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,

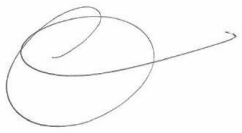
RE: Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020

The *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* ("**the Bill**") has been referred to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) and we appreciate the opportunity to make the following submissions regarding the Bill on behalf of the Queensland Council for Civil Liberties; Liberty Victoria; Electronic Frontiers Australia; and the Australian Privacy Foundation.

The Committee would appreciate that representatives from these organisations have appeared at hearings in relation to similar legislative amendments and we draw particular attention to the joint submission we made to the *Joint Parliamentary Committee on Law Enforcement Inquiry into new Information Communication Technologies* that covered the proposed government hacking powers.[1]

Our submissions are contained in the following pages and we trust that these submissions assist the Committee in their evaluation of the proposed powers.

Yours sincerely,



Angus Murray
Vice-President, Queensland
Council for Civil Liberties

Dr Monique Mann
Vice-President and Co-Chair Privacy Committee
Liberty Victoria

Chair, Policy Committee of
Electronic Frontiers Australia

Vice-Chair and Chair Surveillance Committee
Australian Privacy Foundation

[1] Mann, Monique, Molnar, Adam, Warren, Ian, & Daly, Angela (2018) *Joint Submission by Australian Privacy Foundation, Electronic Frontiers Australia, Digital Rights Watch and Futurewise - Submission to Joint Parliamentary Committee on Law Enforcement Inquiry into new Information Communication Technologies (ICTs) and the challenges facing law enforcement agencies.* Joint Parliamentary Committee on Law Enforcement, Australia at Page 9 & 10 for coverage of computer network operations.

Submissions

1. The Bill introduces legislative provisions in four (4) broad categories that can be described as follows:

    a. a data disruption warrant which enables the AFP and the ACIC to access data on one or more computers and perform disruption activities for the purpose of frustrating the commission of criminal activity ("**Data Disruption Warrants**").

    b. a network activity warrant to enable the AFP and the ACIC to collect intelligence on criminal networks operating online ("**Network Activity Warrants**").

    c. an account takeover warrant to allow the AFP and the ACIC to take over a person's online account for the purposes of gathering evidence of criminal activity ("**Account Takeover Warrants**").

    (collectively, "**the Warrants**")

    d. Minor amendments to the controlled operations regime, to ensure controlled operations can be conducted effectively in the online environment ("**Minor Amendments**").

2. This submission addresses broad issues arising from the Bill before making recommendations regarding the Bill.

Broad Issues with the Bill

3. At the outset broadly and generally speaking, the Bill introduces powers for State-authorised hacking (also known as: lawful hacking, government hacking, computer network operations, network exploitative techniques). It is our position that Australia does not have an adequate federal human rights framework. Therefore, should the Bill come into force, Australians do not have sufficient safeguards of their fundamental rights to protect them from abuse of power by authorities.

4. We also note that the Bill provides similar power to the measures that were introduced by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* ("**the AA Act**") (i.e. to do an unlimited range of "acts or things" to access information) and the justifications for the Bill are similar to the AA Act. We submit that it is appropriate in these circumstances for the Committee to ensure that evidence is provided by the Department of Home Affairs as to the necessity of the Bill and that evidence is given of the complete and proper scrutiny that is necessary in the context of ever-expanding digital surveillance in Australia.

5. Notwithstanding the above, and unlike many new surveillance powers that have been introduced over the previous years (i.e. metadata retention, anti-encryption), one positive of the Bill requires the issue of a warrant (either via an appointed member of the Administrative Appeals Tribunal or a Judge). This provides a modicum of independent oversight. However, we are concerned that the Bill expressly precludes judicial or merits review of the decision to issue warrants[2] and have concerns about the independence of the AAT.[3] It is imperative that the Australian community is afforded the fullest benefit of the rule of law. It is vital that Australians have a proper and clear avenue to address abuses of power when their human rights can be seriously affected.

6. In this context, the Explanatory Memorandum sets out that:

> "*the purpose of the Bill is to protect national security, ensure public safety, and to address online crime and particularly the challenges posed by the dark web and anonymising technologies...*".[4]

7. We appreciate that there is an imperative placed upon the Government to protect our national security; however, that imperative should not be used as a "blanket" to enable the passage of all legislation that seriously impact and override human rights. As it stands, the Bill's powers would operate in contexts other than just national security. We submit that the operation of the Bill should be narrowed to the reasons supporting the justification of the introduction of the bill, that is for national security reasons. The amendment by s. 3ZZUK provides for the operative definition of "relevant offence" which includes "a serious Commonwealth offence; or a serious State offence that has a federal aspect". Section 15GE(2) of the *Crimes Act 1914* provides that any of the following may constitute a serious commonwealth offence where the maximum sentence is greater than three (3) years:

> (a) theft;
> (b) fraud;
> (c) tax evasion;
> (d) currency violations;
> (e) controlled substances;
> (f) illegal gambling;
> (g) obtaining financial benefit by vice engaged in by others;
> (h) extortion;
> (i) money laundering;
> (j) perverting the course of justice;

---

[2] Explanatory Memorandum to the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* at para 44.

