Stanford Law School

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

November 26, 2018

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

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

Re: Supplemental Letter to Parliamentary Joint Committee on Intelligence & Security on the Telecommunication & Other Legislation Amendment (Assistance & Access) Bill 2018

To the Parliamentary Joint Committee on Intelligence and Security:

I am writing to follow up on my recent testimony before the Parliamentary Joint Committee on Intelligence and Security (PJCIS or the Committee) concerning the Telecommunication and Other Legislation Amendment (Assistance and Access) Bill 2018 (the Bill). 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 the past 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. Previously, I submitted written comments on the Bill on 9 September, 11 October, and 13 November 2018, and testified at a Committee hearing on the Bill on 16 November 2018. This letter pertains to the first-reading draft of the Bill of 20 September 2018[1] unless otherwise specified.

I write to express my concern about a proposal for enabling swift passage of certain parts of the Bill. Following the recent terror attack and disrupted terror plot in Melbourne, the Home Affairs Minister[2] and the Prime Minister[3] have exhorted the Committee to expedite its review of the Bill. Their goal is to see the Bill passed by Parliament before it rises for the year on 6 December—just a few short days from now. While I am sympathetic to law enforcement's mission to protect Australians from terror threats, I urge the Committee not to be swayed by the atmosphere of urgency that Messrs. Dutton and Morrison are trying to whip up. The Committee's deliberations must be allowed to run their course.

[1] As available in PDF at https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r6195_first-reps/toc_pdf/18204b01.pdf;fileType=application/pdf. Citations to page numbers refer to this PDF's numbering.
[2] Chris Duckett, "Dutton Leans on Encryption Laws Committee to Hurry Up," ZDNet (Nov. 20, 2018), https://www.zdnet.com/article/dutton-leans-on-encryption-laws-committee-to-hurry-up/.
[3] Chris Duckett, "Australian PM Insists on Encryption-Busting Bill Being Passed in Next Sitting Fortnight," ZDNet (Nov. 22, 2018), https://www.zdnet.com/article/australian-pm-insists-on-encryption-busting-bill-being-passed-in-next-sitting-fortnight/.

It would be extremely ill-advised to rush headlong into passing such a large and complex piece of legislation. The Bill has serious ramifications for Australia's national security, economic and trade interests, international alliances, and the rights of its people. Those interests should not be steamrolled in response to the regrettable incidents in Melbourne. Even after the mass shooting in San Bernardino, California, three years ago—then the worst terror attack on U.S. soil since 11 September 2001—Congress declined to pass legislation mandating exceptional access for law enforcement to encrypted smartphones, despite the centrality of such a device in the "Apple vs. FBI" court battle that followed the attack.[4] Cooler heads prevailed.

Nor should the Committee truncate its review just because the Christmas break is coming up for Parliament and for holidaying Australians. Mr. Duncan Lewis of ASIO admitted, upon questioning during yesterday's hearing, that there is no specific Christmas threat at present. Stoking fears of an unspecified danger, and manufacturing a sense of urgency to rush through a Bill that has been in the works for a year and a half, are incompatible with the careful deliberation, debate, and (as I think the Committee recognizes) extensive amendments that the Bill requires. I believe the Committee understands that, and thus I appreciate that it appears committed to proceeding with the scheduled hearings between now and 4 December.

Nevertheless, I am alarmed by news reports that the Hon. Mark Dreyfus has proposed a potential compromise to enable swift passage of parts of the Bill during the current parliamentary sitting while reserving the remainder of the Bill for further consideration.[5] In yesterday's hearing, Mr. Dreyfus suggested "interim processing of part of the bill in order that the government's stated purpose of urgency can be served." The idea would be for the Committee's report to "hypothetically support conferring the powers outlined in the bill on agencies conducting counter-terrorism operations, such as ASIO, while other agencies, such as a number of anti-corruption bodies, would not receive new powers."

This proposal will not work as intended. It would not serve the (over-)stated "purpose of urgency," and its effect would not be limited solely to the context of counter-terrorism.

First, even if the Bill passes on 6 December (the last day Parliament sits for the year), an urgent demand would not be met with immediate compliance—certainly not in the 19 days between then and Christmas! That is true for both technical and legal reasons. On the technical side, technology companies cannot turn on a dime. There is an unfortunate tendency among legislatures and courts to ascribe something approaching omnipotence to technology companies, particularly the larger ones. But they are not wizards who can wave a magic wand and instantly do anything a government desires. At present, providers covered by the Bill have implemented their products and services' encryption designs and other security features in a way that would likely require extensive re-engineering if they were to be served (and decided to comply) with a technical capability notice (TCN), or even a technical assistance notice (TAN) or request (TAR). And, as I have pointed out previously, even if they were to work at top speed to comply, such a rushed, high-pressure atmosphere would likely result in their doing a sloppy job—with all the security risks that entails.

