Stanford Law School

Riana Pfefferkorn
Cryptography Fellow
Stanford Center for Internet and Society
[redacted]

September 9, 2018

Via E-Mail to [redacted]

Australian Government
Department of Home Affairs
[redacted]
Australia

Re: Comments on Exposure Draft of Assistance and Access Bill 2018

To Whom It May Concern:

Thank you for the opportunity to submit comments on the Government's exposure draft of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (the Bill). I am an American attorney and researcher working primarily on encryption policy. For the past three years, I have been the Cryptography Fellow at the Center for Internet and Society at Stanford University's Law School, located in California's Silicon Valley. In that role, I focus on investigating and analyzing the U.S. and other governments' policies and practices for forcing decryption and/or influencing crypto-related design of online platforms and services, devices, and products, both via technical means and through the courts and legislatures. I also research the benefits and detriments of strong encryption on free expression, political engagement, economic development, and other public interests. In addition, during the past academic year I co-taught a course on cybersecurity at the University.

As an initial matter, I would like to voice my strong agreement with the comments submitted by a group of organizations including New America's Open Technology Institute (OTI), the Electronic Frontier Foundation (EFF), and Access Now. The Government would do well to heed their cogent feedback on the Bill. I intend for my comments below to complement and expound upon some of their points about the Bill's potential ramifications for computer security.

Introduction

Like OTI *et al.*, I appreciate the Bill's express statement in Section 317ZG that providers cannot be required "to implement or build a systemic weakness, or a systemic vulnerability, into a form of electronic protection" (such as encryption). The Explanatory Document explains that this language constitutes "a prohibition on building a new decryption capability or actions that would render systemic methods of authentication or encryption less effective." (§ 317ZG, p. 47).[1] This statement reflects an important

[1] Unless otherwise specified, citations to sections alone refer to the text of the exposure draft, whereas citations to page numbers refer to the Bill's Explanatory Document published in August 2018 by the Government's Department of Home Affairs. Many thanks to Mr. Adam Ingle of that Department for providing a hard copy of the Explanatory Document to me.

acknowledgement by the Government that mandating "so-called 'backdoors'" would pose an unacceptable risk to "the fundamental security of systems and products" (*id.*) and to concomitant personal safety, privacy, economic, national security, and other interests.

Nevertheless, the Bill's attempt to limit its adverse computer security impact is undermined by the Government's cramped definition of "systemic." Specifically, the Explanatory Document interprets "systemic" to exclude "actions that weaken methods of encryption or authentication on a particular device/s." (*Id.*). Pursuant to that carve-out, the Government says the Bill would permit "requir[ing] a provider to enable access to a particular service, particular device or particular item of software, which would not systemically weaken those products across the market." (*Id.*).

This overlooks the potential for seemingly "one-off" instances of compelled technical assistance to have broader effects. In truth, the Bill's "no 'systemic' weaknesses" provision is not the strong safeguard it might seem to be. It would not pose a meaningful barrier to misuse and abuse of the forensic capabilities the Bill would empower the Government to order providers to create. The Bill risks forcing technology companies to create insecure versions of their products and services that, while ostensibly limited to a single incidence, in fact open the door to the very systemic vulnerabilities the Bill professes to avoid.

1. The Volume of "Particular" Assistance Demands Will Necessitate an Effectively "Systemic" Approach by the Provider.

The Government ignores the reality of how providers would likely choose to comply with technical assistance/capability notices. In the Explanatory Document, the Government reasons that compelling a provider to implement a device-specific access capability (*e.g.* via one of the "listed acts or things" in § 317E) "will not necessarily mean that a systemic weakness has been built." (§ 317ZG, p. 47). This is a troublingly dismissive attitude,[2] and it misunderstands the likely implementation of supposedly device-specific access solutions by providers. If a provider is forced to enable access to a "particular service, particular device or particular item of software" (*id.*), there is a significant chance that the provider's "one-off" solution in fact will *not* be limited to the specific device.

The Bill's allowance for compelled "particular" device access is likely, in actual practice, to induce providers to create "systemic" access solutions even though the Bill would not require them to do so. Australian law enforcement and security agencies will foreseeably amass a large number of devices to which they will require providers to grant them access. Since the Bill forswears a systemic backdoor requirement, it follows that Australian investigators will instead repeatedly importune providers for "one-off" access to every single device. Consequently, to render prompt, efficient access to numerous "particular" devices at scale, providers will need to come up with a solution that is effectively "systemic."