[3] This concern is not raised to impugn the integrity of the Administrative Appeals Tribunal, rather that the power to authorise covert surveillance of Australians ought to be reserved for a Chapter 3 Court which is subject to a complete operation of the rule of law and the rules of evidence.

[4] Explanatory Memorandum to the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* at para 22.

(k) bribery or corruption of, or by, an officer of the Commonwealth, of a State or of a Territory;
(l) bankruptcy and company violations;
(m) harbouring of criminals;
(n) forgery (including forging of passports);
(o) armament dealings;
(p) illegal importation or exportation of fauna into or out of Australia;
(q) espionage, sabotage or threats to national security;
(r) misuse of a computer or electronic communications;
(s) people smuggling;
(t) slavery;
(u) piracy;
(v) the organisation, financing or perpetration of sexual servitude or a sexual offence against a person who is under 18 outside Australia;
(w) dealings in child abuse material;
(x) importation of prohibited imports;
(y) exportation of prohibited exports;
(z) violence;
(za) firearms;
(zb) a matter that is of the same general nature as a matter mentioned in one of the preceding paragraphs;
(zc) a matter that is prescribed by the regulations for the purposes of this paragraph.

8. We respectfully accept that some of these offences *may* warrant the use of intrusive law enforcement power; however, we do not accept that the significant power authorised by the Bill should be applied to an existing definition of "serious commonwealth offence". More specifically, we do not accept that State-authorised hacking is appropriate in the context of tax or bankruptcy offences. We are also concerned that the Bill's operation can be further expanded by the executive, through the regulations prescribing a "relevant offence".

9. We are also sceptical about the threshold requirement of "reasonable suspicion" to engage the operation of the Bill. As the Committee would appreciate, the concept of "reasonable suspicion" has received judicial attention[5] and it is, in our submission, important to ensure that the Bill, if passed, requires a high enough threshold so as to ensure that the Warrants issued are only in circumstances where cogent evidence is available to support the need for the Warrants. Reasonable suspicion is an inappropriately low threshold for the issue of any of the Warrants.

10. Finally, we note that the Assistance Orders provided at s. 3ZZVG of the Bill are remarkably similar to the Technical Assistance Requests contained within the AA Act.

[5] See: *George v Rockett* [1990] HCA 26.

We are unsure why the Executive would require additional power beyond what is available under the AA Act. No explanation or evidence has been provided to support this additional power. It is also concerning that the context within which assistance orders are set in the Explanatory Memorandum could include journalists, academics or business owners[6]. The offence which would be created at s. 64B(3) does not contemplate circumstances where:

a. the provision of assistance would constitute a breach of confidence; or
b. the relevant omission which underlies the offence arises as a consequence of a Warrant that is inadequately or unclearly drafted.

The Warrants

11. At the outset, we submit that each of the Warrants should require statutory inclusion of a requirement that an eligible Judge or Administrative Appeals Tribunal Member must consider the human rights (including specifically the right to privacy) implications of issuing one of the Warrants. As the Bill is drafted, the consideration required by the Court focuses on the reasonable suspicion held by the authorising officer which is insufficient in the context of the potential for serious violations of human rights that may occur, directly or indirectly, to the subject of the warrant or other persons. Balanced against the reasonable suspicion, there ought be a statutory requirement as to whether that reasonable suspicion is grave enough to justify a curtailment of rights, such as the right of privacy.

12. We also submit that the Bill, as with all surveillance legislation ought to be the subject of a Public Interest Monitor to ensure that these intrusive powers remain in the public interest and do not scope creep without oversight and a modicum of transparency.

Data Disruption Warrants

13. The Explanatory Memorandum describes Data Disruption Warrants as "warrants to enable the AFP and the ACIC to disrupt data by modifying, adding, copying or deleting in order to frustrate the commission of serious offences online".[7]

14. We submit that there are two (2) fundamental issues that arise in relation to Data Disruption Warrants.

15. Firstly, and principally, it is a dangerous step to enable law enforcement to modify what would be evidence in a criminal proceeding. We appreciate that the intention is to

---

[6] See Explanatory Memorandum to the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* at para [250] which provides that: "*In a case where the computer is the subject of a data disruption warrant or emergency authorisation, the particular person must be either reasonably suspected of having committed a relevant offence, or the owner or lessee of the computer, or an employee or contracted person of the owner or lessee, or a person who uses or has used the computer, or a person who is or was a system administrator for the computer*".

[7] Explanatory Memorandum to the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* at para [6].

frustrate and prevent the distribution of child exploitation material, as that is the example given in the Explanatory Memorandum; however, this inherently causes evidence to be altered and this needs to be addressed. If there is an intention that this power is only to be used in limited circumstances, then that limitation ought be enshrined in the statute, so the power is not used in circumstances that were not in the contemplation of Parliament.

