-by-case basis.

Twitter considers that these subcategories of information could be modelled on the subcategories articulated in s 261 of the IP Act (UK). These would include communications data, entity data, and events data. At the access stage, the new framework would then specify the thresholds that agencies would need to meet to obtain each subcategory of information, with higher thresholds imposed for more intrusive types of data. This approach is consistent with the findings of the Comprehensive Review.[10]

Twitter considers that only targeted surveillance and interception, rather than bulk or mass collection, should be permitted within the new framework. If "all of the kinds of information that pass over the network" were amenable to access by agencies, the volume of additional material and the systems required by industry to make it available to agencies would be astronomical and have significant implications for user privacy.[11] Such a result would unduly burden industry in circumstances where there is no identifiable utilitarian value supporting this burden or intrusion, and impede the ability of agencies to process and comprehend the information obtained.

[8] See Comprehensive Review, Volume 1, from [13.55].
[9] Comprehensive Review, Volume 2 at [29.15].
[10] Comprehensive Review, Volume 2 at [29.19].
[11] As referred to in Comprehensive Review, Volume 2 at [29.16].

Clarifying key terms

Twitter submits that the definition of 'serious offence' should be tightened to reflect the considerable expansion of electronic surveillance powers available to agencies in recent years. Twitter considers that an appropriate definition of 'serious offence' would be:

(d) an offence punishable by a maximum penalty of at least 7 years' imprisonment; or

(e) other specified offences which cannot be effectively investigated without covert access to communications content and which are punishable by a maximum penalty of at least 3 years' imprisonment.[12] Such offences should be expressly set out in the legislation.

Twitter notes that this definition is consistent with Recommendation 12 of the PJCIS in its recent report on the SLAID Act.[13]

Twitter also supports the proposal by the Law Council of Australia in its submission to the PJCIS that the offences falling within the definition of 'serious offence' should be limited to certain subject matter, including offences against the security of the Commonwealth; offences against humanity (including child exploitation and human trafficking); serious drug, weapons and criminal association offences; and certain money laundering and cybercrime offences.[14]

Twitter submits that the definition of 'serious offence' should be applied consistently across the new framework.

Twitter considers that broad terms such as 'national security' may be inappropriate for use in justifying the exercise of electronic surveillance powers because they are vague and opaque. Twitter submits that there is a need for a more granular and explicit definition of 'national security' in the new framework in order for it to be relied on by agencies as a legitimate purpose for intercepting or accessing data. It is submitted that it may be suitable for the content of this definition to be determined in public debate, and set out in clear guidance, rather than being purely for the executive to determine.

Addressing emerging technologies

Twitter adopts the position set out in the Comprehensive Review, namely that it is currently "premature to [meaningfully] legislate to control the use of artificial intelligence for intelligence purposes" as "these capabilities are in their infancy."[15]

Research is currently being undertaken regarding concerns about the impact that quantum computing may have in the near future on the reliability of conventional encryption algorithms that protect information and on privacy more generally.[16] Twitter believes that recommendation and ranking algorithms should be subject to human choice and control. In the long term, as we envision through our @bluesky project, this control will extend to the choice between ranking algorithms built on an open standard for social media.[17]

The idea of “Protocols not platforms” is instructive not only for the technological potential for standardisation of ranking algorithms but also the underlying impact this would have on protecting free expression and driving competition.[18]

Accordingly, Twitter considers that the scheme should embed a requirement for a mandatory review of the operation of the new framework to be undertaken within two years after it comes into force. The

[12] Comprehensive Review, Volume 2, Recommendation 89.
[13] PJCIS, *Advisory report on the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* (August 2021) at [6.71].
[14] Ibid at [2.42].
[15] See Comprehensive Review, Volume 1 at [3.96]
[16] See, for example, A Question of Trust, Report of the Investigatory Powers Review (June 2015) by David Anderson QC, Independent Reviewer of Terrorism Legislation at [4.56]
[17] https://blueskyweb.org/
[18] knightcolumbia.org/content/protocols-not-platforms-a-technological-approach-to-free-speech

review should consider the impact of emerging technologies on privacy and information protection, and the continuing ability of the framework to deliver on its policy objectives.

Defining communication, content, and non-content information

The definition of 'communication' to be applied in the new framework needs to be settled prior to considering the definition of 'content' and 'non-content' information and whether there should continue to be any distinction between the two categories of information.

The distinction between content and non-content material derived from a perception, at the time of enactment of the mandatory data retention scheme, that accessing and intercepting content material was a greater invasion into the privacy of the individual than non-content information.[19] The Discussion Paper states that:

(a) 'content' information is the substance or meaning of a communication. For example, words spoken during a telephone conversation or the contents of an email;

(b) 'non-content' information is information about the form, time and location in which a communication occurred. For example, the time a telephone call was placed, the duration of the call, the participants, and where each participant was calling from.[20]

While seemingly innocuous, the distinction is important under the current legislative framework in that it provides that content information can only be accessed and intercepted under an interception or stored communications warrant, or in other limited circumstances (including, but not limited to, a life threatening emergency). Conversely, non-content information can be obtained by various agencies by way of an internal authorisation where it is arguable that the information is necessary to an investigation.

Twitter submits that proper consideration should be given to whether or not it is appropriate to continue to separately define content and non-content information once the definition of 'communication' and the subcategories of information falling within that definition are settled. It may be that the distinction is no longer relevant depending on how the subcategories of information are framed.

By way of illustration, Twitter is of the view that certain information which is currently treated as 'non-content' information is as much an integral part of a communication as its 'content'. The current definitions of content and non-content information are less applicable to the types of communications facilitated by a service such as Twitter than to a traditional telecommunications provider. Digital messaging forms a part of Twitter's service. Information about the sender and recipient of a message, as well as the time and location, forms a fundamental part of the whole communication. Unlike telephone conversations, where such data is easily severable from the substance of the words spoken, time, location, sender and recipient data forms a part of a digital message and by extension, a digital footprint. Twitter submits that such information should, for the purpose of the legislation, be considered a formative part of the whole communication. It follows from this that Twitter's view is that access to both content and non-content information should require a warrant rather than an internal authorisation.

The categorisation of location information as content, rather than non-content information, is broadly reflective of the jurisprudence in the USA, where the US Supreme Court ruled that access to historical location data from a cellular device should generally only be granted pursuant to a warrant.[21] Twitter considers the majority decision of the US Supreme Court to be an appropriate acknowledgement of the sensitive nature of location data. This is particularly so in circumstances where location data coupled with other relevant information provides meaning as to part or all of a communication. We discuss location information further in response to Question 19.