What is more, Australian agencies will not be the only ones demanding access. Australia's Bill, with its technical assistance/capability notice model, will prompt similar legislation and/or demands from other governments as well. Many governments besides Australia's will take a keen interest in the access solutions providers will have to create at the Government's behest. Governments of other countries where providers sell their devices or offer their software or services will want the same treatment the providers will have given to Australia's Government. The number of technical assistance demands served on the providers will multiply accordingly.

The upshot is that providers are unlikely to build from scratch, and then dispose of, a custom, tailored solution to access each particular device, every time they are served with a government access demand. Developing software is complicated, time-consuming, and costly. It would be expensive and difficult for a

[2] Not least because the Explanatory Document provides no reassurances that the Government will take heed of providers' assertions about "[t]he nature and scope of any weaknesses and vulnerabilities" during consultation with the provider. (*See id.*).

provider to build a custom access solution for a "particular" device. But once built, it could be trivial for the provider to change it to work on any other instance of its product. Given the demand, the provider would keep the "one-off" solution on hand and then either modify it for each of the many devices covered by future technical assistance/capability notices, or, more likely, create a solution that does not tie the access capability to one particular device.

In sum, the provider's solution to accessing a "particular" device in compliance with a supposedly one-off technical assistance/capability notice probably will neither be tied to the specific device, nor be deleted after use. Such an effectively "systemic" solution would be the only practical way for the provider to keep pace with the voluminous notices for "particular" devices that the provider would constantly be receiving from Australia and other governments.

The Government must recognize that the foreseeable real-world consequences of the Bill would largely vitiate Section 317ZG's "systemic" limitation. At best, this reality suggests that Explanatory Document's explanation of the limitation is simply public-relations puffery intended to mollify the Australian public's well-founded concerns about the Bill. At worst, it reflects a serious misunderstanding of computer security on behalf of the Government.

2. The Software for Enabling Government Access Is Likely to Contain Vulnerabilities, Which May Have a "Systemic" Impact.

There is no guarantee that providers will be able to implement one-off access to a particular device or service without any vulnerabilities in the implementation. The reality of software development is that creating software (especially secure software) is complex. Vulnerabilities are common in software code, despite providers' best efforts. To address this problem, providers employ rigorous, extensive pre-release testing; after-the-fact audits, including by independent security researchers; and regular updates. Even so, none of these practices, alone or in concert, can ensure that software will not be vulnerable and subject to misuse.

Where the Government serves a technical assistance/capability notice on a provider, any software the provider develops to comply with the notice (or that the Government supplies to the provider, *see* § 317E(1)(c)) is unlikely to go through this testing/audit/update lifecycle. The Bill provides that both technical assistance and capability notices "may require a specified act or thing to be done within a specified period" of time. (§§ 317N, 317U). For the former, the Explanatory Document states that an agency "may request that a provider remove security controls from a particular device … in a short timeframe to assist with an urgent operation." (§ 317N, p. 34). Short timeframes are incompatible with normal software quality assurance processes. Their curtailment, under rush conditions and compliance pressures, only increases the risk that providers' code-based means of implementing "particular" device access will import flaws not previously present in the device's code.

This might not matter so much if an access solution really would be limited to one particular device and never deployed again. But as explained above, given the likely scale of access demands, providers are likely to keep and re-use the code they developed for a "particular" instance. True, that would give the provider additional time to test that code for flaws. But even with time and extensive testing, it is extremely difficult (if not impossible) to write bug-free code. Software bugs can interact with existing code in complex ways, creating unanticipated new paths for bypassing security and exploiting the device (or service or item of software). And as explained below, the provider will not necessarily be able to retain exclusive control over the code, *i.e.*, prevent it from affecting "a wide range of" devices or services, thereby "making them vulnerable to interference by malicious actors." (§ 317ZG, p. 47). That is: bugs in the code intended for accessing one "particular" device would, through code re-use, risk affecting the entire device ecosystem, even "devices … with no connection to an investigation." (*Id.*). That is how a provider's enabling "one-off" access as required by Section 317ZG could result in the very "systemic vulnerability" that section says the Government cannot mandate.

