12 February 2021

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

By email: pjcis@aph.gov.au

Dear Committee,

Thank you for the opportunity to provide a written submission to the Australian Parliamentary Joint Committee on Intelligence and Security (PJCIS) regarding the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* ("the Surveillance Bill").

Transparency is fundamental to the work we do at Twitter. We are committed to providing meaningful transparency to the public and people who use Twitter through ongoing improvements and updates.

It is more important than ever we shine a light on our own practices, including enforcement of the Twitter Rules that govern and guide our service every day. We endeavour to provide people with recurring and updated insights into government actions and pressures that impact the general public, such as overt political censorship or by way of compelling account data through information requests. We believe it will take sustained research, discussion, and effort from government, industry, and relevant expert civil society to appropriately reform this draft legislation and its relevant processes in the interests of Australians and all those using Twitter.

The public and policy makers want to be better and more informed, and more regularly, about our actions. We recognise the public's right to know and respond, and we strive to meet the calls for open frameworks, democratic processes, accountability, and greater transparency. We believe these fundamental principles and the commitment to the open exchange of information should be shared by governments and regulators alike, and that when we do so, we contribute to a safer and open Internet. We believe this is in support of, not at odds with, evolving efforts to keep Australians safe and free from harms. Core in that work is a commitment to, and expectation from the public and people who use Twitter, access to reasonable, updated knowledge of what is happening on our service, their accounts, and the role of Government and law enforcement in relation to these factors.

Twitter remains committed to working with the Australian Government, industry, academia, and civil society to build our shared knowledge and understanding of these and apply optimal ways to approach them together.

Kind regards,

[redacted]
Kara Hinesley
Director of Public Policy
Australia and New Zealand

[redacted]
Kathleen Reen
Senior Director of Public Policy
Asia Pacific

Overview

Our submission to the Australian Parliamentary Joint Committee on Intelligence and Security (PJCIS) regarding the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* ("the Surveillance Bill") stands together with the submission from the trade association, the Digital Industry Group Inc. (DIGI), of which Twitter is a member. For clarity, and to complement and reinforce these statements, we've structured this submission to address the key issues contained in the Bill as they pertain to Twitter operating in Australia, including:

- The scope of the Bill and the process to issue an Account Takeover Warrant;
- Inconsistencies with powers to access data held by foreign and domestic service providers;
- Extraterritorial application of the Account Takeover Warrant and the absence of safeguards to protect companies including, for example, lack of notification that an account has been taken over; and
- The Account Takeover Warrant allows law enforcement to remove security safeguards that may be in place, alter account data that is held on servers, and access private messages in transit all without the knowledge of Twitter.

We trust this written submission, together with DIGI's submission, will be useful inputs to the Government's work. We urge and encourage the Committee to consider this holistic feedback while undertaking the review of this legislation.

Twitter's Transparency Efforts

In order to illustrate our position in relation to this Bill, we first want to share our principled approach to support open standards and open architecture on our service, as well as an overview of our law enforcement policies and processes.

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 highlighted trends in requests made to Twitter from around the globe.[1]

In our latest Transparency Report, Twitter saw global governments and law enforcement agencies submit approximately 44% more information requests (combined emergency and routine requests) compared to the previous reporting period. Notably, the aggregate number of accounts specified in these requests increased by nearly 26%. The total volume of requests and specified accounts are respectively the largest we've seen to date.[2]

[1] Twitter, 2021. Transparency Centre. [online] Transparency.twitter.com. Available at: <https://transparency.twitter.com/en.html> [Accessed 12 February 2021].
[2] Twitter, 2021. Transparency Centre. [online] Transparency.twitter.com. Available at: <https://transparency.twitter.com/en/reports/information-requests.html#2020-jan-jun> [Accessed 12 February 2021].

