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

11 September 2019

Via E-Mail to INSLM@inslm.gov.au

James Renwick CSC, SC
Independent Natonal Security Legislation Monitor
3-5 National Circuit
Barton ACT 2600
Australia

Re: Submission to INSLM for His Review of the Telecommunications and Other Legislation Amendment (Assistance & Access) Act 2018

Dear Mr Renwick:

Thank you for inviting me to make a submission to you in your capacity as the Independent National Security Legislation Monitor (INSLM) for your 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 nearly four years. 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. Previously, I submitted written comments on the Act to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) both before and after the Act's passage, on 9 September, 11 October, and 13 and 26 November 2018 and on 14 February and 14 June 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.

Per the PJCIS's referral, the INSLM's present review is to focus on whether the Act:

1. contains appropriate safeguards for protecting the rights of individuals, and
2. remains proportionate to any threat of terrorism or threat to national security, or both; and
3. remains necessary.[3]

---

[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.

[3] *See* Parliament of Australia Media Release, "Intelligence Committee refers Assistance and Access Act for Independent Review," https://www.inslm.gov.au/sites/default/files/files/pjcis-media-release-assistance-access-act.pdf. It is not clear whether either the PJCIS or the INSLM is using the terms "necessary" and "proportionate" in the same sense as the so-called "Necessary and Proportionate Principles," formally known as the International Principles on the Application of Human Rights to Communications Surveillance, which were issued six years ago as a framework for assessing whether an existing or proposed surveillance law comports with international human rights law. *See* About the Principles, Necessary &

This submission will address each question in turn.

1. Whether the Act Contains Appropriate Safeguards for Protecting Individual Rights

My prior submissions to the PJCIS have answered this question in the negative. The Act puts the human rights of non-Australians in jeopardy, and it threatens Australians' individual rights. Those include press freedom and the right against self-incrimination as I discuss below, as well as other free expression rights and privacy rights that have been cogently discussed in others' submissions to the PJCIS.[4]

Human rights of non-Australians. My first submission to the PJCIS (9 September 2018)[5] described how the Act would give cover to oppressive governments to abuse the human rights of their people. If Australia forces providers covered by the Act to give Australian investigators technical assistance in accessing the data and communications of Australians, then governments with dismal human rights records will demand that those providers do the same for them, so that they can investigate such "crimes" as political dissent, being gay, or speaking ill of the king. And Australia will not have a leg to stand on if it wishes to condemn such abuses, because Australia, in passing and enforcing the Act, will have been a catalyst for them.

Press freedom. My most recent PJCIS submission (14 June 2019)[6] addressed the adverse impact of the Act (particularly Schedules 1 and 3) on press freedom in Australia. As that comment describes (and as you are surely aware), mere months after the Act's passage, the Australian Federal Police conducted a disturbing series of raids on journalists and media outlets, aided by new powers granted under the Act. These incidents have already demonstrated concretely that the Act lacks appropriate safeguards. By empowering the raids as well as threatening journalists' ability to protect their sources' confidentiality, the Act flouts internationally agreed-upon principles of press freedom. Moreover, by chilling journalism, the Act also undermines the right of individuals to *receive* information without government censorship. In sum, the Act (particularly taken together with other surveillance legislation passed in recent years) threatens Australian democracy as a whole, because a free press and an informed public are essential to a functioning democracy.

Self-incrimination. Another troubling aspect of the Act, which I have not discussed in prior submissions, is Schedule 3's amendment of subsection 3LA(5) of the Crimes Act 1914 to increase the penalty for refusing to unlock one's phone (or other "computer or data storage device") for the police from two years' imprisonment to five (ten for serious offenses or serious terrorism offenses).[7] There are obvious privacy problems in forcing people to let investigators see everything contained in their cell phones. "With all they contain and all they may reveal," cell phones "hold for many [people] 'the privacies of life,'" as the U.S. Supreme Court observed in a 2014 ruling imposing a warrant requirement for cell phone searches.[8] But in addition to the privacy problem, the requirement to unlock one's phone for police or else go to prison for five years or more also waters down Australia's already-weak right against self-incrimination and is disproportionate to the underlying crime being investigated.

