The Great Australian Foot-Gun: An Expert's Grievances with the Backdoor Legislation.

Aleksa Sarai [redacted]
Sydney, Australia

(Dated: 26 February 2019)

There has been a lot of collective (and justified) hand-wringing over the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018[1], after it was rushed through Parliament. I hope this expert opinion by one of many Australian software engineers appalled by our Parliament's actions (in passing this legislation) will be taken seriously this time. This legislation will not fulfill its goals, is a direct existential threat to Australia's technology industry, and will destroy faith in Australian software developers for years to come. It simply must be repealed and re-thought entirely (or at the very least, significantly amended to ensure the safety and security of the general public).

This Parliament has managed to single-handedly, and seemingly cluelessly, caused one of the largest existential threats to Australia's technology industry. It appears that the sheer lack of understanding on matters of technology has resulted in you passing legislation that had (within a few days) significantly reduced faith in the security of software written by Australian companies and Australian developers. And this was done with full knowledge that there was an enormous public outcry about this legislation – with more than 99.7% of all commenters in the ridiculously short public comment period stating they were *against* the Act's passage[2]. A grand total of 1 comment was in support of this legislation.

There is a very serious ethical argument to be considered when discussing this legislation, on whether it is reasonable and ethical for a government to spy on its citizens to the point where (the digital equivalent of) whispering is no longer permitted. That is not the point of this letter, because it is clear that this Parliament is not interested in the human rights of its citizens (or of non-citizens for that matter)[3–5]. Australia has very few protections for the human rights of its people, despite a long history of attempts to change this[6]. I really do hope that one day this will change, but there are more practical problems to consider with this piece of legislation.

For the rest of this letter, I will refer to capabilities created under Technical Capability Notices as "backdoors". I realise that the Government doesn't agree with the use of this term, but that is because the Government decided to **redefine technical terms in order to make experts sound incoherent**. The term "backdoor" in discussions of this legislation was used to refer to the concept of a vulnerability that nobody except the discoverer is aware of (thus if the Government is aware of the vulnerability, it tautologically cannot be a "backdoor"). This is simply an incorrect definition – the correct term for this is a "0-day", and the Government intentionally re-defined the term in order to make reasonable discussion difficult. **The vast majority of credible experts would consider capabilities created due to a Technical Capability Notice to be "backdoors".** It is *completely irrelevant* that the backdoor happens to be government-sanctioned.

Similarly, the definition in the legislation of "systemic weakness" does not match the common meaning of the word – if any single end-to-end encryption technology has the ability for its developers to read messages sent using it, that is a systemic weakness **in that technology**, but would not be considered as such under this legislation (since it doesn't affect "a whole class of technology"). Not to mention that the meaning in the legislation is so weak it's effectively useless – it would be almost impossible for a single company to "systematically weaken a whole class of technology", as most core technologies are developed collaboratively with people in many different jurisdictions (as discussed in section II).

This redefinition of words to confuse your critics is a blatantly Orwellian tactic that I won't participate in.

I. SUMMARY OF CONCERNS

The primary points made in this letter are broken down by sections, each of which justifies the statement made in the section title. This legislation will

1. ... not succeed in its goal to prevent terrorism or other serious crimes, due to the ubiquity of secure (and easy-to-use) communications software that simply cannot be secretly backdoored — not to mention that criminals have a greater incentive to find methods of communication that cannot be read by the Government than the general public (section II).

2. ... destroy trust in Australian software developers, due to concerns that any Australian software developer might be compromised by a notice under this legislation (section III).

3. ... destroy trust in Australian software, due to similar concerns that the software may have intentionally weakened security due to a request from the Australian Government (section IV).

4. ... systemically weaken encryption in Australia, despite the wording that attempts to dismiss this concern (section V).

5. ... weaken the security of users around the world, due to the 5-Eyes spying alliance and due to the nature of software backdoors (section VI).

6. ... have no judicial oversight on Technical Capability Notices, making them rife for potential abuse (section VII).

7. ... likely experience "authority creep" and more agencies will be given the powers under this legislation, as has occurred with the mandatory metadata retention legislation (section VIII).

And I give my personal recommendation in section IX, which is that **the legislation is unacceptable and I recommend that Schedule 1 of this legislation be repealed** and that there be a more lengthy discussion of the "going dark" problem. As an alternative, I would propose that my amendments outlined in section IX be adopted. There clearly is an education problem, where law enforcement should learn other methods of doing investigations other than the mandating of backdoors into systems that the general public uses. Schedule 2 does have some provisions that I am not sure I understand well enough to comment on (given that they are extensions to existing warrant laws and have judicial oversight), so they are not the subject of this letter.

