Electronic Frontiers
AUSTRALIA

W www.efa.org.au
E email@efa.org.au
@efa_oz

1July 2019

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

By Email: pjcis@aph.gov.au

Dear Secretary,

RE: REVIEW OF THE AMENDMENTS MADE BY THE TELECOMMUNICATIONS AND OTHER LEGISLATION AMENDMENT (ASSISTANCE AND ACCESS) ACT 2018

We appreciate this further opportunity to make submissions in relation to the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (**"the Act"**). EFA's submission is contained in the following pages.

About EFA

Established in January 1994, EFA is a national, membership-based non-profit organisation representing Internet users concerned with digital freedoms and rights. EFA is independent of government and commerce and is funded by membership subscriptions and donations from individuals and organisations with an altruistic interest in promoting civil liberties in the digital context. EFA members and supporters come from all parts of Australia and from diverse backgrounds.

Our major objectives are to protect and promote the civil liberties of users of digital communications systems (such as the Internet) and of those affected by their use and to educate the community at large about the social, political and civil liberties issues involved in the use of digital communications systems.

EFA thanks its Policy Committee for their assistance with the preparation of this submission. Information about EFA's Policy Committee is located here: https://www.efa.org.au/our-work/policy-team/

Yours sincerely,

[redacted]

Angus Murray
Chair of the Policy Committee
Electronic Frontiers Australia

Introduction

1. Firstly, we repeat our previous submissions respectively made to the Department of Home Affairs and to the Parliamentary Joint Committee on Intelligence and Security in response to the *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* ("**the Bill**").

2. These previous submissions were made in September and October 2018 in collaboration with a number of other organisations and individuals and are available via the links below:

    - September 2018 Submission to the Department of Home Affairs[1]; and
    - October 2018 Submission to the Parliamentary Joint Committee on Intelligence and Security[2].

    (collectively, "**the Previous Submissions**")

3. This submission is also to be read in conjunction with the further submission made by a large group of civil society organisations under the Australian Civil Society Coalition Submission ("**the ACSC Submission**"). The Committee ought to have particular regard to the qualifications of the authors of the Previous Submissions and the ACSC Submission and that these submissions have been significantly peer-reviewed. The common consensus reached by civil society organisations ought to be recognised.

4. We reiterate and repeat the recommendations contained within the ACSC Submission and in the Previous Submissions.

5. We also note that it is clear from this incredibly short turnaround from the closing of submissions on the exposure draft and the introduction of the Bill into the Lower House that the Australian Government had absolutely no intention of meaningfully engaging with experts or civil society on an issue that is central to Australia's digital critical infrastructure. The actions in this "consultative process" show an alarming disregard of, and disrespect for, the fundamental principles of a liberal democratic society. The Bill was pushed forward with minimal consultation, and in the face of widespread criticism from both Australian and international civil society, as well as the community of academic experts with deep knowledge in this field.

6. Given the lack of change to the Bill since the exposure draft, our comments in the Previous Submissions are still relevant to the effect of the Act.

7. As such, in this current submission to this Review primarily the EFA repeats our view that the Act is disproportionate to the reasonable expectation of the Australian community in the absence of enforceable human rights legislation at the Federal level. The Act vests significant power with law enforcement that may be used covertly and with an international application - with insufficient oversight.

---

[1] https://ww.efa.org.au/main/wp-content/uploads/2018/10/Submission-Assistance-and-Access-Bill-2018_collaborative_submission.pdf.
[2] https://digitalrightswatch.org.au/wp-content/uploads/2018/10/PJCIS-Encryption-Bill-Sub.pdf

8. While we have responded in line with the Terms of Reference, this submission must be read within a context requiring the immediate repeal of the Act until such time as an enforceable federal human rights framework has been implemented in Australia.

Areas of Focus

9. We understand that the Committee requested that the Independent National Security Legislation Monitor review the "*operation, effectiveness and implementation*" of the amendments to the Act focused on whether the Act:

    - *"contains appropriate safeguards for protecting the rights of individuals;*
    - *remains proportionate to any threat of terrorism or threat to national security, or both; and*
    - *remains necessary."*

10. This submission responds to each of the focus areas with specific regard to the resolution of the Committee to focus on the following aspects of the Act:

    - the threshold, scope and proportionality of powers provided for by the Act;
    - authorisation processes and decision-making criteria;
    - the scope of enforcement provisions and the grant of immunities;
    - interaction with intelligence agencies other powers;
    - interaction with foreign laws, including the United States' Clarifying Lawful Overseas Use of Data Act;
    - impact on industry and competitiveness; and
    - reporting obligations and oversight measures.