The distinction between live communications and stored communications in the current framework is reflective of the user trends and habits at the time the legislation was enacted. At present, and looking toward future user behaviour, such a distinction is no longer relevant or reflective of how users of electronic communication services interact, communicate, or create data.

---

[19] Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (Cth), p 9-10
[20] Discussion Paper, p 23
[21] *Carpenter v. United States*, 138 S. Ct. 2206 (2018)

The current distinction was based on the assumption that stored communications would be more considered, by virtue of their seemingly more permanent nature, whereas live communications were viewed as more spontaneous. While these statements in isolation are seemingly true, the nexus between the spontaneity of a live communication and a greater emphasis on limiting access to that form of communication is not established. Further, in the modern era of technology, instant messaging on various platforms is the dominant form of communication. As such, the need to distinguish between live and stored communications is now, in many ways, obsolete.

Further, in circumstances where a communication can be both live while in transit and then stored, the distinction creates legislative ambiguity. This arises for most digital communications. For example, while an instant message is being uploaded, it may be considered 'live'. However, once that message is completely uploaded onto a platform, it transitions from a 'live' communication to a 'stored' communication. The content of the communication has not changed in the process. Nor has the relevant metadata, being the sender, recipient, location, or time. The differing definitions in these circumstances are reflective of outdated concepts of how communications are sent and received.

Finally, in relation to stored communications, there is a greater risk that the information will contain communications or records associated with third parties, who are not the intended subject of the investigation.

For these reasons, the distinction between live communications and stored communications should not be maintained in the new framework. Although, we would also highlight the extraterritoriality considerations for service providers, like Twitter, that manage stored data across different regions. Given the distinction between live communications and stored communications remains in US law, there may be legal obligations that dictate under what circumstances stored data may be disclosed to another government.

Obligations for communications providers

Twitter does not wish to comment specifically on which communications providers should be obligated to retain, protect, and produce information under the new framework.

It is incumbent on the agencies seeking such information to justify what types of information they require access to in order to carry out their functions and to identify the communications providers which can best provide such access. As stated in the Discussion Paper, any change introduced under the new framework should avoid placing unnecessary additional burdens on industry and extra-territorial implications will need to be considered and accommodated.

Twitter notes that if there is any proposal to increase the obligations on communications providers under the new framework, it requests an opportunity to comment on each specific proposal once further details are provided.

An outcomes-based framework

Twitter is of the view that the new framework should primarily focus on the regulation of electronic surveillance by reference to the type of information sought to be accessed, as opposed to the means of access (i.e. the specific type of surveillance device being used).

In particular, Twitter considers the current threshold distinction between tracking devices and optical devices, listening devices and data surveillance devices does not adequately protect the significance of the information obtainable from a tracking device. As such, Twitter submits location-based information should only be accessible pursuant to a warrant, which is explored in further detail throughout this submission.

While Twitter considers that the new framework should focus on the outcome of what information is sought to be obtained by an agency via electronic surveillance, the framework should still require that the method of access be disclosed and justified in terms of its privacy impact (including an assessment of

whether the proposed method of access is the least intrusive means available that would be effective in the circumstances). Further discussion on this issue is contained below.

HOW CAN INFORMATION BE ACCESSED?

Warrant frameworks

The current legislative framework consists of nine Acts which set out the functions, powers, immunities, administrative arrangements, and oversight of national security intelligence and law enforcement agencies in Australia.[22] Further legislation of more general application also applies.[23] This is in contrast to comparable jurisdictions overseas, such as New Zealand which has a single Act[24] and the UK which is regulated by four Acts.[25]

As stated in the Discussion Paper, the 10 agencies which make up the National Intelligence Community may currently obtain information under more than 35 different warrants and authorisations, many of which overlap in the types of information that can be accessed and their impact on the privacy of individuals. The complexity of, and inconsistencies between, current laws gives rise to uncertainty in interpretation and makes compliance by companies, such as Twitter, more challenging, particularly in relation to extraterritorial application.

Twitter considers that the current warrant framework should be simplified by the adoption of a common legislative framework, which would consolidate, simplify, and streamline the legislation currently in effect. The new warrant framework should apply consistently across all agencies which are granted electronic surveillance powers, with flexibility provided based on the function being exercised by the agency, and a a common mechanism of scrutiny for how powers are exercised.

With regards to warrants, the Discussion Paper proposes that requesting agencies would need to justify that the method of access proposed is necessary and proportionate and/or the least intrusive with respect to the privacy of the individuals involved.

Twitter agrees with a proportionality test that takes into consideration necessary privacy concerns; however, the current proposal remains significantly flawed as currently drafted. As proposed in the Discussion Paper, it appears that this regime would apply only to the warrants that currently exist and to warrants that will be required for new categories of communications that are proposed to fall under the proposed definition of 'content.'

We noted our concern with the definition of 'communication,' the distinction between 'content' and 'non-content,' and the principle that all metadata would always be considered non-content information (see page 10), which would be available under authorisation and not be subject to the criteria mentioned above regarding necessity, proportionality and intrusiveness with respect to privacy.

The proposed regime for warrants would lead to a focus on only some categories of content information while leaving large areas of metadata subject to authorisation. This approach would likely lead to an increase in the use of large-scale surveillance by means of metadata analysis, given the substantially lower justification that needs to be met. Such data, especially when used in aggregation, would prove a very powerful surveillance tool without adequate safeguards or oversight.

Thus, we recommend the proposed approach be reconsidered and a common set of principles apply across all types of information and agencies to ensure that the most intrusive forms of information will be appropriately protected in a future surveillance framework. Further, the regime should require relevant law

---

[22] *Australian Crime Commission Act 2002* (Cth), *Australian Federal Police Act 1979* (Cth), *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth), *Australian Security Intelligence Organisation Act 1979* (Cth), *Inspector-General of Intelligence and Security Act 1986* (Cth), *Intelligence Services Act 2001* (Cth), *Office of National Intelligence Act 2018* (Cth), *Surveillance Devices Act 2004* (Cth) and *Telecommunications (Interception and Access) Act 1979* (Cth)

[23] *Australian Border Force Act 2015* (Cth), *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth), *Crimes Act 1914* (Cth), *Criminal Code Act 1995* (Cth), *Public Interest Disclosure Act 2013* (Cth), *Archives Act 1983* (Cth), *Privacy Act 1988* (Cth), *Freedom of Information Act 1982* (Cth) and *Public Governance and Performance and Accountability Act 2015* (Cth)

[24] *Intelligence and Security Act 2017* (NZ)

[25] *Security Service Act 1989* (UK), *Intelligence Services Act 1994* (UK), *Investigatory Powers Act 2016* (UK) and *Regulation of Investigatory Powers Act 2000* (UK)

enforcement agencies and ASIO to obtain a warrant in circumstances in which there is a dispute as to whether data is appropriately classified as content, as opposed to non-content. The regime should also include a mechanism to ensure and enforce rules against unlawful use of data for political or public communication, to obtain privileged information, identify a journalist source, or a whistle-blower and provide a mechanism that applies across the system to protect privileged information and the source of information provided to journalists and protect whistle-blowers.