Country Insights

Twitter has received government information requests from 93 different countries since 2012 when Twitter first began compiling and publishing our Twitter Transparency Report. 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. We also maintain dedicated contact and dedicated reporting channels for law enforcement and respond to legal processes issued in compliance with applicable law.[3]

From January 2012 to our last reporting period in June 2020, Australia has collectively filed 259 information requests, and Twitter has a 47.5% compliance rate with 581 accounts specified. This represents less than 1% of Global Information requests received by Twitter to date.[4]

Emergency and Preservation Requests

In regards to emergency requests and preservation requests that we receive from law enforcement, Twitter may disclose account information to law enforcement officials in response to a valid emergency request as described in our Guidelines for Law Enforcement.[5] Twitter also accepts government requests to preserve account information.[6] Government entities issue preservation requests that direct service providers like Twitter to temporarily save information pertaining to an investigation. These requests give law enforcement, prosecutors, etc. the time needed to get the valid legal process, such as a search warrant, required to lawfully obtain that saved information. Upon receipt of a valid preservation request, we will temporarily preserve, but not disclose, a snapshot of the relevant account information for 90 days pending issuance and service of valid legal process.[7]

Request Considerations

Where appropriate, Twitter will push back on requests for account information that are incomplete or improper, such as requests that are facially invalid or overbroad in scope. Depending on the circumstances, we may produce some data after working to narrow a request, or we may not disclose any data. We also may not have any responsive records to produce. We notify specified account holders of requests for their account information unless we are prohibited or the request falls into one of the exceptions to our user notice policy.[8]

International Cooperation

---

[3] Twitter, 2021. The Twitter Rules. [online] Help.twitter.com. Available at: <https://help.twitter.com/en/rules-and-policies/twitter-law-enforcement-support> [Accessed 12 February 2021].
[4] Twitter, 2021. Transparency Centre. [online] Transparency.twitter.com. Available at: <https://transparency.twitter.com/en/reports/information-requests.html#2020-jan-jun> [Accessed 12 February 2021].
[5] *Ibid.*
[6] Twitter, 2021. The Twitter Rules. [online] Help.twitter.com. Available at: <https://help.twitter.com/en/rules-and-policies/twitter-law-enforcement-support> [Accessed 12 February 2021].
[7] Twitter, 2021. Transparency Centre. [online] Transparency.twitter.com. Available at: <https://transparency.twitter.com/en/reports/information-requests.html#2020-jan-jun> [Accessed 12 February 2021].
[8] *Ibid.*

Enacted in the United States in March 2018, the Clarifying Lawful Overseas Use of Data Act ("CLOUD Act") established a framework for the U.S. Government to enter into bilateral agreements with certain qualifying foreign governments. Once a relevant bilateral agreement goes into effect, U.S. providers, such as Twitter, may receive compulsory legal demands directly from foreign government entities to disclose account information and content of communications, as well as real-time surveillance orders for account information, which are akin to pen register/trap and trace and wiretap orders as described in our U.S. report.[9]

Broadly speaking, Twitter supports reforming the Mutual Legal Assistance Treaty (MLAT) process, and we have participated in consultations with the Department of Home Affairs and the Australian Government in relation to the International Production Order regime, which will facilitate a bilateral agreement under the CLOUD Act to enable streamlined legal processes between U.S. providers and Australian authorities.

Twitter continues to closely monitor developments related to cross-border legal requests for user data. We will update our policies as necessitated by changes in the legal landscape, in keeping with our commitment to defending and respecting the user's voice and transparency.

Additionally in regards to international standards with respect to surveillance reform, Twitter would encourage the Australian Government to consult the Reform Government Surveillance ("RGS") principles in reference to the development of surveillance legislation.[10] These overarching principles provide guidance to help achieve a safe, secure internet while also protecting user privacy and freedom of expression.

Scope of the Bill and corresponding processes

Twitter shares the Australian Government's goal of disrupting bad actors and removing illegal content from the Internet. The Surveillance Bill introduces measures to address the investigation of online crime where criminals seek to exploit technologies and services, including the dark web. However, to achieve this goal, the Bill contains three new types of warrants including: (1) Data Disruption Warrants, (2) Network Activity Warrants, and (3) Account Takeover Warrants.