In the United States, the Fifth Amendment to the U.S. Constitution guarantees the right not to be compelled to testify against oneself.[9] Although Australia has no federal bill of rights comparable to that of the

---

Proportionate, https://necessaryandproportionate.org/about. Lacking any background in international human rights law, I am not invoking that framework when I use the terms "necessary" or "proportionate" in this submission. Nevertheless, I encourage the INSLM to review the Principles and evaluate the Assistance and Access Act against them.

[4] For example, see the submission by the International Civil Liberties and Technology Coalition dated 11 July 2019, available at https://www.aph.gov.au/DocumentStore.ashx?id=126ab875-3079-4b36-9c72-f0c422b9bf25&subId=668108.

[5] Available at https://cyberlaw.stanford.edu/files/publication/files/2018-09-09%20Pfefferkorn%20Comments%20to%20Australian%20Govt%20on%20Assistance%20%26%20Access%20Bill.pdf.

[6] Available at https://cyberlaw.stanford.edu/files/publication/files/2019-06-14%20FINAL%20Pfefferkorn%20letter%20to%20PJCIS%20re%20A%26A%20Act.pdf.

[7] *See supra* n.2, Schedule 3, ¶ 9 (amending Subsection 3LA(5)).

[8] *Riley v. California*, 573 U.S. 373, 403 (2014) (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)).

[9] U.S. CONST. amend. V.

U.S. Constitution,[10] it, along with over 100 other countries around the world, recognizes some variant of the right against self-incrimination.[11] However, Australia's right of suspects and arrestees not "to say or do anything" as provided in the Crimes Act 1914 is much weaker than the Fifth Amendment, because the Crimes Act just plain erases the right if "another law of the Commonwealth requires the person to answer questions put by, or do things required by, the investigating official."[12] That is: you have the right not to incriminate yourself, except when you don't.

The things an Australian investigator can require someone to do include unlocking one's phone, as noted above. By contrast, in the U.S., thanks to the Fifth Amendment, someone ordered by police to unlock their phone may (depending on the circumstances) have the constitutional right not to do so, as the act of unlocking can be considered testimonial.[13] If so, the individual could not be punished for exercising their constitutional right. That is, their refusal to unlock their phone could not be penalized by even two years' imprisonment (as the Crimes Act formerly allowed), much less five or ten. In increasing that penalty, the Act only underscores that Australians have little protection against compelled self-incrimination to begin with.

That increased penalty is also problematic because it is out of proportion to the underlying crime. Indeed, that is the amendment's entire purpose: to dissuade people from refusing to incriminate themselves in an offense (*i.e.*, unlock their phones) by punishing the refusal much more harshly than the offense.[14] This turns the entire concept of the right against self-incrimination on its head. And, as Australia's Human Rights Commissioner said, it "seems to be a disproportionate impact on human rights."[15] His Commission noted in a submission to the PJCIS last year that such a disproportionate and arbitrary penalty may violate multiple articles of the International Covenant on Civil and Political Rights (ICCPR),[16] which Australia has ratified (albeit without adopting the rights the ICCPR enumerates into domestic legislation).[17]

Repealing the portion of the Assistance and Access Act that amends Subsection 3LA of the Crimes Act (or even repealing Subsection 3LA itself) would not fix the larger problem that Australia lacks a bill of rights. But it would at least restore a little bit of color to the pallid right against self-incrimination in Australia.