11. Our previous submissions provide extensive comment on the Act's lack of safeguards to protect the rights of individuals - including that the Act:

    - contains insufficient consideration of the public interest in decision-making criteria for technical access notices, technical access requests or technical capability notices.
    - introduces covert computer access warrants enabling law enforcement to search computers and electronic devices without an individual's knowledge; and
    - increases the powers of law enforcement to use and apply the currently available search and seizure warrants.

12. We also respectfully repeat our previous submission that any legislative provision should be subjected to rigorous assessment as to its necessity, adequacy and proportionality[3]. It is difficult to make a meaningful submission on this area of focus because it conflates the concern of civil society into a construct of confidential national security information. It is our position that the scope, terms and purpose of the Act are not proportionate to the reasonable expectations of the Australian community and we; while this submission acknowledges the fundamental importance of keeping the Australian community safe, note that, during 2017-2018, there was only two (2) "disruptions of planned terrorist attacks" from a total of 14,227 leads investigated at a cost of $533,449,000.00[4].

[3] https://www.eff.org/deeplinks/2014/09/australians.
[4] See: https://www.asio.gov.au/sites/default/files/ASIO%20Annual%20Report%20to%20Parliament%202017-18.pdf at Page 7.

Authorisation processes and decision-making criteria

13. As noted in our previous submissions in relation to Schedule 1 of the Act, there is no requirement to consider the public interest in the decision-making criteria for technical access notices, technical access requests or technical capability notices. Further, the decision-making criteria set out for technical assistance notices and technical capability notices is too narrow (sections 317P and 317Q(10); sections 317V and 317X(4)), and not present at all for technical access requests. Nor is the scope of what is "*reasonable and proportionate*" defined. Section 317P(a) should be amended to include an obligation that the requirements imposed by any notice is reasonable and proportionate to the legitimate privacy expectations of the subject individual and the Australian community.

14. This lack of detail in the Act shows insufficient "*appropriate safeguards for protecting the rights of individuals*" and this concern is heightened whilst Australia lacks an enforceable Federal human rights framework.

15. It is our submission that the definitions of "*designated communication provider*"[5], "*electronic service*"[6], "*acts or things*"[7] and "*computer*"[8] ought to be significantly narrowed together with providing legislative certainty regarding the manner by which a computer and a designated communication provider's services may be compromised by law enforcement. It is position that the lack of certainty and broad scope of the definition of designated communication provider (including "*acts or things*" and "*electronic services*") and the definition of "*computer*" which seems to be broader than the internet and services associated thereto generally is entirely unacceptable.

16. We also maintain our position that clear and well-articulated definitions must be implemented for "*systemic weakness*", "*systemic vulnerability*" and "*target technology*".

17. The Orwellian and oppressive nature of these provisions and lack of clarity in key definitions stifles innovation, significantly erodes privacy and creates a system where law enforcement is able to covertly monitor Australia (and our international allies) without transparent or readily available recourse.

Warrant Issuance

18. As indicated in the Previous Submissions on Schedule 2 of the Act, we have concerns on the lack of limitations on the proportionality and intrusiveness of computer access warrants under the *Surveillance Devices Act 2004* ("**SDA**"). These are primarily set out by the issuing authority (whether a judge, magistrate, or member of the Administrative Appeals Tribunal (AAT)) when determining the application. The SDA stipulates that when a computer access warrant is sought, the issuing authority "*must have regard to the extent to which the privacy of any person is likely to be affected and the existence of any alternative means of obtaining the evidence or information sought to be obtained.*" This lack of limitations on warrant issuance shows a clear lack of "*appropriate safeguards for protecting the rights of individuals*".

---

[5] Section 317C of the Act.
[6] Section 317D of the Act
[7] Section 317E of the Act
[8] Section 6(1) of the *Surveillance Devices Act 2004* as that definition is amended by the Act and incorporated to the *Mutual Assistance in Criminal Matters Act 1987* and the *Australian Security Intelligence Organisation Act 1979*.