The Government does not seem particularly troubled by this possibility. The Bill says that providers cannot be *forced* to build a systemic weakness into their products or services. (§ 317ZG). But in leaving providers free to *choose* to do so, the Bill does not even require them to make any effort to minimize the security impact of that systemic flaw. Perhaps that omission stems from an implicit acknowledgement that, as said, bugs are nearly impossible to avoid and can manifest in unexpected ways, despite developers' best efforts and even given adequate time and vetting. That is, perhaps the Government knows there simply is no such thing as a "secure backdoor,"[3] and so the Bill does not purport to require providers to do the impossible. Nevertheless, it is surprising that the Government would display such a laissez-faire attitude toward the security consequences of the access solutions it will compel providers to build.

Tellingly, the Bill does not overtly provide for the revocation of a technical assistance/capability notice if the provider's compliance leads to a widespread negative security impact. (*See* §§ 317R, 317Z). Such an impact might be interpreted to count as one of the enumerated conditions for revocation (*e.g.* "not reasonable and proportionate"). (*Id.*). But since it is not expressly stated in the Bill (*id.*) nor contemplated in the Explanatory Document (pp. 35, 40), that interpretation would be left up to the discretion of the respective revocation authority.

In effect, the Bill seems to say that the Government won't *make* providers harm the security of their product or service across the board in order to serve the paramount goal of fulfilling Australian investigators' access demands—but if they *do*, that is not the Government's concern. That is an odd policy to adopt, as it conflicts with the Government's professed interest in promoting "internet, computer and data security, supporting Australian economic growth and protecting consumer data," as well as "secur[ing] Government and citizen information, critical infrastructure and computer networks" (p. 7). Again, these omissions suggest that either the Government does not have a firm grasp of the likely computer security consequences of the Bill, or that its statements about "protect[ing] the fundamental security of systems and products" (§ 317ZG, p. 47) are in truth meaningless.

3. Providers May Lose Control of the Code for Enabling Government Access.

Another shortcoming of the Bill's computer security vision is that it seems to assume that the means for accessing an encrypted device (or other product, service, or software) would never fall out of the provider's control. As said, the provider is unlikely to discard the code after accessing a "particular" device, but instead will keep and re-use it, and likely will not tie the code to a specific device. That code will instantly be an attractive target for malicious actors. Keeping it secret is essential to ensuring that it will not pose a broader security threat to the provider's users. But the high demand for access to encrypted products and services poses a serious risk that the code will not be restricted to the context of legitimate investigations by the Australian Government.

If a provider's security practices are inadequate, it could inadvertently leave the code exposed or lose it through hacking by malicious actors. The code would be vulnerable to "insider threats": that is, the provider's employees, who might leak the code to unauthorized third parties either inadvertently (by being hacked, phished, or fooled), for profit, or due to extortion. These risks increase as the number of access demands rises. The more often the provider is compelled to use an access capability, the more employees at the provider will need to have access to it, and thus the more likely it will leak.[4]

---

[3] *See generally* H. Abelson *et al.*, *Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications*, 1 Journal of Cybersecurity 69–79 (Nov. 2015), *available at* https://academic.oup.com/cybersecurity/article/1/1/69/2367066.

[4] These risks are described in more detail in my February 2018 whitepaper, "The Risks of 'Responsible Encryption.'" I previously submitted this whitepaper to the Government via email dated 8 February 2018, in response to the Parliamentary Joint Committee on Law Enforcement's call for submissions of comments concerning the impact of new and emerging information and communications technology. The whitepaper is highly relevant to the Government's

Government possession of the code would add to these risks. Once a provider creates an access capability for the Government, the Government might decide to eliminate the middleman and compel the provider to turn over the code directly, as the Bill appears to allow. (*See* § 317E(1)(b), (e)(viii)-(x) (technical assistance/capability notices can compel providers to "provid[e] technical information" to agencies and give them "access to … software")). Another government, wanting the same access, might do likewise. Like a provider, a government agency—even one generally savvy about computer security—could leak the code through poor security practices.[5] Corrupt or negligent government officials, like the provider's own employees, could lose, sell, or get blackmailed for the code (which for certain devices and software would fetch an immense price, *e.g.* from organized crime rings). Those officials might also use the access capability for their own agendas, such as to target political or personal enemies.[6]

If, as described above, the provider's code for enabling access is not tied to a specific device, then it should be clear that leaking it would pose a serious public danger. If malicious actors gained the use of Government-mandated access capabilities, it would jeopardize the security of any user of the affected product or service, from a stalking victim to an airplane pilot to a head of state.