Twitter agrees that an outcomes-based framework (focused on subject or data type), rather than a method-based framework (focused on the means of access to data), is more appropriate and better adapted to electronic means of communication and ongoing technological advancements.

The common legislative framework should:

- Be technology-neutral;
- Adopt consistent treatment of common activities, processes and systems where the same policy outcome is intended;
- Consistently use common concepts where the same meaning is intended;
- Ensure that differences in approaches are principled and as a result of policy design;
- Reduce or eliminate unnecessary duplication;
- Remove unnecessary prescriptiveness;
- Use modern, reader-friendly drafting techniques to improve the readability of the legislation;
- Specify in legislation the objectives and guiding principles of each of the agencies comprising the National Intelligence Community for the purposes of enhancing transparency and public confidence;
- Specify in legislation the powers that can be exercised under warrant, including general descriptions of the ways agencies access information;
- Require agencies to specify the type and volume of information sought to be accessed by a warrant;
- Require agencies to specify the particular technical methods proposed to access the information the subject of the warrant, including whether assistance is required from a communications provider;
- Require agencies to assess the privacy impact of a warrant on a case-by-case basis by satisfying the issuing authority that the proposed methods of access are the least intrusive means available that would be effective in the circumstances;
- Adopt consistent thresholds, safeguards and oversight mechanisms for the issue of warrants and the exercise of emergency authorisations, including by strengthening authorisation requirements for all warrant applications to explicitly require an issuing authority to consider necessity and proportionality before authorising access to information or data;
- Prohibit unlawful access to, use and disclosure of information via electronic surveillance and provide for strong disincentives, including robust enforcement powers and penalties for breach;
- Provide for additional safeguards and protections against access to privileged information, information that may identify a journalist's source or information that may identify a whistle-blower; and
- Provide for a common reporting regime which ensures that warrants are reported annually both in terms of numbers, the offences for which they were common, whether or not information was relevant to the prosecution of those offences, how many prosecutions were commenced and how many prosecutions resulted in a conviction.

In light of its commitment to transparency, Twitter submits that the new framework should enable communication providers to report basic, de-identified information regarding the information they have provided to agencies under warrants, the threshold required to be met before that information was made available and its intended uses.

Twitter requests the opportunity to make further submissions to the Department as more specific proposals and recommendations are developed regarding the proposed new system and how it will operate in practice.

WHEN WILL INFORMATION BE ACCESSED?

Legislative thresholds

Warrant provisions specify a particular threshold which must be met before the relevant power can be used and generally require the issuing authority to reach a particular level of satisfaction in respect of specified matters. These thresholds differ depending on the type of warrant.

Twitter supports the harmonisation of legislative thresholds for electronic surveillance by agencies where existing warrants are determined to be functionally equivalent. Twitter agrees that having a streamlined set of provisions relating to warrants (including the test for issuing the warrant) is likely to reduce the length and complexity of those provisions, improve the ability of agencies to use and comply with the provisions, enhance cooperation and collaboration among agencies operating under similar frameworks, reduce compliance costs and improve certainty for and responsiveness by communications providers.

In particular, Twitter agrees that consistent thresholds should be adopted for:

- The use of ASIO's powers to intercept telecommunications, access stored communications, access computers, and use optical and listening devices. The higher threshold (which presently applies to computer access warrants) that the exercise of powers would 'substantially assist' in obtaining intelligence in relation to a matter that is important in relation to security should apply to all methods of access.
- The use by law enforcement agencies of these powers. The threshold should be that the exercise of powers would 'substantially assist' the investigation of a 'serious offence' (the definition of which is discussed in response to Question 6).

As stated above, Twitter considers that an outcome-based framework (focused on subject or data type), rather than a method-based framework (focused on the means of access to data), is appropriate and better adapted to electronic means of communication and ongoing technological advancements.

However, Twitter is of the firm view that the method of access must remain a key aspect of the legislative thresholds which are imposed, by requiring agencies seeking authorisation of a warrant to:

- specify the particular technical methods which will be used to access information the subject of the warrant; and
- provide an assessment of the privacy impact of a warrant on a case-by-case basis by satisfying the issuing authority that the proposed methods of access are the least intrusive means available that would be effective in the circumstances.

Twitter also supports the strengthening of authorisation requirements for all warrant applications to explicitly require an issuing authority to consider necessity and proportionality before authorising access to information or data. Although the Comprehensive Review recommended that the new legislation should not include standalone proportionality tests as part of the threshold for the authorisation of intrusive powers, Twitter considers that including such tests within the legislation for the new framework will provide certainty for communication providers and will increase public confidence in agencies.[26]

Mandatory data retention scheme

The PJCIS published its report in respect of its review of the mandatory data retention scheme under the TIA Act in October 2020.[27] The inquiry currently has no Government response. Despite this, the Discussion Paper states that the new framework will implement the Government's response to the review.

A delay of more than 15 months in the Government's response to this review is unreasonable, particularly in circumstances where the PJCIS has made certain recommendations to implement changes within 18 months of the report, including that the Department should prepare national guidelines on the mandatory

[26] Comprehensive Review, Volume 2, Recommendation 29
[27] PJCIS, *Review of the Mandatory Data Retention Regime* (Final Report, October 2020)

data retention scheme. The PJCIS was of the view that the mandatory data retention scheme requires changes to improve certainty, transparency, and privacy protections, and it would be detrimental to allow the PJCIS report to lapse with the upcoming Australian Federal Election in 2022.

Twitter is aligned with the view that the new framework should implement the PJCIS' recommendations for improvement to the mandatory data retention framework. In particular:

- the mandatory data retention scheme should be amended and its requirements clarified to provide greater certainty and enhance privacy protections;
- concerns surrounding access to telecommunications data outside of the mandatory data retention scheme should be addressed, including by:
    - imposing legislative requirements that the agency must not use information not caught by the scheme (including the contents or substance of a communication or web browsing history), must immediately quarantine the information, must notify the Commonwealth Ombudsman or IGIS (as applicable) of the disclosure and, following consultation, must destroy the information; and
    - specifying in the legislation that agencies can only access telecommunications data through Part 4-1 of the TIA Act and through no other legal mechanism;
- measures should be introduced to increase transparency, including additional reporting and record-keeping requirements for agencies;
- 'authorised officers' who can authorise an agency's access to telecommunications data must be sufficiently senior and must have the requisite experience, knowledge and skills to exercise the powers under Chapter 4 of the TIA Act;
- the 'serious offence' threshold referred to in response to Question 17 above should be adopted before access to telecommunications data can be authorised;
- the thresholds for authorising access to telecommunications data should be increased to be consistent with the threshold for agencies to intercept telecommunications or access stored communications, and a proportionality assessment should be undertaken which considers the impact on privacy before an authorisation is made; and
- only agencies specifically listed in the legislation should be permitted to authorise the disclosure of telecommunications data.