2. Act's Proportionality to Terrorism and/or National Security Threats

The details of terrorism threats and/or national security threats are typically kept under wraps, which precludes me and other members of the general public from giving fully-informed comments on this aspect of

[10] *See How Are Human Rights Protected in Australian Law?*, Australian Human Rights Commission (2006), https://www.humanrights.gov.au/how-are-human-rights-protected-australian-law ("Unlike most similar liberal democracies, Australia does not have a Bill of Rights.").
[11] *See Miranda Warning Equivalents Abroad*, Law Library of Congress (May 2016), available at https://fas.org/sgp/eprint/miranda.pdf.
[12] *See* Section 23F of the Crimes Act 1914, available at https://www.legislation.gov.au/Details/C2017C00297.
[13] *See generally* Orin Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 Tex. L. Rev. 767 (2019), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248286.
[14] Commonwealth, *Parliamentary Debates*, House of Representatives, 20 Sept. 2018, at 21 (the Hon Peter Dutton MP, Minister for Home Affairs) ("The increased penalties for noncompliance with orders for access to a device reflect … the fact that persons who have undertaken criminal activity would rather accept the current low penalties than provide data that could be evidence in a more serious prosecution.").
[15] Paul Karp, "Australia's War on Encryption: The Sweeping New Powers Rushed into Law," *The Guardian* (7 Dec. 2018), https://www.theguardian.com/technology/2018/dec/08/australias-war-on-encryption-the-sweeping-new-powers-rushed-into-law.
[16] Human Rights Commission submission to PJCIS dated 12 Oct. 2018, at ¶¶ 384-395, available at https://www.aph.gov.au/DocumentStore.ashx?id=a7b9ff25-7c09-41e9-b97a-56dae1ac0e94&subId=661055.
[17] "6. Implementing the ICCPR in Domestic Law," Joint Standing Committee on Foreign Affairs, Defence and Trade, Inquiry into the Status of the Human Right to Freedom of Religion or Belief, Interim Report (November 2017), https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Foreign_Affairs_Defence_and_Trade/Freedomofreligion/Interim_Report/section?id=committees%2Freportjnt%2F024110%2F25347.

the INSLM's review. I suspect that the Act, which has been criticized as "draconian,"[18] is a disproportionate response to the actual size of the threat. But without being privy to non-public threat information (as the INSLM likely will be), I cannot meaningfully test that suspicion. Nevertheless, I hope my outside perspective might still be helpful insofar as I can illuminate the proportionality issue from a different angle.

Specifically, I want to emphasize that encryption and other cybersecurity measures help to *protect* national security interests, whereas by undermining cybersecurity (as I have explained previously),[19] the Act risks *harming* those interests. In evaluating the Act's proportionality, the INSLM should compare the extent to which the Act undermines those interests against the degree to which it can be shown to help combat the threats to them.

I have explained before[20] that the basic trouble with access mechanisms intended for use only by the "good guys" is that they are susceptible to discovery and abuse by the "bad guys" as well. The "bad guys" can then use that access mechanism to snoop on the "good guys" and damage national security. In one notorious example, attackers exploited the wiretap functionality of Greece's largest cell service provider, subverting a means of access intended only for legitimate law enforcement use in order to snoop on the calls of the country's prime minister, the mayor of Athens, and at least 100 other high-ranking officials.[21]

Why was that hack possible? Because those officials used the same cellular network that everyone else did, and that network had been designed to be wiretappable by the police. Similarly, governments regularly procure the same so-called "commercial off-the-shelf" hardware, software, and services that are available in the marketplace to ordinary consumers and businesses (*e.g.*, Microsoft software), then tailor them to organizational needs. That means any vulnerabilities in those "COTS" products could pose a risk to the government customers' security as well.[22] Typically those vulnerabilities would be unintentional. But when governments impose access mandates (such as the Act), then, to comply, COTS products and services will contain vulnerabilities *by design*—for that is what a "capability" under the Act is: a vulnerability.[23] Australia can recognize the risk that insecure products could pose to national security when the government suspected of mandating those insecurities is China,[24] but it seems incapable of turning that same reasoning on itself.

---

[18] David Meyer, "Australia Just Passed a Draconian Anti-Encryption Bill That Will Create a Headache for Big Tech," *Fortune* (6 Dec. 2018), https://fortune.com/2018/12/06/australia-encryption-law/.

[19] See my submission to PJCIS dated 9 September 2018, *supra* n.5.