In short, there are numerous vectors for providers to lose control over the access capabilities that this Bill would compel them to create. Once that control is lost, the Government would no longer be able to keep for itself the ability to access encrypted devices and data. That capability—as well as exploits enabled by unintended bugs in the compelled access code, as discussed above—would risk affecting "a wide range of" devices or services, "making them vulnerable to interference by malicious actors." (§ 317ZG, p. 47). That is inconsistent with the Government's expressed desire to avoid "systemic vulnerabilities," but it is precisely where the Bill will lead. Computer security is extremely difficult, and mandating that providers weaken their products' and services' security—even in seemingly one-time, "particular" instances—can and will have systemic repercussions.

4. The Bill Will Give Cover to Human Rights Abuses by Oppressive Governments.

What is more, "malicious actors" are not limited to criminals; they can include nation-states. The Bill emphasizes the procedural underpinnings and oversight that its technical-assistance scheme would entail. But not all countries are democracies. If Australia mandates compliance with the Bill by providers whose "services or products have a nexus to Australia" (p. 9), then as said, those providers will be subjected to similar demands by the governments of every country where they have such a nexus. That includes authoritarian governments with no respect for human rights or the rule of law.

Such governments might use a compelled access capability to target at-risk individuals such as journalists, dissidents, or ethnic, religious, or sexual minorities.[7] If a provider refused to create or hand over

present request for comment on this Bill as well. It is available in PDF format at http://cyberlaw.stanford.edu/publications/risks-responsible-encryption.

[5] As the Government is surely aware, this happened recently with hacking tools developed by the U.S. National Security Agency, a key partner of Australia's in the Five Eyes intelligence alliance. *See* Scott Shane, *Malware Case Is Major Blow for the N.S.A.*, The New York Times (May 16, 2017), https://www.nytimes.com/2017/05/16/us/nsa-malware-case-shadow-brokers.html?_r=0.

[6] Again, a case from the United States provides an example. A New York City prosecutor abused her wiretap authority by forging judges' signatures on wiretap orders in order to eavesdrop on a former love interest and his new girlfriend, reading their text messages and listening in on their calls for almost 18 months. Jennifer Bain, *Ex-Assistant DA Who Wiretapped NYPD Love Interest Gets Year in Jail*, The New York Post (Feb. 2, 2018), https://nypost.com/2018/02/02/ex-assistant-da-who-wiretapped-nypd-love-interest-gets-year-in-jail/. The Government cannot assume that corrupt officials exist only in corrupt governments; it must consider that Australian officials may misuse their powers too.

[7] For example, in 2007 Yahoo settled a lawsuit brought by families of two dissidents whom China prosecuted and imprisoned; Yahoo had helped the Chinese government identify them by handing over their email records, claiming "it had no choice other than to comply with a request from Beijing to share information about the online activities of the

the means of access, the government could threaten to jail in-country employees,[8] seize the provider's assets, or shut down its business, as leverage to induce the provider to relent.

If passed, then, the Bill will jeopardize the personal safety of countless people in other countries (including some in Australia's sphere of influence). And Australia will have thrown away both a moral and a practical argument against authoritarian abuses of encryption's many innocent users. The Bill does not and cannot account for these eventualities.

Conclusion

Again, I appreciate the opportunity to submit these comments on the exposure draft of the Bill. Please do not hesitate to contact me if I can be of any further assistance as the Government continues to evaluate this matter.

Sincerely,

[redacted]
Riana Pfefferkorn
Stanford Center for Internet and Society
[redacted]
USA
Tel: [redacted]
Fax: [redacted]
[redacted]

journalists." Ewen MacAskill, *Yahoo Forced to Apologise to Chinese Dissidents over Crackdown on Journalists*, The Guardian (Nov. 14, 2007), http://www.theguardian.com/technology/2007/nov/14/news.yahoo.

[8] In 2016, Brazil arrested and briefly jailed a Facebook executive over Facebook-owned WhatsApp's inability to comply with court orders to give investigators access to their targets' WhatsApp messages, which were end-to-end encrypted. Brad Haynes, *Facebook Executive Jailed in Brazil as Court Seeks WhatsApp Data*, Reuters (Mar. 1, 2016), https://www reuters.com/article/us-facebook-brazil-idUSKCN0W34WF.