19. In this context, it is relevant to repeat the Court's finding *Big Brother Watch v United Kingdom*, namely that:

> "*Review and supervision of secret surveillance measures may come into play at three stages: when the surveillance is first ordered, while it is being carried out, or after it has been terminated. As regards the first two stages, the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual's knowledge. Consequently, since the individual will necessarily be prevented from seeking an effective remedy of his or her own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding his or her rights. In a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole,* ***it is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure.***[9]"
>
> (our emphasis)

20. It is our position that all provisions implemented by the Act be subject to judicial review. That is, review by a judge where that judge is required to apply independence, impartial and proper procedure to the issuance of TANs, TCNs and Computer Access Warrants. In the interest of clarity, this recommendation can be made very simply: if law enforcement is unable to persuade a judge that an Australian's privacy should be compromised – it certainly should not happen.

The scope of enforcement provisions and the grant of immunities

21. It is our position that the grant of immunities should include journalists, doctors, lawyers, and whistleblowers. Each of these (non-exhaustive) classes deal with confidential, sensitive and privileged information and serve a great public benefit. The need for protection for journalists and their sources has become particularly clear with the recent raids on journalists[10] and this aspect should form a priority area for redress in the Committee's report.

Interaction with intelligence agencies other powers

22. We respectfully consider that the integration with intelligence agencies other powers could be addressed by adopting and meaningfully implementing the recommendations made in the joint civil society submissions and that this question would be best placed in the context of the Act being repealed with a proper consultation occurring in relation to any further proposed Bill.

Interaction with foreign laws, including the United States' *Clarifying Lawful Overseas Use of Data Act*

23. It our understanding that the United States' *Clarifying Lawful Overseas Use of Data Act* (**"CLOUD Act"**) essentially allows the United States to enter an agreement with a qualifying country to circumvent the *Mutual Legal Assistance Treaty* and the protection of rights

[9] Case of *Big Brother Watch & Ors v United Kingdom* (Application Nos.: 58170/13; 62322/14; 24960/15) Judgement at [309].
[10] See for example: https://www.abc.net.au/news/2019-06-05/abc-raided-by-australian-federal-police-afghan-files-stories/11181162; https://www.theguardian.com/australia-news/2019/jun/04/federal-police-raid-home-of-news-corp-journalist-annika-smethurst

contained therein. It is abundantly clear that the Act interacts with foreign law and we refer to committee to the work conducted by the Australian Privacy Foundation on this point[11]

24. It is our position that the Act disproportionately interacts with the CLOUD Act as it:

- fails to provide effective protection of human rights;
- it lacks proper judicial oversight; and
- the fundamental operation of the Act is not transparent.

Impact on industry and competitiveness

25. It is our position that the Act, particularly the lack of clarity in key definitions; stifles innovation, significantly erodes privacy and creates a system where law enforcement is able to covertly monitor Australia (and our international allies) without transparent or readily available recourse. This has a negative impact on industry and competitiveness.

26. By way of short example, we have taken a case study of *Centralized* (www.centralized.me) which is an Australian technology company which produces an innovative web platform for the self-management of independent creatives such as musicians, writers, film makers.

27. We understand that *Centralized* currently employs five people and will be scaling up to fifteen employees later this year following the completion of capital raising. The company's platform by its nature will have detailed and intimate user data. The company's ability to protect the privacy of that data will underpin their reputation for integrity in the eyes of their users and the wider creative community.

> *"The draconian nature of the practical execution of the AA Act as it is currently legislated makes it impossible for us to protect our users' data and maintain that reputation for integrity. The lack of properly qualified and independent judicial oversight of the execution of this legislation by law enforcement is most concerning. In addition it's a display of both ignorance and arrogance by Australia's politicians of the LNP and Labor."*
>
> Brian Dubb, Centralized, CEO.

28. We are informed that, as a direct result of the Act, *Centralized* have relocated the intellectual property of the company to the United States and relocated the research and development to Israel. The company will now not will not hire any Australian developers nor will the company base any operations in Australia.

29. It is our submission that this case study is not unique and that it is highly likely that a significant portion of the Australian technology industry has been required to either relocate, cease development and/or restrict operations. Whilst this may not be a great issue for established technology companies, it is concerning that the uncertainty and potential reputational and business cost associated with the Act has caused an adverse impact on technology confidence in Australia.

---

[11] See: https://privacy.org.au/2019/06/04/report-on-the-international-implications-of-the-telecommunications-and-other-legislation-amendment-assistance-and-access-act-2018/.

Reporting obligations and oversight measures

30. We respectfully repeat our previous submissions and the submissions made herein in relation to authorisation, decision-making and warrant issuance.

31. EFA appreciates the opportunity to make this submission and please do not hesitate to contact Mr Angus Murray should you require any further information or comment.