[20] See my submission to PJCIS dated 26 November 2018, available at https://cyberlaw.stanford.edu/files/publication/files/2018-11-26%20Pfefferkorn%20letter%20to%20PJCIS%20re%20compromise%20bill.pdf.

[21] Vassilis Prevelakis and Diomidis Spinellis, "The Athens Affair," *IEEE Spectrum* (29 June 2007), https://spectrum.ieee.org/telecom/security/the-athens-affair.

[22] Wikipedia, "Commercial off-the-shelf," https://en.wikipedia.org/wiki/Commercial_off-the-shelf (last visited Sept. 9, 2019). The risk is not limited to government devices and systems. Government employees, just like any other consumer, typically have COTS smartphones, home computers, email and cloud accounts, etc. for their personal, private use. Those can also become a vector for national security risk. For example, when a contractor for the U.S. National Security Agency took highly classified documents home to catch up on work at night, that allegedly enabled Russian hackers to steal the information from his home computer via antivirus software made by Russia-based Kaspersky Lab. Scott Shane, "He Took Home Documents to Catch Up on Work at the N.S.A. He Got 5½ Years in Prison.," *N.Y. Times* (25 Sept. 2018), https://www.nytimes.com/2018/09/25/us/politics/nghia-pho-nsa-prison-sentence.html. Kaspersky products have now been banned from use by U.S. government agencies and federal contractors. Aaron Boyd, "U.S. Finalizes Rule Banning Kaspersky Products from Government Contracts," Nextgov (9 Sept. 2019), https://www.nextgov.com/cybersecurity/2019/09/us-finalizes-rule-banning-kaspersky-products-government-contracts/159742/.

[23] *See supra* n.20 at 3.

[24] *See, e.g.*, "Australian Cyber Officials Warned India against Using Huawei: Newspapers," Reuters (9 Sept. 2019), https://www.reuters.com/article/us-australia-cyber-india/australian-cyber-officials-warned-india-against-using-huawei-newspapers-idUSKCN1VU2JU.

The upshot is that, by passing the Act, Australian government officials will open themselves up to exploitation by using the very same products and services they are forcing to be less secure, be it a smartphone, chat app, cloud storage service, or what have you. And it is no answer that, per Section 317ZG, the Act does not intend for covered providers to create "systemic weaknesses" or "systemic vulnerabilities": that will still likely be the result, as I have explained before.[25] Government officials are already targets for cyberattacks as it is;[26] by compelling covered providers to weaken their security, the Act risks adding new vectors for such attacks.

In short: the Act was meant to improve national security, but it will only end up undermining it. This is why multiple former top intelligence officials in the U.S. have publicly opposed weakening encryption—even though they know firsthand what national security and terrorism threats the country faces.[27] They have concluded that the cost of mandating weaker security outweighs the benefit.[28] As the INSLM, you are well-positioned to ask Australia's intelligence agencies why they have not come to the same conclusion as their American counterparts.

3. Necessity of the Act

As above, since I lack insight into the precise scope of the criminal, terrorist, and national security threats that Australia faces, I cannot give a fully-informed opinion on whether the Act "remains necessary" to combat those threats. But, again as above, I suspect the Act (which as passed ran to 224 pages[29]) was not necessary to begin with and still isn't.

An initial question is what "necessary" means. As said, this is not defined by the PJCIS or the INSLM. If one takes the view that in an age of ubiquitous encryption, law enforcement agencies could not do their jobs *at all* without the new powers granted under the Act, then by that view, the Act was "necessary." But this is not a serious view. A new report by a working group convened by the Carnegie Endowment for International Peace calls it a "straw man" argument "that law enforcement will be unable to protect the public unless it can obtain access to all encrypted data through lawful process" and "that law enforcement must have access to all