Primarily in this letter I talk about Technical Capability Notices, because they are the necessary instrument by which Technical Assistance Notices and Technical Assistance Requests can then be issued (a backdoor must already exist to send a valid assistance notice or request). I freely admit that my knowledge of law is exceptionally limited, and so my understanding of the restrictions of Technical Assistance Notices is quite limited – the practical upshot of s317ZH(1) and s317ZGA would appear to be that *a warrant is always required*. And while s317ZH(4) and (5) appear to be exceptions to this rule, they still appear to require warrants for all relevant cases. As such, I've avoided talking about such notices in this letter. The *mere development* of a backdoor is a fundamental problem — and such development definitely does not have judicial oversight in deciding whether it is "reasonable and proportionate" and whether it respects "the legitimate expectations of the Australian community relating to privacy and cybersecurity".

This letter was drafted by a software engineer and not a lawyer. Therefore sections where I attempt to interpret the legislation should be taken with a grain of salt – just like attempts by politicians to claim an understanding of technology should also be taken with a grain of salt. Statements about technology should be taken as being my own expert opinion.

II. IT WILL NOT SUCCEED IN ITS GOALS

First and foremost, the very concept that this legislation will be able to be effectively used to read the messages of suspected criminals is laughable. It is clear that Parliament is not aware of how much of modern software development is done in the open, or as an international community. The internet allows for software development that transcends individual countries' jurisdictions.

Many pieces of core infrastructure that power the internet and provide secure communications are Free and Open Source Software (FOSS). This means that the source code (the working version of a program that programmers edit to create programs) is available for all users (this is often enforced by copyright licenses such as the GNU General Public License[7] – where the corresponding source code must be provided to all users). Attempting to put a secret backdoor in such a program would be futile, since all changes to such software are public – and are often reviewed by developers in other countries. Developers might even be sued for copyright infringement if they do not provide the corresponding source code for the program (and systems like reproducible builds[8] allow users to verify that their program was produced by a given version of the source code). This means that it is possible for users (or a community of users) to audit the communications software they use, and remove any backdoors if they find them (and if they're provided a binary to use, they can verify that it actually came from the backdoor-free source code they've collectively audited). This makes hidden-to-users backdoors not possible with FOSS software[9].

Of course, not all software is FOSS. But enough secure FOSS software exists that a moderately sophisticated criminal would be more than capable of using it to send secure messages in a way that this legislation would not be able to assist law enforcement (and to be clear, more outrageous legislation wouldn't help either – it's a fundamental problem with such legislation). Secure communication applications such as Signal[10] are readily available, FOSS, and are developed by people who are outside Australian jurisdiction. So all a would-be criminal would have to do is use Signal (instead of some other chat application) and there would be no technical mechanism by which a Technical Capability Notice would be able to be used. The same applies for GnuPG[11], Matrix.org[12], and many other secure messaging systems.

There are even secure encryption schemes that do not require any software (such as Solitaire[13–15] or ElsieFour[16], which both only require physical objects such as a deck of playing cards or tiles) and thus are completely impossible to backdoor. Such techniques can easily be learned in a weekend by someone without any mathematical understanding, and then messages can be sent using any insecure system (because the message itself is secured by pen-and-paper encryption that is sufficiently secure, even when compared to modern encryption schemes).

And it should be noted that, in many ways, serious criminals have a much greater reason to "go out of their way" in finding communications systems that cannot be backdoored by the Government. Therefore, any moderately sophisticated criminal would be willing to "put in the hours" to learn how to use secure encryption tools (and again, many of these are incredibly easy to use). Therefore only *unsophisticated* criminals and **the general public** are likely to use these backdoored encryption systems, and if the Government is seriously claiming that they cannot catch *unsophisticated* criminals without backdooring the security systems that protect the general public then maybe we need to have better law enforcement.

Most mistakes made when using encrypted messaging

are related to operational security, which is something that can be detected and investigated by law enforcement (with the right training) without the need to create backdoors. Many sophisticated security professionals already can do such investigations of their own targets – surely law enforcement is able to do the same thing (especially considering that law enforcement can attain search warrants). If they aren't, then they should be educated in how to do such investigations (many security professionals are contractors – so law enforcement could contract them to teach them how to investigate technically capable adversaries).

