Riana Pfefferkorn
Associate Director of Surveillance and Cybersecurity
Stanford Center for Internet and Society
Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610
USA
[redacted]

February 14, 2019

Via E-Mail to pjcis@aph.gov.au

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

Re: Comments to Parliamentary Joint Committee on Intelligence & Security on the Telecommunications & Other Legislation Amendment (Assistance & Access) Act 2018

To the Parliamentary Joint Committee on Intelligence and Security:

I am writing to submit comments to the Parliamentary Joint Committee on Intelligence and Security (PJCIS or the Committee) concerning the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (the Act). I am the Associate Director of Surveillance and Cybersecurity at the Center for Internet and Society (CIS) at Stanford Law School in California. I write this letter as a researcher who has studied encryption law and policy for over three years. I am commenting in my personal capacity and do not represent Stanford University, Stanford Law School, or the Center for Internet and Society. My institutional affiliation is provided for identification purposes only. Prior to the Act's passage, I submitted written comments on the then-bill on 9 September, 11 October, 13 November, and 26 November 2018, and testified telephonically at a Committee hearing on the bill on 16 November 2018. This letter pertains to the Act as assented to on 8 December 2018[1] unless otherwise specified.

I was disappointed to see the Assistance and Access Bill pass into law in early December 2018. I and numerous other academics, computer scientists, industry representatives, civil society organizations, and ordinary Australians had cautioned this Committee about the bill's many shortcomings, which need not be rehearsed again here. Yet Parliament rushed the bill into law despite openly conceding its flaws. Federal law enforcement and security agencies immediately began exercising their new powers.[2] It is not publicly known—and maybe never will be—which providers have been served to date with technical assistance/capability notices or requests under the new law, or what the providers have secretly done to their products and services in order to comply.

[1] Available at https://www.legislation.gov.au/Details/C2018A00148.
[2] Ry Crozier, "Home Affairs Says Encryption-Busting Laws Now in Use," ITnews.com.au (Jan. 30, 2019), https://www.itnews.com.au/news/home-affairs-says-encryption-busting-laws-now-in-use-518612; Aimee Chanthadavong, "AA Bill Notices 'Already Issued,'" InnovationAus.com (Feb. 6, 2019), https://www.innovationaus.com/2019/02/AA-bill-notices-already-issued.

As the Committee undertakes the current review, federal agencies are already touting the law's benefits to their investigations.[3] I am sure the new powers have been advantageous to them, though as said, the public is not allowed to know the details. But the new legislation has been equally swift to cause harmful effects as well. The Committee must not look away from these downsides.

As predicted, the new Assistance and Access law has caused immediate and ongoing harm to Australia's technology sector (according to industry leaders), which may ripple out to other sectors as well.[4] A formal inquiry should be convened to evaluate the law's economic effects, as Mr Dreyfus of the PJCIS has suggested.[5] On top of the economic impact, Mr Dreyfus has "all but admitted" that the law, which he voted for, hurts Australians' data security.[6] Those adverse effects risk being felt worldwide, not just in Australia.[7]

These negative trade-offs were foreseeable. A year ago, I published an explanation of how so-called "exceptional-access" mandates pose a significant risk to (among other things) the economic and data-security interests of any country that adopts such a requirement.[8] Now, as the Australian public prepares to go to the polls, the new law's downsides are readily visible to them, whereas they are told to simply accept on faith that the agencies' new powers are secretly keeping them safe.

There is still time to stanch the bleeding. Many submissions to the instant inquiry have already urged the law's repeal.[9] But the Overton window has shifted. "To pass or not to pass," that used to be the question.

---

[3] *Id.*; Paul Smith and Bo Seo, "Atlassian Leads Encryption Law Revolt as Peter Dutton Stands Firm," *Financial Review* (Feb. 11, 2019), https://www.afr.com/technology/web/security/atlassian-leads-encryption-law-revolt-as-peter-dutton-stands-firm-20190207-h1ayk2 (quoting Peter Dutton's claim that "[t]hese new laws have already assisted agencies in the detection and investigation of several major crimes").

[4] Smith and Seo, *supra* n.3 (quoting co-CEO of Atlassian as saying, "We view this legislation as a choke hold on the Australian tech industry," but noting that "the scope of the legislation means [it] could have similarly negative consequences to companies across sectors" beyond tech). *See also* the submissions to the instant PJCIS review by Lee Sinclair (Jan. 14, 2019) (Submission 10), *available at* https://www.aph.gov.au/DocumentStore.ashx?id=e8c9f8cc-cf5d-4677-a3fe-ab9686a666c6&subId=665643; Senetas Corporation Limited (Feb. 11, 2019) (Submission 38) at pp. 1-5, *available at* https://www.aph.gov.au/DocumentStore.ashx?id=9dbf370b-26fb-4a67-a8fc-91f99f1b4a18&subId=666482; and anonymous (no date) (Submission 41), *available at* https://www.aph.gov.au/DocumentStore.ashx?id=ffe63405-7d65-410c-8789-39a5458534e1&subId=666248.

