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
+1 (650) 721-1491
riana@law.stanford.edu

June 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 PJCIS on its Review of the Amendments Made by the Telecommunications & Other Legislation Amendment (Assistance & Access) Act 2018

To the Parliamentary Joint Committee on Intelligence and Security:

I write to submit comments to the Parliamentary Joint Committee on Intelligence and Security (PJCIS or the Committee) concerning its review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (the Act).[1] 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, and as someone who believes in a robust free press. I write 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. I have submitted other written comments on the Act both before and after its passage, on 9 September, 11 October, and 13 and 26 November 2018 and on 14 February 2019, plus telephonic testimony on 16 November 2018. This letter pertains to the Act as assented to on 8 December 2018[2] unless otherwise specified.

The Committee has stated that its present review will focus on the following seven aspects:

1. the threshold, scope and proportionality of powers provided for by the Act;
2. authorization processes and decision-making criteria;
3. the scope of enforcement provisions and the grant of immunities;
4. interaction with intelligence agencies' other powers;
5. interaction with foreign laws, including the United States' Clarifying Lawful Overseas Use of Data Act (CLOUD Act);
6. impact on industry and competitiveness; and

[1] *See* Review of the Amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/AmendmentsTOLAAct2018.
[2] Available at https://www.legislation.gov.au/Details/C2018A00148.

7. reporting obligations and oversight measures.[3]

Most of my previous submissions have focused on the cybersecurity ramifications of the Act. I don't see "impact on security" on the list of things the Committee is interested in hearing about, so I'll confine my comments to the listed focus areas instead. I have covered some of those in earlier submissions, but I would like to make some additional comments to account for developments in Australia since my last submission four months ago. These comments will discuss focus areas **#4, #5, #6, and #7.** Let's start with the recent attacks on freedom of the press in Australia **(#4, #5, and #7)**, then move on to the economy **(#6)**.

As the Committee is aware, earlier this month the Australian Federal Police (AFP) began investigating journalist Ben Fordham, raided the home of journalist Annika Smethurst (which included a search of her mobile phone, computer, and her underwear drawer), and raided the headquarters of the Australian Broadcasting Corporation (ABC).[4] The AFP's actions are deeply troubling. They appear intended to intimidate both the targeted journalists and all their Australian colleagues, to chill the press's willingness to investigate and inform the Australian public about newsworthy topics of legitimate public concern. Unsurprisingly, the raids quickly drew condemnation from both within and outside of Australia.[5] They are relevant to this Committee's review because they implicate at least three of the review's focus areas: **#4, interaction with agencies' other powers; #5, interaction with the CLOUD Act; and #7, reporting obligations and oversight measures.**

#4: Interaction with agencies' other powers.[6] While the AFP's actions are widely considered an abomination, they were not, in the most literal sense of the word, lawless—because Parliament in recent years had changed the law to allow them. The authorizations for AFP's actions came from the Act and other legislation passed in recent years in the name of national security. Thanks to new powers granted by Schedule 3 of the Act, the warrant to ABC allowed the AFP to "add, copy, delete or alter" material on the ABC's computers.[7] That is, the police had authorization to change, tamper with, even destroy other ABC computer files, so long as they could say it was necessary to get access to the data they were seeking.[8]

---

[3] *See* Terms of Reference, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/AmendmentsTOLAAct2018/Terms_of_Reference.

[4] Rebecca Ananian-Welsh, "Why This Week's Raids on Australian Media Present a Clear Threat to Democracy and Press Freedom There," NiemanLab (June 6, 2019), https://www.niemanlab.org/2019/06/why-this-weeks-raids-on-australian-media-present-a-clear-threat-to-democracy-and-press-freedom-there/; John Lyons, "Australia Is at War with Journalists," *Washington Post* (June 10, 2019), https://www.washingtonpost.com/opinions/2019/06/10/australia-is-war-with-journalists/?utm_term=.be258e765e58.

[5] *E.g.*, Shannon Molloy, "Radio Star Ben Fordham Targeted After Australian Federal Police Raid Political Editor Annika Smethurst's Home over Spy Story," News.com.au (June 4, 2019), https://www.news.com.au/national/politics/australian-federal-police-raid-political-editor-annika-smethursts-home-over-spy-story/news-story/135c27ced2becde0333c0ef61d901007 ("The 'heavy-handed' raid of Smethurst's home this morning by several AFP offices has sparked widespread outrage."); Jamie Tarabay, "Australian Police Raids Target News Media over Leaked Documents," *N.Y. Times* (June 4, 2019), https://www.nytimes.com/2019/06/04/world/australia/journalist-raid-annika-smethurst.html ("The Australian union for journalists, the Media, Entertainment and Arts Alliance, called it 'an outrageous attack on press freedom.'"); Matt Ford, "Australia's Media Raids and the Decline of Press Freedom Worldwide," *New Republic* (June 6, 2019), https://newrepublic.com/article/154091/australias-media-raids-decline-press-freedom-worldwide ("It's not unusual for journalists to face such treatment in more authoritarian countries, which makes it especially disturbing to see them subjected to it in a free nation like Australia. It shows that even liberal-democratic governments will use their power to suppress legitimate journalism").