The Government's response to the PJCIS' Press Freedom Inquiry should also be adopted, including by strengthening the safeguards that apply when agencies seek telecommunications data in relation to a journalist or media organisation (as discussed further in response to Question 24).[28]

The Journalist Information Warrant scheme and the role of the Public Interest Advocate currently applies only in circumstances of professional journalism due to the narrow definition of a "source" in the TIA Act as a person who provides information to another person "who is working in a professional capacity as a journalist."[29] Twitter submits these safeguards should be extended to others who engage in legitimate and good faith news breaking activity who are not employed as professional journalists,[30] including relevant Twitter users. Twitter is frequently used as a platform on which to break news, with millions of people worldwide relying on Twitter as their source of news; thus, additional protections are required.

Twitter is also concerned about the implications of the assistance orders introduced into the Crimes Act and the Surveillance Devices Act by the SLAID Act last year.[31] An agency may apply for an assistance order where it requires a 'specified person' to provide information or assistance such as to enable them to take control of an account or access data held in a computer, and failure to comply is an offence. It is possible that employees of electronic services, such as Twitter, could be charged with an offence for

[28] PJCIS, *Inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press* (August 2020)
[29] TIA Act, s 5 (definition of source)
[30] Rebecca Ananian-Welsh, 'Journalistic Confidentiality in an Age of Data Surveillance' (2019) 41(2) *Australian Journalism Review* 225 at 235
[31] Crimes Act, s 3ZZGVG and Surveillance Devices Act, s 64A

failing to comply with an assistance order, even where compliance would directly conflict with obligations under international laws or where compliance is not technically feasible.[32]

Twitter notes that the PJCIS recommended that amendments be made before the SLAID Act was passed to require the issuing authority to be satisfied that compliance with the request is practicable and technically feasible,[33] and to introduce good faith immunity provisions for assisting entities and their employees or officers who are acting in good faith with an assistance order;[34] however that did not occur. [35] This is despite the fact that these additional safeguards are found in the industry assistance measures introduced into the Telecommunications Act by the TOLA Act.[36] The Telecommunications Act also requires that agencies consult with communications providers before issuing assistance notices, which is not a requirement under either the Crimes Act or the Surveillance Devices Act. Despite the provisions of the TOLA Act containing more robust protections than the SLAID Act, the INSLM found that the TOLA Act is not "proportionate," nor appropriately protective of human rights.[37] To date, the Government has not yet responded to the INSLM's review and recommendations.

Locational data and information

Twitter considers that it is appropriate that tracking devices should be subject to the same thresholds that apply to optical devices, listening devices, and data surveillance devices. Even though tracking devices do not provide access to the content of communications, the fact that they may reveal a person's pattern of movement and associations is significant.

The conclusion in the Comprehensive Review, which is adopted in the Discussion Paper, states that tracking information may have less impact on privacy than other surveillance information, which is in stark contrast to other recent Commonwealth reports. The final report of the Digital Platforms Inquiry published by the Australian Competition and Consumer Commission (ACCC) on 26 July 2019 recommended that technical data, including location data, should be regulated in the Privacy Act, reflecting concerns about gaps in the coverage of the Privacy Act in light of how data is collected across the digital economy.[38]

The Privacy Act Review Discussion Paper published in October 2021 also contains a proposal to amend the Privacy Act to include a non-exhaustive list of the types of information that could be capable of falling within the definition of "personal information", including location data. [39] In its submission, the Office of the Australian Information Commissioner pointed out the intrusive nature of location information, noting that it can reveal other sensitive attributes such as information about health or religious beliefs.[40]

For these reasons, Twitter submits that it is not appropriate that location-based information should continue to be accessible by agencies without a warrant, and considers that the new framework should provide for an independent issuing authority to authorise the use of tracking devices, as discussed further in response to Question 24.

Warrant authorisation frameworks

Twitter agrees that electronic surveillance powers should be directed to the person who is the subject of the investigation at first instance, so as to minimise the privacy impact on third parties unrelated to the investigation. Twitter acknowledges that this may need to be subject to limited exceptions, including

---

[32] See also Twitter's submissions in response to the PJCIS *Review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* (12 February 2021). Available at <https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/IdentifyandDisruptBill/Submissions>.
[33] Recommendation 20, PJCIS *Advisory Report on the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* (August 2021)
[34] Recommendation 24, Ibid
[35] Supplementary Explanatory Memorandum to the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2021*
[36] Telecommunications Act, Part 15
[37] Independent National Security Legislation Monitor, *TRUST BUT VERIFY: A report concerning the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 and related matters*, (30 June 2020)
[38] Digital Platforms Inquiry Report, Part 1, Recommendation 16(a), p 34
[39] Privacy Act Review Discussion Paper, Recommendation 2.1, p 27
[40] Submission by the Office of the Australian Information Commissioner, *Privacy Act Review – Issues Paper*, at [3.24]

where a suspect has not yet been identified, in which case an object or premises-based warrant may be appropriate.

As stated in its submissions to the PJCIS at the time, Twitter remains concerned about the recent powers introduced by the SLAID Act, namely data disruption warrants, network activity warrants and account takeover warrants[41]. When incorporating these powers into the new framework, Twitter urges the Department to reconsider the impact of these powers on communications providers. In particular, Twitter submits that communications providers should be consulted on the form and detail of a warrant before it is issued, to allow the communications provider to suggest any changes that might reasonably be necessary to support the implementation of the warrant and to ensure that the privacy interests of third parties who are not the subject of an investigation are protected.[42] Further, law enforcement "hacking" or other manipulation of a service in order to obtain access may threaten the security of other users of that service by identifying and exploiting a vulnerability in the security of the service, which may then be exploited by bad actors.

Twitter places an extremely high importance on the privacy of its user's information, data and communications. We therefore agree that additional thresholds must be met before agencies can obtain third party warrants.

Twitter considers it appropriate that agencies be required to satisfy the issuing authority that, in addition to the test for an ordinary warrant, obtaining information directly from the person the subject of the investigation would be impractical or ineffective. The threshold for third party warrants in the new framework should require that privacy concerns be taken into account in assessing whether the warrant is necessary for investigating criminal or security-related conduct.