All three classes of warrants contain potentially problematic and inconsistent processes. For example, the Data Disruption Warrant and Network Activity Warrant both amend the *Surveillance Devices Act 2004* (Cth)[11] ("SD Act") whereas the Account Takeover Warrant amends the *Crimes Act 1914* (Cth)[12] ("Crimes Act"). As these warrants are amending different pieces of legislation, they take divergent approaches to accountability, issuing authorities, and extraterritorial application causing inconsistent and irreconcilable standards.

---

[9] *Ibid.*
[10] Reform Government Surveillance. 2021. RGS Principles - Reform Government Surveillance. [online] Available at: <https://www.reformgovernmentsurveillance.com/principles/> [Accessed 12 February 2021].
[11] *Surveillance Devices Act 2004* (Cth). [online] Available at: <https://www.legislation.gov.au/Details/C2017C00193> [Accessed 12 February 2021].
[12] Federal Register of Legislation - Australian Government. [online] Available at: <https://www.legislation.gov.au/Series/C1914A00012> [Accessed 12 February 2021].

Overall, we have overarching concerns across the relevant sections of the Bill that these three types of warrants can be implemented without providing proper notification to service providers. With regards to Twitter's service specifically though, we will focus on Account Takeover Warrants in this submission, which pose sweeping expansions to surveillance powers and covert activities that could impact Twitter's platform and operations inside and outside of Australia.

Account takeover warrant and issuing authorities

As drafted, Division 2 focuses on Account Takeover Warrants that would enable the Australian Federal Police (AFP) or the Australian Criminal Intelligence Commission (ACIC) to take control of a person's online account for the purposes of gathering evidence about serious offences; however, the additional legislative supporting documentation is unclear regarding the scope of an Account Takeover Warrant.[13]

In the Explanatory Memorandum (EM), the Overview of the Bill outlines that "an account takeover warrant [is] to allow the AFP and the ACIC to take over a person's online account the purposes of gathering evidence of criminal activity." However Schedule 3, paragraph 25 states that "this power enables the action of taking control of the person's account and locking the person out of the account. Any other activities, such as accessing data on the account, gathering evidence, or performing undercover activities such as taking on a false identity, must be performed under a separate warrant or authorisation. Those actions are not authorised by an account takeover warrant."[14] Thus, the scope regarding what activities are ultimately authorised under an Account Takeover Warrant remains unclear.

Additionally within the exposure draft of the Bill, in order to effectuate the execution of the Account Takeover Warrant, it appears that a law enforcement officer would be authorised to take control of one or more accounts and access account-based data in addition to adding, copying, deleting, or altering account credentials. The Surveillance Bill also provides that access to account-based data is allowed under the warrant if it is necessary to enable evidence to be obtained for an alleged offence.

The Department of Home Affairs has confirmed that an Account Takeover Warrant is designed to be used in circumstances where law enforcement officers have a person's account credentials, but the person has not given his or her permission for law enforcement to use the account. The Minister in his second reading speech stated:

> *"the account takeover power will allow officers to take over online accounts and gather evidence about a person's online criminality and their associate's activity…Through the new account takeover warrant, AFP and ACIC will be authorised to take control of a person's online account to gather evidence leading to prosecutions of a serious offence."*[15]

---

[13]Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 – Parliament of Australia. [online] Available at: <https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6623> [Accessed 12 February 2021].

[14]*Ibid.*

[15] Dutton, P., 2021. ParlInfo - BILLS: Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020: Second Reading. [online] Parlinfo.aph.gov.au. Available at: <https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22chamber%2Fhansardr%2F11b18738-de56-4d82-82f6-2c10fddd6b2b%2F0024%22> [Accessed 12 February 2021].