On the legal side, to the extent a compromise Bill's powers would be aimed at U.S. providers, the reality of the legal landscape is at odds with "the government's stated purpose of urgency." You have heard my testimony and read my 13 November submission regarding the U.S. CLOUD Act. As I said, Australia currently must go through the months-long MLAT process (or the letters rogatory process) in order to get data from U.S. providers; there is no CLOUD Act agreement in place that would allow Australia to circumvent the MLAT; TARs are barred by U.S. law; and I do not believe TANs/TCNs could validly be served either through the MLAT or a putative CLOUD Act agreement. None of that will change just because of a hastily-passed compromise Bill. The fog of urgency in Canberra simply will not extend to the United States.

[4] Dustin Volz, Mark Hosenball, Joseph Menn, "Push for Encryption Law Falters Despite Apple Case Spotlight," Reuters (May 27, 2016), https://www.reuters.com/article/usa-encryption-legislation-idUSL2N18O0BM.
[5] Rohan Pearce, "Compromise Could See Quick Passage for Parts of Encryption Bill," Computerworld (Nov. 26, 2018), https://www.computerworld.com.au/article/650034/compromise-could-see-quick-passage-for-parts-of-encryption-bill/.

Second, it is a fallacy that a compromise Bill would apply only to "counter-terrorism operations." Again, this is true for both technical and legal reasons. On the technical side, it is not possible for a provider to let the agencies make use of (*i.e.*, in response to a TAN or TAR) or to newly build (*i.e.*, in response to a TCN) a capability that can be used *only* by particular agencies *only* for counter-terrorism investigations. There simply is no such thing as exceptional access "just for the good guys," or even for just one subset of the good guys investigating one subset of offenses. Once built, the security weakness—for that is what a "capability" is—would be exploitable by anyone,[6] and any knock-on effects from the provider's compliance (as I have discussed in past submissions) could occur, notwithstanding the intent to circumscribe the compromise Bill.

On the legal side, it is fatuous to expect that powers conferred solely for certain agencies' counter-terrorism operations will stay confined to that context and those agencies. Australia's law enforcement and intelligence agencies have taken liberties with their powers (and limitations) under existing Australian law, and they inevitably would do the same with the proposed compromise Bill—or, for that matter, the full Bill as it stands. As said, a capability built for one purpose can be used for other purposes. If an agency such as ASIO requires a provider to build a capability for a counter-terrorism investigation, what is to stop other agencies (federal, state, or territory) from demanding the provider use the capability in some non-terrorism-related context? There is precedent for this, as the CEO of the Communications Alliance testified in the 19 October hearing. Federal law specifies 22 agencies that can seek telecommunications data, and yet in reality, "we have seen some authority creep"; "there are many more than 22 agencies because … many state based agencies have come forward and started using their own state based powers to request metadata" under that law.[7] A Bill ostensibly limited to counter-terrorism investigations would see similar creep. What is more, even the agencies that *do* pursue counter-terrorism operations have at times taken a very expansive view of what falls within their remit.[8] Is the price of shrimp in Jakarta in-scope for the proposed compromise Bill?

In sum: Please do not be railroaded into a hasty compromise that won't even achieve its stated goals.

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

[6] *See, e.g.*, Max Eddy, "What It's Like When The FBI Asks You To Backdoor Your Software," PCMag (Jan. 8, 2014), http://securitywatch.pcmag.com/security/319544-what-it-s-like-when-the-fbi-asks-you-to-backdoor-your-software (quoting Nico Sell, CEO of encrypted-messaging app Wickr, saying "It was very clear that a backdoor for the good guys is always a backdoor for the bad guys.").

[7] Testimony of Mr. John Stanton, Communications Alliance (p. 42), 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 (Oct. 19, 2018), *available at* https://parlinfo.aph.gov.au/parlInfo/download/committees/commjnt/2a1771c8-f314-43f2-b9b0-cd09ad8123ae/toc_pdf/Parliamentary%20Joint%20Committee%20on%20Intelligence%20and%20Security_2018_10_19_6680.pdf;fileType=application%2Fpdf#search=%22committees/commjnt/2a1771c8-f314-43f2-b9b0-cd09ad8123ae/0000%22.

[8] *See* "Australia's Gone Too Far Spying on Shrimp Trade Talks, Indonesia Says," Reuters (Feb. 17, 2014), https://www.telegraph.co.uk/news/worldnews/asia/indonesia/10643265/Australias-gone-too-far-spying-on-shrimp-trade-talks-Indonesia-says.html.