Twitter considers that group warrants should only be available in limited circumstances, and where a higher legislative threshold is applied to ensure proportionality is considered in applying for and issuing such warrants. Twitter agrees that the issuing authority should be satisfied that individual warrants would be impractical or ineffective, such as in cases where the identities of all group members are unknown.

The Department states that where an agency requires a service provider's assistance to execute the warrant (such as to intercept communications), the agency will be required to identify the services, devices or communications that should be accessed, so that providers are able to action the request. As stated above in response to Question 20, Twitter submits that the new framework should require agencies to consult with service providers on the form and detail of a warrant, including a group warrant, before it is issued. Twitter considers that such co-operation will improve the efficacy and implementation of the warrant and ensure that the privacy interests of third parties who are not the subject of an investigation are better protected. This is particularly so in relation to the powers introduced under the SLAID Act.

Proportionality tests

Twitter agrees that the use of electronic surveillance powers should only be authorised when they are necessary and proportionate, in that the use is for a legitimate and lawful objective and the intrusion on privacy and other rights does not outweigh the benefits of that objective. Twitter is therefore supportive of the recommendation in the Comprehensive Review that the new framework should introduce a more consistent and explicit necessity and proportionality test.[43]

Twitter considers that the tests for necessity and proportionality should be set out in the legislation establishing the new electronic surveillance framework, including requirements for agencies to specify in a warrant, and for the issuing authority to consider, matters such as the impact on privacy, the gravity of the threat of the offence, allegations and the availability of other investigative methods. Such information should be available to the recipient of a warrant to enable them to assess whether the scope of the warrant is within power and not overbroad.

---

[41] Available at https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/IdentifyandDisruptBill/Submissions

[42] See also the submissions by the Communications Alliance, DIGI and Telstra, which are available at the same link

[43] Comprehensive Review, Volume 2, Recommendation 80

The inclusion of these tests should be in the legislation itself, as opposed to agency guidelines, also increases the accountability of agencies in applying for warrants. Guidelines may also vary between agencies, and the thresholds may therefore be interpreted and applied differently, leading to inconsistency and uncertainty.

It is important that the proposed new regime has absolute clarity regarding the evaluation and appropriateness for the issue of electronic surveillance powers in each instance. Twitter agrees with the list of factors set out on page 52 of the Discussion Paper, and considers that these should be expressly stated in the legislation, namely:

- the gravity of the matter under investigation – is the crime or security matter, and the resulting likely harm, serious enough to justify the use of the power;
- the intrusion on privacy – how much will the use of the power intrude on the privacy of the target or any other person;
- the likelihood the surveillance will achieve the warrant objective – will the use of the power actually provide the information that the agency is seeking;
- the likely relevance and usefulness of the information – is the information likely to further the agency's investigation, including preventing further criminal activity or threats to security;
- whether there are less intrusive means of achieving the purpose of the warrant – could the agency use some other less intrusive power to obtain the information it is seeking; and
- what other intrusive powers have been, or are being, used in relation to the target.

Twitter would add to this list that, where assistance is required by the agency from a communications provider, consideration of whether the agency has engaged with the communications provider regarding the scope of the warrant.

Further, Twitter submits that the legislation should require that a record is made and retained by an issuing authority of each assessment of necessity and proportionality according to these factors. Any practical guidance which is given by the Department to assist in applying these tests should be consistent across all agencies.

Warrant issuing authorities

It seems incongruous to Twitter that, under the current electronic surveillance framework, some information can be accessed following internal authorisation by an agency (such as location-based information using tracking devices), ASIO warrants are issued by the Attorney-General, some warrants may be authorised by magistrates (such as stored communications warrants and account takeover warrants) and other warrants must be authorised by nominated federal judges and senior AAT members.

Given the intrusive nature of electronic surveillance powers, subject to the exceptions stated below, Twitter considers that there should be an additional approval by an independent issuing authority for all warrants and authorisations under the new framework. The issuing authority should be independent of the Executive. The Comprehensive Review records significant support for the adoption of a 'double lock' system, including its adoption in comparable jurisdictions overseas which provide for independent bodies to play a part in the authorisation process for at least some if not all powers, despite the fact that it was ultimately not recommended for the new framework (but was also not ruled out).[44]

Twitter supports the Department's commitment to ensuring that, under the new framework, only appropriately senior independent officers can issue warrants for access to journalists' and media organisations' data. In this regard, Twitter refers to the findings of the PJCIS[45] that "powers such as these need careful consideration by a senior lawyer or judicial officer, especially when they potentially affect the free operation of the media" and the recommendation that all warrants related to a person working in a professional capacity as a journalist or media organisation should be issued by a judge of a superior court of record or the Federal Court.

[44] See Comprehensive Review at [3.105]-[3.109] and [18.64]-[18.115]
[45] PJCIS *Inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press* (August 2020) at [3.129] and [3.139] (Recommendation 2) and the Government Response

Twitter submits that this position should extend to where a warrant or authorisation relates to information held by whistle-blowers and communications providers (including carriage service providers and social media providers), given such warrants may therefore have implications for freedom of expression and freedom of political communication. Twitter considers this is particularly so in relation to account takeover warrants introduced by the SLAID Act, which can currently be approved by magistrates, despite the fact that they enable agencies to gain access to a user's account via "hacking" or otherwise manipulating the service unilaterally without notice to the service provider. The PJCIS also recommended in its report on the SLAID Bill that some powers should only be authorised by a Federal Court judge or a state or territory Supreme Court judge.[46]

Twitter notes that this approach would be consistent with the requirements for Australian agencies to obtain orders for electronic data held by carriage service provided in the United States under the CLOUD Act, given Australia's agreement with the US that orders must be authorised by a court, judge, magistrate or other independent authority. The same requirements should apply for agencies to issue warrants in respect of Australian-based communications providers.

Twitter acknowledges that there may need to be some exceptions to these approval requirements, such as in emergency situations (discussed further in relation to Question 27 below) and in relation to ASIO (in which case, Twitter supports the recommendations by the Comprehensive Review[47] as to new legislative provisions relating to the Attorney-General's power to issue warrants for ASIO).

Twitter also supports the Department's commitment to expand the role of Public Interest Advocates beyond journalists' telecommunications data to apply also to warrants in relation to the investigation of an unauthorised disclosure of government information or a Commonwealth secrecy offence where the warrant relates to a person working in a professional capacity as a journalist or a media organisation. Twitter submits that consideration should also be given to providing for a role for Public Interest Advocates in respect of whistle-blowers and others engaged in legitimate news breaking activity who are not working as professional journalists.