Under applicable laws, generally the police cannot search your computer or mobile device for emails, social media posts, or other digital information without your consent unless they first obtain a warrant.[16] When issuing a warrant, a magistrate must consider, and may approve, certain activities for the purpose of taking control of the account including the altering of account credentials. The magistrate must also have regard to the nature and gravity of the offences, the impact on privacy, the likely evidentiary value, and the existence of any alternative means of obtaining the evidence.

While the Bill may include these limited safeguards regarding considerations for privacy and proportionality before issuing an Account Takeover Warrant, there is no consideration or reference in the Bill of the implications of law enforcement agencies accessing a service without the knowledge of the service provider. We are very concerned about the implications for Twitter's own obligations as a company, as well as the rights and privacy implications for the users of Twitter and other online services.

Furthermore, the policy decision to utilise lower-level magistrates rather than a judge or Administrative Appeals Tribunal (AAT) member to issue Account Takeover Warrants is inconsistent with other electronic surveillance warrants. For example, the Government recently agreed to recommendations made by this Committee regarding search warrants against journalists and whistleblowers needing to be signed off by senior judges.[17]

One of the criticisms regarding the raids in June 2019 on the ABC's Sydney headquarters and former News Corp political journalist Annika Smethurst was that the search warrants were authorised by the registrar of a local state court. As recommended by this Committee, the power to issue such serious search warrants should be solely held by senior judges, such as those on State and Territory Supreme Courts, given the sensitivity of such investigations.[18] However, that was not the approach taken in this Bill.

Additionally, the Data Disruption Warrants and Network Activity Warrants follow the model currently in the SD Act, the *Telecommunications (Interception and Access) Act 1979* (Cth), and the proposed International Production Order regime requiring warrants be issued by an eligible judge or nominated Administrative Appeals Tribunal (AAT) member acting in his or her personal capacity.

Consistent with the Committee's recommendations regarding search warrants against journalists and whistleblowers, as well as Attorney-General Christian Porter's announcement that the Government agrees with that recommendation, we encourage the Government to implement consistent levels of

[16] *Crimes Act 1914* (Cth), s 3LA.
[17] Doran, M., 2021. Government agrees to recommendations to strengthen press freedom. [online] Abc.net.au. Available at: <https://www.abc.net.au/news/2020-12-16/federal-government-agrees-to-changes-to-media-protection/12990498> [Accessed 12 February 2021].
[18] Parlinfo.aph.gov.au. 2021. [online] Available at: <https://parlinfo.aph.gov.au/parlInfo/download/committees/reportjnt/024411/toc_pdf/Inquiryintotheimpactoftheexerciseoflawenforcementandintelligencepowersonthefreedomofthepress.pdf;fileType=application%2Fpdf> [Accessed 12 February 2021].

review with regards to the judicial authority in the context of the Bill to ensure proper oversight and accountability, along with other recommended changes to the proposed warrant process.[19]

Additionally, the Bill is unclear regarding standards of review and the means of appeal available to a service provider, like Twitter. This is especially in the context where notice is not provided to the company that these Account Takeover Warrants are being applied. Also, it does not appear that the Bill has contemplated any processes to consider and protect the rights of any third party users who may interact with the account that has been subject to an Account Takeover Warrant.

This again raises a number of inherent privacy concerns and potential violations of substantive rights, as well as potential conflict of laws if these third party users are outside of Australia. Therefore, we would recommend that the Government institute the necessary protections and procedures to address these issues in order to preserve democratic processes, extend privacy protections, and enshrine procedural fairness within the context of the Bill.

Extraterritorial Application

As currently written, the Account Takeover Warrant would be divorced from standard due process requirements. It would be antithetical to core legal principles enshrined in democratic law and procedural fairness.

Twitter is concerned that the proposed Bill will allow law enforcement direct access to data regardless of the location of the server, without requiring knowledge of such access being provided to the service provider, and in the case of Account Takeover Warrants, absent the agreement of an appropriate consenting official of the relevant foreign country where the warrant would be enforced.