[6] Technically this item says only "intelligence agencies." *See* Terms of Reference, *supra* n.3. It is not clear whether this phrasing was intended to omit domestic law enforcement agencies, but those are the focus of my comments here regardless.

[7] Stilgherrian, "Huge Scope of Australia's New National Security Laws Reveals Itself," ZDNet (June 6, 2019), https://www.zdnet.com/article/huge-scope-of-australias-new-national-security-laws-reveals-itself/.

[8] *See* Assistance and Access Act Schedule 3 (adding subsection 3F(2A)(b) to the Crimes Act 1914).

What data, then, were they after? One of the AFP's overt goals seems to have been discovering journalists' confidential sources. "There is widespread recognition in international agreements, case law and declarations that protection of journalists' sources is a crucial aspect of freedom of expression that should be protected by all nations."[9] Nevertheless, thanks to Australian law including the Act, the Australian authorities were empowered to disregard that international consensus.

In an article about the raids, law lecturer Dr Rebecca Ananian-Welsh pointed out that the Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 permits "access to a professional journalist's metadata in order to identify a confidential source"; consequently, after 2015, "journalists were advised to avoid using their mobile devices in source communications … [and] wherever possible, to encrypt communications."[10] But, Dr Ananian-Welsh observed, the Assistance and Access Act makes it even harder for journalists to communicate with their sources without jeopardizing their confidentiality, thanks to the Act's provisions for forcing telecommunications providers and other entities to assist investigators in decrypting communications.[11] "This week's raids suggest the Australian Federal Police would be prepared to target journalists under this framework in order to identify journalists' confidential sources," she wrote.[12]

In short, law enforcement's powers granted under the Data Retention Act in 2015 were augmented by the new powers the Assistance and Access Act provided at the end of 2018, creating the framework that authorized the federal police in mid-2019 to raid the homes and offices of journalists over articles published in July 2017 and April 2018, in defiance of international norms.[13] Because Parliament passed these laws—on the recommendation of this Committee[14]—the federal police had the power to strike a chilling blow against press freedom in Australia, and call it lawful.

#7: Reporting obligations and oversight measures. In a recent report, the Parliamentary Joint Committee on Law Enforcement (whose membership has some overlap with this Committee) "acknowledge[d] the public debate" over the Act in regard to whether it strikes "the most appropriate balance between law enforcement powers and human rights," and it "consider[ed] that the powers given to law enforcement agencies must be subject to regular monitoring to ensure that the legislative and regulatory framework is … respecting the human rights and fundamental freedoms of Australians."[15] By now, it should be clear to both committees that the current legislative landscape, the Act included, has allowed that balance to tilt dangerously in favor of law enforcement and away from human rights and freedoms.

The AFP's thuggish attacks on press freedom did not occur in a vacuum. They are only the latest and most egregious example of how Australian agencies have already been emboldened to interpret and apply national-security legislation such as the Act in ways this Committee might, when recommending a bill's passage, have thought beyond the pale. To take another example, last month it came out that Home Affairs interprets the Act's definition of "designated communications providers" to mean that even fast-food joints

[9] David Banisar, Privacy International, *Silencing Sources: An International Survey of Protections and Threats to Journalists' Sources* (2007), p. 12, *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1706688.
[10] Ananian-Welsh, *supra* n.4.
[11] *Id.*
[12] *Id.*
[13] *See* Tarabay, *supra* n.5.
[14] *See* PJCIS, Report, *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (Feb. 27, 2015), pp. 251-58, *available at* https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Data_Retention/Report.
[15] Parliamentary Joint Committee on Law Enforcement, Report, *Impact of New and Emerging Information and Communication Technology* (April 2019), ch. 4, ¶¶ 4.47, 4.49, *available at* https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Law_Enforcement/NewandemergingICT/Report (hereafter PJCLE Report).

can be dragooned into helping agencies carry out surveillance.[16] This is hard to reconcile with earlier claims by agencies that the Act is narrowly targeted, such as the assertion by the head of the Signals Directorate that the Act "was designed to target terrorists, paedophiles and criminals, not law-abiding Australians."[17] During its review last year, did the Committee anticipate that the Act would allow snooping on Australians who browse the Internet while enjoying a hamburger? When evaluating the Data Retention Act five years ago, did the Committee foresee police rifling through a female journalist's underwear drawer?