Twitter considers that information obtained by lawful electronic surveillance for law enforcement or security purposes should be used and disclosed only for the purposes for which was sought and obtained – to investigate threats to security and serious offences. Twitter recognises that a tiered approach may be required, so long as the permitted purposes are specified in the legislation and are appropriately confined to ensure there is not a disproportionate impact on a person's privacy and reputation and to ensure public trust is not undermined.

There should be clear offences and penalties associated with the use or disclosure of information for a purpose other than a permitted purpose. Twitter is supportive of the consolidation and simplification of secrecy offences so that they are clear, effective and consistent across all types of warrants.

Independent supervisory agencies, namely the IGIS and the Commonwealth Ombudsman, should have oversight over the use of electronic surveillance powers by agencies and should be required to audit and verify the integrity of evidence gathering activities in compliance with the new framework.

Destruction of information

Twitter considers that agencies should be required to destroy records of information obtained by conducting electronic surveillance where:

- that information is obtained without having obtained a required warrant or authorisation;
- the information is obtained by conducting electronic surveillance activities beyond those authorised by a warrant or authorisation;
- the information obtained falls outside the scope of what is permitted to be accessed under a warrant or authorisation in accordance with the legislation (for example, where additional

[46] PJCIS *Advisory Report on the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* (August 2021), Recommendation 9
[47] See Comprehensive Review at [3.110]

information is inadvertently provided by a service provider), such as in the circumstances referred to in response to Question 18 in respect of the mandatory data retention scheme;
- the information relates to a third party who is not the subject of an investigation and is not relevant to the investigation being conducted;
- the information is deemed by the agency to not be required for any permitted purpose for which it was sought and obtained; and
- it is determined that the subject of the warrant or authorisation is no longer a person of interest in an investigation or the subject's activities are no longer relevant to security.

The destruction requirements in the new framework should be clear and consistent across all types of warrants and authorisations.

Emergency authorisations

Twitter considers that emergency authorisations should only be permitted where it is not possible to get a warrant or authorisation according to usual procedures and the case falls within a limited and defined list of critical situations, including where there is a serious and imminent threat to life or property, a terrorist attack, a suspected kidnapping, a missing person or the recovery of a child under court order. Twitter is strongly of the view that the use of an emergency authorisation process should be used sparingly and only in exceptional circumstances.

Under the new framework, the emergency authorisation process should be made consistent across activities and agencies. The process should require agencies to complete the necessary documentation and reporting process within a specified timeframe after an emergency authorisation is granted, to ensure that checks and balances remain in place. Where an oversight body reviews the legality and propriety of the emergency authorisation and determines that the emergency authorisation process should not have been utilised in the circumstances, there should be ramifications for the agency to provide a disincentive to using the emergency authorisation process where it was not actually necessary.

Otherwise, the default position should be for agencies to use conventional procedures, which should be made available outside office hours and should be able to be fulfilled within a short period of time when necessary. Sufficient provision should be made under the new framework for issuing authorities on an urgent basis and at short notice.

SAFEGUARDS AND OVERSIGHT

Strengthening safeguards

Twitter agrees that existing safeguards should be strengthened and consolidated. In relation to the points listed on pages 62-63 of the Discussion Paper, Twitter repeats its comments above in respect of Parts 3 and 4 of the Discussion Paper.

In addition to those matters, Twitter considers there are three further matters which are critical to industry in relation to providing for safeguards under the new framework:

(c) the need for the new framework to implement legislation that ensures organisations such as Twitter (including its employees) are immune from civil and criminal liability where they act in good faith in responding to requests or warrants from the various agencies;

(d) the need for robust and independent oversight by specified bodies of the relevant agencies that deploy the new framework to ensure they are acting lawfully and consistently; and

(e) the need for a review of the new framework after it comes into effect to ensure it contains appropriate protections for individual rights, remains proportionate to terrorism or national security threats, and is necessary.

Immunity from civil and criminal liability

The Discussion Paper does not give consideration to the immunity of an organisation and its employees in the course of their work responding to or complying with requests from agencies, such as responding to a warrant or an assistance order, under the new framework.

Twitter submits that the new framework must provide for the immunity from civil liability for organisations *and* their officers, employees and agents who act in good faith in the course of responding to a warrant or an assistance order from an agency. The terms of the immunity set out in Division 8 of Part 15 of the Telecommunications Act should be given consideration by the Department, and should be adopted consistently across all agencies and forms of warrant, authorisation and order (taking into account the recommendations of the INSLM in relation to the TOLA Act). Twitter further submits that organisations and their officers, employees and agents should not be exposed to a potential criminal offence where they have responded to a warrant or assistance order in good faith, bearing in mind limitations such as technical feasibility and obligations under international laws.

Oversight and transparency

As outlined in the Discussion Paper, robust independent oversight is necessary to ensure agencies use the new electronic surveillance framework lawfully and with propriety.

The Comprehensive Review recommends that the oversight framework for law enforcement agencies should be rationalised.[48] The difficulty with the current regime is that, for example, the TIA Act fragments oversight for state and territory law enforcement agencies between the Commonwealth Ombudsman (which oversees their access to stored communications and telecommunications data, as well as their use of surveillance devices and computer access powers under the Surveillance Devices Act) and the relevant state or territory oversight body (which oversees their use of telecommunications interception powers). This fragmentation is likely to lead to inconsistent oversight over the use of arguably the most intrusive powers under Commonwealth law.

Twitter agrees with the recommendation in the Comprehensive Review[49] that the oversight framework under the Surveillance Devices Act, which provides for the Commonwealth Ombudsman to oversee all aspects of each Commonwealth, state and territory agencies' use of the powers under that Act, should be adopted as the model. This would expand the role of the Commonwealth Ombudsman and would require additional resourcing.

Consequently, Twitter supports the position adopted in the Discussion Paper that the IGIS and the Commonwealth Ombudsman continue to oversee the use of electronic surveillance by ASIO (and other intelligence agencies) and law enforcement agencies respectively.[50] Ensuring these bodies have the right scope of oversight and sufficient powers to perform these functions is critical for developing public confidence in the new framework.

Any supervisory body must be independent, properly funded and operate separately from the relevant regulated law enforcement or national security agency.

Review of the new framework

Twitter submits that the operation, effectiveness and implications of the new framework should be subject to review by an independent supervisory body. Twitter submits that a review would be appropriate after the new framework has been in force for two years.

Twitter considers that the INSLM is the appropriate body to conduct this review, given their role in reviewing the operation, effectiveness and implications of national security and counter-terrorism laws, and considering whether the laws contain appropriate protections for individual rights, remain proportionate to terrorism or national security threats, and are necessary.[51] The requirement for a review should be included in the legislation implementing the new framework.