[5] Ry Crozier, "Labor Concedes Decryption Laws Weakened Security for Internet Users," ITnews.com.au (Feb. 12, 2019), https://www.itnews.com.au/news/labor-concedes-decryption-laws-weakened-security-for-internet-users-519203.

[6] *Id.*

[7] Nellie Bowles, "Did Australia Hurt Phone Security Around the World?", *N.Y. Times* (Jan. 22, 2019), https://www.nytimes.com/2019/01/22/technology/australia-cellphone-encryption-security.html (also commenting on the detriment to the Australian tech industry); *see also* Submission by Paweł Głaz (Dec. 21, 2018) (Submission 7), *available at* https://www.aph.gov.au/DocumentStore.ashx?id=0b70bcf8-5707-4bbd-b29d-f1b7f700d9fd&subId=665633.

[8] Riana Pfefferkorn, "The Risks of 'Responsible' Encryption" (February 2018), http://cyberlaw.stanford.edu/publications/risks-responsible-encryption. I previously noted this publication in my September 9, 2018 comments to Home Affairs on the exposure draft of the then-bill. Those comments are available at http://cyberlaw.stanford.edu/files/publication/files/2018-09-09%20Pfefferkorn%20Comments%20to%20Australian%20Govt%20on%20Assistance%20%26%20Access%20Bill.pdf.

[9] *E.g.*, Supplementary Submission by Associate Professor Vanessa Teague and Dr Chris Culnane (no date) (Submission 5), *available at* https://www.aph.gov.au/DocumentStore.ashx?id=8615dd74-acef-4e57-a22e-3103ecec789b&subId=664287; Anonymous submission (no date) (Submission 6), *available at* https://www.aph.gov.au/DocumentStore.ashx?id=b806b34c-a21b-401e-b922-bc3a8fff2e1d&subId=664589; Submission by Mr Jake Bloom (Dec. 18, 2018) (Submission 9), *available at* https://www.aph.gov.au/DocumentStore.ashx?id=b9e21592-5d73-45b5-9427-a73ab157a1f3&subId=664629; Submission by Mr Justin Warren (no date) (Submission 12), *available at* https://www.aph.gov.au/DocumentStore.ashx?id=ee360507-abeb-49ce-89b1-5a1b6d73a760&subId=665836; Anonymous submission (no date) (Submission 13), *available at* https://www.aph.gov.au/DocumentStore.ashx?id=b17a4bb2-355b-42c9-8e58-f42976c24cc2&subId=665881; Anonymous submission (no date) (Submission 19), *available at* https://www.aph.gov.au/DocumentStore.ashx?id=e4b7be81-c842-41a4-97ea-27fb28505d21&subId=665996; Submission by Dr Joe Zucco (no date) (Submission 22), *available at* https://www.aph.gov.au/DocumentStore.ashx?id=47b89b27-ec0e-448f-ac2d-e41af8b51c97&subId=666408; Submission by

Now that the bill has passed into law, it appears that members of Parliament are treating that decision as irreversible. Repealing the law, full stop—restoring the *status quo ante*—does not seem to be among the options under consideration. Instead, the debate now focuses on how to amend the law. But when a ship is on a collision course with an iceberg, it does not matter how the deck chairs are arranged.

Sincerely,

[redacted]

Riana Pfefferkorn
Stanford Center for Internet and Society
559 Nathan Abbott Way
Stanford, CA 94305
USA

[redacted]

Mr Andrew Tyson (Jan. 14, 2019 (Submission 23), *available at* https://www.aph.gov.au/DocumentStore.ashx?id=5e714b28-9cf0-40c6-a7ee-7edd7b9e6d5e&subId=666150; Submission by Dr Peter Serwylo (no date) (Submission 24), *available at* https://www.aph.gov.au/DocumentStore.ashx?id=80422206-8ad8-4a80-b139-67c096c256ae&subId=666320; Submission by Mr Peter Jardine (Feb. 9, 2019) (Submission 28), *available at* https://www.aph.gov.au/DocumentStore.ashx?id=612213e9-ba84-4a89-9e99-965ca809914e&subId=666429; Submission by Pirate Party Australia (Feb. 8, 2019) (Submission 31), *available at* https://www.aph.gov.au/DocumentStore.ashx?id=7f499ec1-df49-4dbf-99c4-31a1d29e1d1a&subId=666412; Submission by Mr Peter Young (no date) (Submission 34), *available at* https://www.aph.gov.au/DocumentStore.ashx?id=d73469f5-2e66-46ee-b18c-86b8acc0c3c6&subId=666439; Submission by Kosmas Stergiou (Feb. 11, 2019) (Submission 35), *available at* https://www.aph.gov.au/DocumentStore.ashx?id=77546dbb-ae3e-4147-a3ff-0f00101c18ef&subId=666448; Submission by Senetas Corporation Limited (Feb. 11, 2019) (Submission 38) at p.2, *available at* https://www.aph.gov.au/DocumentStore.ashx?id=9dbf370b-26fb-4a67-a8fc-91f99f1b4a18&subId=666482; Anonymous submission (no date) (Submission 42), *available at* https://www.aph.gov.au/DocumentStore.ashx?id=1db5347b-5f23-43b6-9798-45290533658c&subId=666430.