These examples underscore the need to meaningfully monitor and oversee how agencies are using the powers granted under the Act and other national security legislation. Already there is a disturbing trend toward overreach. Parliament must take action to right the ship, and soon.

I am hardly the first one to call for reform: following this month's raids, Labor called upon this Committee to conduct an inquiry into press freedom. Specifically, it asked you "to investigate whether the balance between press freedom and national security is right in legislation passed since the conservative government was first elected in 2013."[18] That legislation (which Labor voted for too) includes the Data Retention Act and the Assistance and Access Act.

This Committee would be well advised to take a hard look at the decline of press freedom in Australia. You enabled that decline by approving laws such as the Assistance and Access Act and the Data Retention Act that expanded Australian law enforcement and intelligence agencies' powers in recent years, to the predictable detriment of Australians' rights. Now you must reckon with the role you played.

Freedom of the press is an integral component of freedom of expression; freedom of expression is a human right.[19] Not only do journalists have the right to engage in investigation and reporting without interference or reprisal from government, their audiences—everyday people attempting to keep informed about current affairs—have the right to receive that information without censorship by the state. The AFP's investigations and raids, empowered by the Act and other national security legislation of recent years, are a grave threat to those rights. They must not be allowed to continue.

I am reminded of the Committee Chair's words during one of the Committee hearings on the Act before its passage. He repudiated any comparison between Australia and China, which he said has "a totalitarian government, as opposed to ours, which is a liberal democracy with all the appropriate safeguards that make us distinct [from China] … [T]here's no equivalence in the character of our government, nor our institutions."[20]

Frankly, it becomes harder to resist that comparison when federal police agents are raiding journalists' homes and offices in response to their news reporting, seizing reams of files and hunting after confidential sources, under the auspices of laws designed to give ever-freer rein to the police and intelligence

[16] Paul Karp, "Spies with That? Police Can Snoop on McDonald's and Westfield Wifi Customers," *The Guardian* (May 28, 2019), https://www.theguardian.com/business/2019/may/28/spies-with-that-police-can-snoop-on-mcdonalds-and-westfield-wifi-customers.
[17] PJCLE Report, *supra* n.15, ch. 4, ¶ 4.26.
[18] Rod McGuirk and Nick Perry, "Australian Opposition Calls for Review of Press Freedom," *Washington Post* (June 12, 2019), https://www.washingtonpost.com/world/the_americas/australian-opposition-calls-for-review-of-press-freedom/2019/06/12/0a2cfbc6-8cdf-11e9-b6f4-033356502dce_story.html?utm_term=.d9580ffbad83.
[19] *See* Universal Declaration of Human Rights, Art. 19, *available at* https://www.un.org/en/universal-declaration-human-rights/.
[20] Statement of Mr Andrew Hastie (p. 4), as transcribed in the Proof Committee Hansard, Parliamentary Joint Committee on Intelligence and Security, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, Canberra, ACT (Nov. 30, 2018), *available at* https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;adv=yes;db=COMMITTEES;id=committees%2Fcommjnt%2Fb9247c77-dfa4-44bb-8aa3-ce6bc01d20ca%2F0001;orderBy=priority,doc_date-rev;query=Dataset%3AcomJoint%20Decade%3A%222010s%22%20Year%3A%222018%22%20CommitteeName_Phrase%3A%22parliamentary%20joint%20committee%20on%20intelligence%20and%20security%22;rec=4;resCount=Default.

services, and justifying their outlandish conduct by invoking national security—the implication being that the state considers it a threat to national security for the public to know what its government has been up to. Had the foregoing description of the AFP's actions been presented to any one of you, and you had been asked to name the country where you suspect it happened, which would come to your mind first: Australia—or China?

#5: Interaction with the U.S. CLOUD Act. Restoring press freedom would have international ramifications for Australia as well as domestic. I previously addressed the topic of the U.S. CLOUD Act in my written comments of 13 November 2018 and my telephonic testimony of 16 November 2018. During that testimony, Mr Mark Dreyfus noted that Australia's eligibility for a CLOUD Act agreement with the U.S. is contingent upon whether Australian law, "including the implementation of that law, affords robust substantive and procedural protections for privacy and civil liberties in light of the data collection and activities of" the Australian government.[21] This is to be evaluated by factors including "adhere[nce] to applicable international human rights obligations and commitments or demonstrate[d] respect for international universal human rights, including … protection from arbitrary and unlawful interference with privacy … [and] freedom of expression."[22] The question is whether, in light of the Act (and its other law), Australia can meet that eligibility bar.