---

[48] See Comprehensive Review at [3.71]
[49] See Comprehensive Review at [3.72]
[50] See Discussion Paper at p 63
[51] *Independent National Security Legislation Monitor Act 2010* (Cth), s 6(1)

By way of example, the PJCIS referred the operation of the TOLA Act to the INSLM for review no later than 18 months following the Bill's enactment. In a media release on the referral, the PJCIS stated:

> *In our view, the INSLM provides a valuable, independent perspective on the balance between necessary security measures and the protection of civil liberties. As such, the INSLM is an important and valued component of Australia's national security architecture*.[52]

Twitter suggests that the objectives of the review conducted by the INSLM, could be to:

(a) consider how the new framework is operating in practice, including considering how various aspects of the new framework have been interpreted and applied by agencies;

(b) ensure the new framework has appropriately protected for individual's rights, is proportionate to criminal, terrorism and national security threats and is necessary; and

(c) consider whether the new framework is operating as it intended or whether it is having unintended consequences (such as an oversimplification of the warrant framework resulting in a threshold for obtaining a warrant being too low).

An important feature of INSLM reviews is that public engagement is welcomed. The INSLM can be assisted by written submissions from non-government entities who may have been affected by the new framework in some way. It is critical that the INSLM reports on its findings to the Government and to the public.

Legally privileged information

The rationale behind legal professional privilege is the need for full and frank communications between a person (the client) and their lawyer to enable the client to receive informed and properly considered advice on their legal rights. In Australia, it is a fundamental right that exists not only to protect the rights of individuals but also to facilitate the administration of justice.

It is for this reason that Twitter submits that the new framework should prohibit the use of surveillance and information gathering powers for the purpose of obtaining legally privileged information. It is not clear in what circumstances it would be appropriate for any agency to have access to documents and/or information subject to legal professional privilege.

Oversight mechanisms and obligations

Given the use of electronic surveillance powers by the agencies is highly intrusive and covert, the public are unable to scrutinise their operation. It is therefore particularly important that use of these powers by agencies is subject to a dedicated and independent oversight framework that focuses on:

(a) reducing the risk the powers are used unlawfully or improperly;

(b) maximising the likelihood that any unlawful or improper use of these powers is detected;

(c) maintaining the public's confidence in the electronic surveillance framework; and

(d) providing clear and consistent mechanisms to address unlawful or improper use of the powers.

In this respect, Twitter refers to and repeats its submissions in response to Question 28 above.

Twitter notes that a benefit of simplifying, consolidating and clarifying the existing legislative framework for electronic surveillance is that the new framework will hopefully be better understood and more accessible both by communications providers and members of the public.

---

[52] PJCIS, *Intelligence Community to Review Important National Security Legislation* (Media Release 1, 4 April 2019)

The new oversight framework should ensure that cases of non-compliance or malfeasance by agencies and any data breaches associated with information collected under warrants and authorisations are reported on publicly and remedial steps are included in agency reporting.

As highlighted above, the difficulty with the current regime is that there is fragmentation in the oversight of the use by various agencies of electronic surveillance between the Commonwealth Ombudsman, on the one hand, and the relevant state or territory oversight body, on the other hand.

Given the covert and intrusive nature of the agencies' powers, it is important the agencies are subject to robust oversight. This can only be achieved if the Commonwealth Ombudsman has the appropriate powers to require compliance by the agencies with its oversight.

Twitter adopts the Comprehensive Review's recommendation that the Commonwealth Ombudsman must be empowered to review any aspect of a Commonwealth, state or territory law enforcement agency's compliance with the new framework[53]. The reason for this is threefold:

(a) Comprehensive oversight should ensure there is a consistent approach to the oversight of the various agencies. By extension, it should hopefully reduce the possibility for gaps in oversight responsibilities between various State and Commonwealth oversight bodies.

(b) It should give both the industry and agencies more certainty and consistency in how they engage with the Commonwealth Ombudsman during the Ombudsman's review process, including the required information to be provided. Centralisation of oversight should also strengthen the Ombudsman's ability to promote best practice across agencies.

(c) It should reduce the burden on both the industry and agencies having to comply with requests which may overlap from different oversight bodies, resulting in a reduction of costs for all involved.

Twitter submits that the Department should also give consideration to introducing legislative protections for the Commonwealth Ombudsman, in line with the New Zealand Ombudsman model, to provide increased independence and ensure adequate resources.[54]

Twitter considers it appropriate that there be detailed record-keeping and reporting obligations imposed on agencies under the new framework to enhance oversight, transparency and accountability. The existing reporting requirements should be streamlined and made consistent throughout the new framework to ensure that the requirements facilitate meaningful transparency, in that the reports serve a useful function.

The new framework should require that all agencies publish unclassified reports about their electronic surveillance activities, which are accessible by the public, on an annual basis. These reports should include the number of warrants issued, the offences for which they were issued, whether or not information was relevant to the prosecution of those offences, how many prosecutions were commenced and how many prosecutions resulted in a conviction.

Agencies should also be required to proactively report any non-compliance with the legislation or any malfeasance to the appropriate oversight body.

Twitter recommends that consideration be given to strengthening reporting requirements on agencies to provide Parliament and the public with more meaningful information by:[55]

(a) introducing reporting on the number of occasions surveillance information is used in hearings convened by crime commissions and integrity agencies;

---

[53] Comprehensive Review, Volume 2, Recommendation 129

[54] Anita Stuhmcke, 'The Commonwealth Ombudsman: still fit for purpose?', Australian Public Law (September 2021), https://auspublaw.org/2021/09/the-commonwealth-ombudsman-still-fit-for-purpose/

[55] See Comprehensive Review, Volume 2 at [31.34]

(d) introducing reporting on the outcome of prosecutions in relation to which electronic surveillance was used as part of the investigation but which did not ultimately form part of evidence present in Court (e.g. as a result of a guilty plea being entered);

(e) introducing reporting on the number of persons subject to electronic surveillance; and

(f) introducing reporting on the number of occasions on which issuing authorities have required agencies to provide further information in support of warrant applications, or issues a warrant in terms other than those initially sought by the agency.