[25] See my submissions to PJCIS dated 9 September 2018, *supra* n.5, and 11 October 2018, available at https://cyberlaw.stanford.edu/files/publication/files/2018-10-11%20Pfefferkorn%20Comments%20to%20Joint%20Cmte%20on%20Asst%20%26%20Access%20Bill.pdf. It does not matter how the terms "systemic weakness" and "systemic vulnerability" are defined (*see* Section 317B of the Act), though their definitions were a matter of much debate in the lead-up to the Act's passage. However well-meaning Section 317ZG might seem to be, what it boils down to is that the Government wants to eat its cake and have it too, and that contradiction cannot be defined away. As my 9 September 2018 comment explained, *see supra* n.5, Section 317ZG does not *forbid* covered providers from creating systemic weaknesses or vulnerabilities (as defined) in order to comply with notices or requests under the Act, and for various reasons, a systemic weakness or vulnerability is the predictable outcome in actual practice. That remains true no matter how much tinkering and wordsmithing happens to those two terms' definitions.

[26] Amy Remeikis, "Australian Security Services Investigate Attempted Cyber Attack on Parliament," *The Guardian* (7 Feb. 2019), https://www.theguardian.com/australia-news/2019/feb/08/asio-australian-security-services-hack-data-breach-investigate-attempted-cyber-attack-parliament.

[27] Conor Friedersdorf, "Former National-Security Officials Now See the Peril of Weakening Encryption," *The Atlantic* (30 July 2015), https://www.theatlantic.com/politics/archive/2015/07/former-national-security-officials-see-the-peril-of-weakening-encryption/399848/. Recently, one such former official gained attention when he disagreed on Twitter with the U.S. Attorney General's assertion that Americans should accept the security risks of encryption "backdoors," saying: "Not really. And I was the director of [the] [N]ational [S]ecurity [A]gency." Gen. Michael Hayden (@genmhayden) on Twitter, 23 July 2019, 10:43 a.m., https://twitter.com/genmhayden/status/1153722298861535232?lang=en.

[28] Friedersdorf, *supra* n.27 (quoting Gen. Hayden as saying, "The downsides of a front or back door outweigh the very real public safety concerns.").

[29] See the PDF version of the Act as passed, available at https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r6195_aspassed/toc_pdf/18204b01.pdf;fileType=application%2Fpdf.

information or else society will disintegrate."[30] And indeed, that interpretation of the Act's "necessity" does not stack up to reality. The law enforcement and security services were investigating, prosecuting, and preventing crime and terrorism before the Act's new powers went into effect. One does not need to know the secret details of those efforts to see that.

After all, the advent of digital technologies gave rise to a "golden age of surveillance"[31] from which Australia's law enforcement and intelligence agencies have benefited. Through such technologies as email, chat, smartphones, mobile apps, productivity and collaboration software, health trackers, and social media, we now create a vast amount of data about ourselves (including our bodies, movements, activities, and social interactions) that "did not exist or were not recorded in the past."[32] Those already-numerous sources of information will be further augmented by the additional data streams generated by "Internet of Things" devices, from doorbells to cars to toothbrushes. Much of that data (both contents and so-called "metadata") is recorded and stored in a way that law enforcement agents can access with the proper legal process. The transparency reports regularly issued by many technology companies about government requests for their users' data stand as testament to that.[33]

Australia's law enforcement and intelligence agencies were well aware of these many sources of data that were already available to them before the Assistance and Access Act was passed, and they took full advantage of them under the country's existing surveillance statutes. For example, they have used the Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 to serve over 300,000 warrantless requests per year on Australian telcos for the metadata of their subscribers.[34]

In this bounteous cornucopia of information, the contents of a smartphone or chat message are just one morsel. Encryption (and other technologies for preserving the privacy and security of data) may have taken a bite out of investigators' access, but certainly not eaten it whole. "The fact that information is now encrypted does not represent an unprecedented challenge for law enforcement; it merely represents a slight retreat from the 'golden age of surveillance' that we currently live in."[35]

All of which is to say: investigators do not need the Act to do their job. There are many sources of evidence still available to them in pursuit of the ultimate goal of public safety. That goal can be (and was) accomplished without the Act. As the Carnegie report put it: "Can law enforcement operate in an environment where encryption is more broadly available? Yes."[36]