Six months after the Act's passage, with an unprecedented series of raids on the press currently defining Australia's public image on the world stage, the answer is not as clear as Parliament might like. If current trends continue, Australia can expect to have a harder time persuading the U.S. government that its law (both as written and as implemented) protects human rights, privacy, and civil liberties to the degree necessary under the CLOUD Act. Ideally, of course, it would not take the dangled carrot of a CLOUD Act agreement to induce the Government to act to protect journalism in Australia (particularly as this would trade privacy for press freedom, as though that must be a zero-sum game). The AFP's conduct is unacceptable in a liberal democracy, full stop. But if Parliament wants a CLOUD Act agreement with the United States, it would do well to bring the AFP to heel and re-evaluate its national-security legislation framework, including the Data Retention Act and the Assistance and Access Act.

#6: Impact on industry and competitiveness. Finally, while the AFP raids are top of mind at present, the intervening months since the Act's passage have not lessened my concerns about the Act's economic consequences. I previously addressed this issue in my written comments of 14 February 2019. The foreseeable damage to the economic interests and reputation of Australia's tech sector has only continued to play out in the intervening four months.

The Shadow Minister for the Digital Economy lamented in May that the Act "is having a devastating impact locally" on Australian technology firms.[23] During a March trip to Canberra, Microsoft's president and chief legal officer stated that Microsoft's customers have begun asking for their data to be stored elsewhere because they are "no longer comfortable" having it stored in Australia in light of the Act.[24] That same month, a venture capital investor noted that not only are Australians unwilling to buy Australian-made technology, the rest of the world is also hesitant to "buy Australian." He attributed this reluctance to the Act as well as the February cyberattack against Australian politicians, which portrayed Australia as unsophisticated (and thus

[21] Statement of Mr Mark Dreyfus (p. 7), as transcribed in the Proof Committee Hansard, Parliamentary Joint Committee on Intelligence and Security, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, Sydney, NSW (Nov. 16, 2018), *available at* https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;db=COMMITTEES;id=committees%2Fcommjnt%2F25a9cf03-e38f-491b-a5d7-b371811b8181%2F0002;query=Id%3A%22committees%2Fcommjnt%2F25a9cf03-e38f-491b-a5d7-b371811b8181%2F0000%22.

[22] CLOUD Act, 18 U.S.C. § 2523 (b)(1)(B)(iii).

[23] Asha Barbaschow, "Husic Says Labor Is Committed to Reforming Australia's Encryption Laws," ZDNet (May 14, 2019), https://www.zdnet.com/article/husic-says-labor-is-committed-to-reforming-australias-encryption-laws/.

[24] Paul Karp, "Tech Companies Not 'Comfortable' Storing Data in Australia, Microsoft Warns," *The Guardian* (Mar. 27, 2019), https://www.theguardian.com/technology/2019/mar/27/tech-companies-not-comfortable-storing-data-in-australia-microsoft-warns.

untrustworthy) on cybersecurity.[25] "If you set yourselves up as the place least welcoming to cybersecurity practitioners in the world, it's definitely going to make it harder to build great cybersecurity businesses … [M]any other places don't have similar [regulatory] challenges," he said.[26]

In short, the Act is hurting Australian companies, spooking both current and potential customers, and making other countries look like more attractive options for doing business. If the Government wants to help Australia's young cybersecurity sector become a global leader by closing the gaps in innovation, exports, and skills training,[27] it can ill afford to give with one hand while taking away with the other.

* * *

I appreciate that the Committee has focused its review on seven specific aspects of the Act identified in the Terms of Reference. I have addressed the foregoing comments to four of the seven accordingly. No doubt other submissions will add more noteworthy concerns about those points and the other three as well. But one should not miss the forest for the trees. I remain of the opinion (expressed in my 14 February 2019 comments) that amending one or another facet of the Act will not suffice. The Assistance and Access Act should be repealed.

Sincerely,

Riana Pfefferkorn

Riana Pfefferkorn
Stanford Center for Internet and Society
559 Nathan Abbott Way
Stanford, CA 94305
USA
Tel: +1 (650) 721-1491
Fax: +1 (650) 725-4086
riana@law.stanford.edu

[25] Asha Barbaschow, "Australia Isn't Buying Local Cyber and the Rest of the World Might Soon Follow," ZDNet (Mar. 13, 2019), https://www.zdnet.com/article/australia-isnt-buying-local-cyber-and-the-rest-of-the-world-might-soon-follow/.
[26] *Id.*
[27] *See* Catherine Chapman, "Australia Releases Second Round of Funds to Boost Cybersecurity Sector," *The Daily Swig* (June 7, 2019), https://portswigger.net/daily-swig/australia-releases-second-round-of-funds-to-boost-cybersecurity-sector.