WORKING TOGETHER: INDUSTRY AND GOVERNMENT

Technical feasibility and compliance with requests

As a global company, Twitter exercises due diligence to respect local laws in jurisdictions around the world and duly reviews all legal processes. In Australia, Twitter works closely with federal and state law enforcement agencies in the course of their investigations. Twitter also maintains dedicated contact and dedicated reporting channels for law enforcement and responds to legal processes issued in compliance with applicable law.[56]

Twitter's Transparency Efforts

Twitter stands for transparency and has launched a variety of initiatives aimed at building and increasing public trust. We believe that the open exchange of information can have a positive global impact, and we strive to provide our users and the greater public with as much insight into the product updates we implement, the policy changes we make, and the actions we take on an ongoing basis. In line with this philosophy, since 2012 our biannual Twitter Transparency Report has also highlighted trends in requests made to Twitter from around the globe.[57]

Emergency Requests

In line with our Privacy Policy, we may disclose account information to law enforcement in response to a valid emergency disclosure request. Twitter evaluates emergency disclosure requests on a case-by-case basis in compliance with relevant law. If we receive information that provides us with a good faith belief that there is an exigent emergency involving a danger of death or serious physical injury to a person, we may provide any available information necessary to prevent that harm.[58]

Legal and Government Request Considerations

Twitter responds to requests for user account information from law enforcement where valid legal process is issued in compliance with applicable law. Where appropriate, Twitter will push back on requests for user account information that are incomplete or improper, such as requests that are facially invalid or overbroad in scope, or may seek further clarification or information from law enforcement in order to complete our review. Depending on the circumstances, Twitter may or may not disclose any data on receipt of a request from law enforcement. Twitter also may not have any responsive records to produce. Twitter notifies specified account holders of requests for their account information unless it is prohibited or the request falls into one of the exceptions to our user notice policy.

Where legally appropriate Twitter also accepts requests from law enforcement to preserve records that constitute potentially relevant evidence in legal proceedings. We will preserve, but not disclose, a temporary snapshot of the relevant account records for 90 days pending service of valid legal process.[59]

International Cooperation

---

[56] The Twitter Rules, 2022, https://help.twitter.com/en/rules-and-policies/twitter-law-enforcement-support
[57] Twitter, 2021. Transparency Centre. [online] Transparency.twitter.com. Available at: <https://transparency.twitter.com/en.html> [Accessed 12 February 2021].
[58] https://help.twitter.com/en/rules-and-policies/twitter-law-enforcement-support#14
[59] The Twitter Rules, 2022, https://help.twitter.com/en/rules-and-policies/twitter-law-enforcement-support

Separately and importantly, there are extraterritoriality considerations for service providers, like Twitter, which are in a position where compliance with an Australian legal process would directly conflict with obligations under laws of other countries where they operate. For example, service providers could violate laws around privacy and data collection that apply to Twitter's services because of legal obligations owed to customers from other countries, like the U.S. *Stored Communications Act*, where section 2702 forbids providing communications content to anyone absent appropriate *Electronic Communications Privacy Act* legal process.[60]

Consideration must be given to including an express provision in the new framework that provides an exemption for a service provider to not comply with a warrant or assistance order on the basis of there being a conflict with applicable overseas laws. Otherwise the framework may put overseas service providers in an untenable position where it must choose between violating either Australian law or laws in other jurisdictions, giving rise to potential civil and criminal liabilities. Further consideration needs to be given to the interaction between the new framework and foreign laws.

Streamlining collaboration between industry and government

The main way that Twitter considers the new framework could reduce the burden on industry and ensure that agencies and industry are able to work together in a streamlined way is to require agencies to engage in consultation with industry before warrants, authorisations or assistance orders are issued. Such requirements are already present under Part 15 of the Telecommunications Act in relation to assistance notices.

Twitter submits that consultation with communications providers on the form and detail of a warrant before it is issued will allow the communications provider to suggest any changes that might reasonably be necessary to support the implementation of the warrant and to ensure that the privacy interests of third parties who are not the subject of an investigation are protected. Involving communications providers at an early stage in the process will also assist in building a trust-based, respectful and reciprocal relationship between communications providers and agencies.

Twitter supports the recommendation in the Comprehensive Review that the new framework should not require carriers, carriage service providers or other regulated companies to develop and maintain attribute-based interception capabilities.[61]

However, Twitter does not support the recommendation by the Comprehensive Review that the new framework should empower the Attorney-General to require a specific company to develop and maintain a specified attribute-based interception capability.[62] The costs involved for industry in developing such a capability would be material, in circumstances where the potential benefits have been substantially diminished by the increased use of encrypted communications by bad actors.

Twitter supports reforming the Mutual Legal Assistance Treaty (MLAT) process, and has participated in consultations with the Department in relation to the International Production Order regime, which will facilitate a bilateral agreement under the CLOUD Act to enable streamlined legal processes between US-based communications providers and Australian authorities.

In regards to international standards with respect to surveillance reform, Twitter would encourage the Department to consult the Reform Government Surveillance principles in reference to the development of surveillance legislation.[63] These overarching principles provide guidance to help achieve a safe, secure internet while also protecting user privacy and freedom of expression.

INTERACTION WITH EXISTING AND RECENT LEGISLATION AND REVIEWS

Implementing recommendations from existing reviews

[60] *Electronic Communications Privacy Act of 1986* (18 U.S.C. ss 2701 to 2712)
[61] Comprehensive Review, Volume 2, Recommendation 110
[62] Comprehensive Review, Volume 2, Recommendation 111
[63] Reform Government Surveillance. 2021. RGS Principles - Reform Government Surveillance, https://www.reformgovernmentsurveillance.com/principles/

In relation to Question 37(b), Twitter considers that the safeguards that apply when agencies seek telecommunications data or issue a warrant in relation to information held by a journalist or media organisation should be strengthened, including reporting requirements, in order to increase the accountability of and public scrutiny of agencies in circumstances where freedom of the press and the protection of confidential sources may be at stake.

In relation to Question 37(c), Twitter repeats the comments it has made in response to Questions 18 and 24, in that it considers that the Public Interest Advocate framework should be expanded beyond professional journalists and media organisations to others engaging in legitimate and good faith news breaking activity, including Twitter users. Twitter submits that whistle-blowers should be afforded the same level of protection as a journalist's source. In this regard, a review of the *Public Interest Disclosure Act 2013* (Cth) should also be undertaken.

In relation to Question 37(d), Twitter would expect the introduction of a requirement for 'authorised officers' who can authorise the disclosure of telecommunications data to be sufficiently senior and trained is likely to generate positive results for industry in engaging with agencies and to improve public confidence in the new electronic surveillance framework.

Conclusion

Twitter is committed to providing meaningful transparency to the public and the people who use our service through ongoing improvements and updates. We are committed to a safe and open Internet, and believe that both governments and industry should ensure their respective approach to addressing online harm is consistent with universally recognised human rights norms, including proportionality and the protection of privacy and freedom of expression.

We look forward to continuing our engagement and collaboration with the Government, to work in good faith on these complex areas, and find global solutions to support law enforcement and security agencies in their goal of upholding freedom of expression while also protecting Australians from harm.