16. Secondly, law enforcement has a poor record of the consequence of modification or deletion of digital information. The Bill has few, if any, safeguards to protect innocent parties from adverse consequences associated with the disruption of data that may result in significant, though unintended, harm as occurred with the Australian Securities and Investments Commission use of s. 313 of the *Telecommunications Act 1997* to block websites which resulted in some 250,000 websites being inadvertently blocked.[8]

17. The Bill should also include additional remedies to affected parties that suffer harm as a consequence of inappropriate use of these powers. Innocent parties should not be placed at risk by the misplaced zeal of authorities, and use of powers such as those in this Bill should only be contemplated with sufficient duty of care to the public as a whole.

Network Activity Warrants

18. The Explanatory Memorandum describes Network Activity Warrants as "warrants to allow agencies to collect intelligence on serious criminal activity being conducted by criminal networks".[9]

19. For the reasons expressed under the heading "*Broad Issues with the Bill*" do not not accept that Network Activity Warrants ought to be introduced into Australian law.

Account Takeover Warrants

20. The Explanatory Memorandum describes Account Takeover Warrants as "warrants to provide the AFP and the ACIC with the ability to take control of a person's online account for the purposes of gathering evidence to further a criminal investigation".[10]

21. For the reasons expressed under the heading "*Broad Issues with the Bill*" do not not accept that Account Takeover Warrants ought to be introduced into Australian law.

Extraterritorial Application and Potential Interaction with Other Proposed Surveillance Laws

22. These powers are, by design, an attempt to uncover 'dark' networks which operate via identity and geolocation concealing technologies such as Virtual Private Networks

[8] See for example: https://www.itnews.com.au/news/asic-admits-to-lack-of-technical-knowledge-in-s313-use-391441.

[9] Explanatory Memorandum to the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* at para [6].

[10] Explanatory Memorandum to the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* at para [6].

(VPNs) and Tor. This means that the physical location of the target computer and suspect is not known by Australian law enforcement in advance of the exercise of the powers.

23. The powers of Australian law enforcement are limited to the sovereign jurisdiction of Australia. These powers effectively extend the reach of Australian law enforcement outside of the sovereign jurisdiction of Australia with significant extraterritorial impacts. They also require Australian judicial authorities and the AAT to authorise extraterritorial law enforcement operations outside of the scope of their lawful jurisdiction to do so. This means that there are due process risks for suspects located outside of Australia which may jeopardize prosecutions.[11]

24. Further, it is not clear how these proposed laws will interact with other proposed surveillance laws such as the *International Production Orders Bill* that is also presently before the PJCIS for consideration (that supports a data sharing agreement with the United States).

25. In absence of a clear transnational regulatory structure supporting transnational government hacking operations in cases where the physical location of the target computer and suspect is not known these proposed laws should be reconsidered.

Recommendations

26. On the basis of these submissions, we consider that the following recommendations constitute a reasonable and responsible means to addressing deficiencies contained within the Bill. These recommendations ought to be read with the understanding the Recommendation One is proposed as an overarching proposal and the balance of the recommendations are made in the event that Recommendation One is not adopted. The balance of the recommendations are provided for completeness and ought not be read to detract from the importance of Recommendation One.

Recommendation One: The Bill is withdrawn and not re-introduced until such time as a Federal enforceable human rights framework is introduced into Australian law.

Recommendation Two: The issue of any and all of the Warrants proposed in the Bill be the subject of merits and judicial review with the Federal Court of Australia vested with original jurisdiction to hear such applications.

Recommendation Three: The definition of "relevant offence" at s. 3ZZUK of the Bill should be redefined to include an exhaustive list of specific serious offences.

---

[11] See for e.g. Warren, I., Mann, M. & Molnar, A. (2020). Lawful illegality: Authorising extraterritorial police surveillance. *Surveillance and Society, 18*(3), 357-369; Warren, I., Molnar, A. & Mann, M. (2017). Poisoned water holes: The legal dangers of dark web policing. *The Conversation;* Mann, M., Molnar, A;. & Warren, I. (2018). Computer network operations and cross-border data requests. The State of Digital Rights Report. Digital Rights Watch Australia.

Recommendation Four: The threshold for the issue of any of the Warrants be raised to "reasonable belief informed by probative evidence".

Recommendation Five: Assistance Orders be removed from the Bill.

Recommendation Six: The decision making criteria for the issue of any of the Warrants or an Assistance Order explicitly include consideration of the potential impact on the human rights of the subject and any other, directly or indirectly, affected person(s).

Recommendation Seven: Set clear limits for the extraterritorial exercise of Australian law enforcement powers.

Recommendation Eight: The Bill, as with all surveillance legislation ought to be the subject of a Public Interest Monitor.