In the Bill, all three types of warrants provide for access to data, computers, and accounts in any jurisdiction. The Data Disruption and Network Activity Warrants, however, limit extraterritorial operation of warrants to allow access to information that may be held in foreign jurisdictions only if the access has been agreed to by an appropriate consenting official of the foreign country.[20]

Conversely, as currently drafted the Account Takeover Warrant can also apply extraterritorially but does not have the requirement to obtain the agreement of a consenting official in a foreign country, nor provide notice to the service provider who is offering the service.[21] Therefore, the Account Takeover Warrant will apply extraterritorially with Australian law enforcement being authorised to take control of an online account regardless of where the account data is located and without consent from foreign Governments or officials.

---

[19] Attorney General Media Centre 2021. [online] Available at: <https://www.attorneygeneral.gov.au/media/media-releases/enhancing-whistle-blower-protections-16-december-2020> [Accessed 12 February 2021].

[20] *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020,* Clause 11, Schedule 2, Part 1 . [online]. Available at: <https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6623? [Accessed 12 February 2021].

[21] Parlinfo.aph.gov.au. 2021. [online] Available at: <https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r6623_first-reps/toc_pdf/20144b01.pdf;fileType=application%2Fpdf> [Accessed 12 February 2021].

Neither the draft Bill nor the accompanying Explanatory Memorandum (EM) provides clear guidance on these extraterritorial issues. Thus, it is our understanding that the Account Takeover Warrant is a covert warrant and provides for the Australian Federal Police (AFP) or the Australian Criminal Intelligence Commission (ACIC) to take exclusive control of the online account without safeguards afforded other warrant processes.

If the Account Takeover Warrant is to be used to access an online account regardless of the location of the server, and executed without the knowledge of a service provider, or foreign official, then all due process requirements and safeguards that typically surround warrant processes have essentially been removed.

Assistance Orders

Under Division 4 in relation to Assistance Orders, a law enforcement officer may apply for an 'assistance order' pursuant to Section 3ZZVG after a warrant is issued. A magistrate will make an order where law enforcement requires a 'specified person' to provide information or assistance to enable them to take control of an account.[22]

Based on the definition of a 'specified person' under Section 3ZZVG, subsections (b)(vi) and (c), it is unclear if the legislation would require service providers and their relevant employees to comply with assistance orders. Additionally, the EM does not provide clear guidance on this issue.

Beyond the lack of oversight in this process, an 'assistance order' made in conjunction with an Account Takeover Warrant is likely to place service providers, like Twitter, in a position where compliance 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 our 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* (ECPA) legal process.[23] Additionally, Twitter does not store user credentials, including passwords, in plaintext form. Thus, depending on the content of the assistance order, service providers like Twitter could be in a position where our capacity to comply with these orders would be correspondingly limited or not technically feasible. This paradox places service providers in an impossible situation with regard to conflict of laws or technical feasibility and could potentially place Australian national security agencies in direct conflict with relevant international obligations or legal regimes operating in other jurisdictions.

Operating under the understanding that service providers may not even have knowledge that these warrants are being implemented, we would again recommend that this section require agencies to disclose when warrants may be effectuated under this legislation, and evaluate what constitutes reasonable or proportionate conduct in relation to compelling a service provider or their employees to comply with an assistance order as the Bill is currently drafted.

[22] *Ibid.*
[23] *Electronic Communications Privacy Act of 1986* (18 U.S.C. §§ 2701 to 2712).

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. We believe it will take sustained research, discussion, and effort from government, industry and relevant expert civil society to appropriately reform this draft legislation and its relevant processes.

We urge the Government to amend the Bill to reflect practices that are consistent with established norms of privacy, free expression, and the rule of law. Given the seriousness of the issues raised by the Bill and potential adverse impact on the safety and the security of online communications generally, we would recommend that the Government continue to increase dialogue with civil society industry and recognized experts in these complex areas to find global solutions to support law enforcement and security agencies in their goal of protecting Australians from harm.