What the Act's new powers might actually do is to help law enforcement agencies carry out certain investigatory tasks *more expeditiously* and with less friction, such as by making evidence-gathering faster, cheaper, or otherwise less resource-intensive. (For example, threatening to throw someone in prison for ten years is a very quick and cheap way to get access to a locked, encrypted phone, especially when there is no pesky right against self-incrimination getting in the way.) That is, the Act's new powers are not strictly

---

[30] *Moving the Encryption Policy Conversation Forward* 9, Encryption Working Group Paper, Carnegie Endowment for International Peace (September 2019), https://carnegieendowment.org/files/EWG__Encryption_Policy.pdf. The report notes that "some have criticized the Australian approach [of passing the Act] as excessively broad." *Id.* at 20 n.3.

[31] Peter Swire and Kenesa Ahmad, "'Going Dark' Versus a 'Golden Age for Surveillance,'" Center for Democracy and Technology (28 Nov. 2011), https://cdt.org/blog/'going-dark'-versus-a-'golden-age-for-surveillance'/.

[32] *Moving the Encryption Policy Conversation Forward*, *supra* n.30, at 9.

[33] *See generally* Access Now, Transparency Reporting Index (Fall 2016), https://www.accessnow.org/transparency-reporting-index/ (listing some of the companies that have issued transparency reports).

[34] See my submission to PJCIS dated 13 November 2018, available at https://cyberlaw.stanford.edu/files/publication/files/2018-11-13%20Pfefferkorn%20Comments%20to%20JCIS%20re%20TOLA%20%26%20CLOUD%20Act.pdf.

[35] Amie Stepanovich, "Why an Encryption Backdoor for Just the 'Good Guys' Won't Work," Just Security, https://www.justsecurity.org/53316/criminalize-security-criminals-secure/.

[36] *Moving the Encryption Policy Conversation Forward*, *supra* n.30, at 9.

necessary to get the job done, they just make it *easier*—albeit at the expense of security and individual rights, as I have explained before.

This is a point often made by renowned computer security expert Professor Susan Landau of Tufts University in the U.S. Last fall, she responded to the then-pending version of the Act, as well as to a recently-issued Five Eyes statement on encryption, by observing: "The encryption debate is about … the *efficiency* of law enforcement investigations versus personal, business, and national security."[37] On another occasion, she said, "[W]e're looking at efficiency of law enforcement investigations versus security, and there are other ways of improving the efficiency of investigations without harming security."[38] If anything, according to Prof. Landau, the "necessity" question runs the other way: "The wide public availability of strong encryption must be understood as critically necessary for security."[39]

In short, in an age of cybercrime, hacks, and data breaches, it is strong security that is necessary. The Act's measures are not. While they may make investigations easier, investigators can achieve their goals through other means that do not damage security the way the Act does.

* * *

I appreciate that PJCIS's referral to the INSLM focused on three specific matters, and I have confined my comments to those three accordingly. But as I have said before, focusing on particular aspects of the Act should not cause one to lose sight of the big picture: the Assistance and Access Act should be repealed.

Please do not hesitate to contact me again if I may be of additional assistance during the course of your review.

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

[37] Susan Landau, "The Five Eyes Statement on Encryption: Things Are Seldom What They Seem," Lawfare (26 Sept. 2018), https://www.lawfareblog.com/five-eyes-statement-encryption-things-are-seldom-what-they-seem (italics emphasis added). Prof. Landau's article also links to further expressions of support for strong encryption by former top intelligence officials (from the United Kingdom as well as the U.S.), in addition to those cited *supra* n.27.

[38] Andrew Crocker and Nate Cardozo, "Bring in the Nerds: EFF Introduces Actual Encryption Experts to U.S. Senate Staff," Electronic Frontier Foundation (3 May 2018), https://www.eff.org/deeplinks/2018/05/bring-nerds-eff-introduces-actual-encryption-experts-us-senate-staff.

[39] Landau, *supra* n.37.