I (obviously) deplore criminals, and want our law enforcement to have all the power necessary to catch them. But it is clear that this legislation was drafted without any technical understanding of how such measures could be thwarted by those criminals – there is plenty of encryption software which is secure that is not developed by Australian companies. The internet allows for software transmission without physical borders (in a way that is very fundamentally critical for the world we live in today). Therefore the only net effect is that the Government has the power to compel the development of backdoors, but these can be thwarted by using software developed outside Australia (or by using FOSS) – and the general public is unlikely to go through the trouble that criminals will go through to learn what communication methods are secure against backdoors.

This should have been enough for Parliament to have never considered passing this legislation, and even more reason to now repeal it (admitting that it was a mistake from the beginning). But that's not the only problem with it.

III. IT WILL DESTROY TRUST IN AUSTRALIAN SOFTWARE DEVELOPERS

One of the most insidious aspects of this legislation (for myself) is that it **will cause distrust of Australian developers (like myself) working for foreign companies or with foreign developers**, because they are listed as a "designated communications provider" under s317C(6). There has been some discussion over whether this section could be interpreted as including individual employees of a company (because they are developing software on behalf of their employer)[17]. But this misses another key issue – a large amount of FOSS is developed by people in their free time. Software such as Linux (an operating system that powers the majority of the internet, and is used by almost every "electronic service that has one or more end-users in Australia") has had many Australian contributors that worked on this project on their own time. Personally, I first started contributing to such projects when I was a teenager in high-school – might teenagers now be potentially subject to such notices?

The core infrastructure of the internet is developed by many individuals across the world, and fundamentally is built on trust – our Government breaking that trust means that we may no longer be welcome to help build that infrastructure. The fact of the matter is that **even if the Government never uses this legislation in this manner, trust in Australian software developers has been eroded**[18–20]. It doesn't matter if the legislation is only used to target companies, and is only used to add features (like being able to surreptitiously add a law enforcement device to an Apple account to read new iMessages) – Australian software developers will be assumed to be compromised (since assuming otherwise would be a risky assumption that would threaten their users' security).

As a result, it is very likely that many projects will no longer be interested in contributions from (or hiring) Australian developers. As a result, there will be a corresponding erosion of talent – the only way to learn software development is to work on large software projects (and if large software projects won't accept your work, then you can't learn practical skills). It's possible that many Australian software developers will emigrate to find work. This will further atrophy the technology industry in Australia.

If an Australian software developer receives a Technical Capability Notice, they are now faced with a choice. Either they become a saboteur, and destroy their reputation as a trustworthy and ethical software developer, or they will refuse and be fined tens of thousands of dollars under s317ZB (and it's unclear if the Government could just revoke and then re-issue the Technical Capability Notice – meaning that refusing to follow it could result in bankruptcy). They may quit their job in defiance, but it's not clear whether this would allow them to avoid the disproportionate fines imposed on them.

Luckily, it is a defence against the civil penalty if compliance would cause the developer to violate the law of a foreign country under s317ZB(5) – so at least they won't face trial overseas because of a lawful request by their home government. In addition, "designated communications providers" can provide aggregated statistics about how many notices were received "during a period of at least 6 months" under s317ZF(13). However, admitting that you've received notices would damage your credibility as a software developer – so unscrupulous developers would just lie (reducing the usefulness of such statistics as a security measure by the public). In addition, we imagine that many developers would fear being caught on a technicality within s317ZF – and thus would prefer to stay silent than risk **5 years imprisonment** due to improperly disclosing the existence of a Technical Capability Notice.

As a software developer, I expect Parliament to consider the importance of the technology industry and to safeguard its future in Australia. But you didn't. I expect Parliament to listen to my expert opinion (as well as the many other expert opinions being offered) rather than rushing through legislation in order to avoid criticism from the public[21]. However, our elected representatives closed their ears to the public outcry.

IV. IT WILL DESTROY TRUST IN AUSTRALIAN SOFTWARE

Imagine that you were renovating a house, and had to choose a type of lock for your front door. Would you choose a lock by a company that has a solid track record, or a company that is headquartered in a country where the government *might* ask the company to provide master keys for all their locks (so if they suspect someone is a criminal they can check their home)? The answer should be *obvious* — if those master keys exist they will be reverse-engineered (this exact scenario happened with the TSA master keys for luggage locks in 2016[22]).

The same simple risk analysis is done when choosing what software to use. There is such a large array of choices, and Australia is a small player when it comes to this industry. Why would someone *choose* to use software they know might be made insecure? Nobody in their right mind would make such a decision.

This legislation appears to contradict the GDPR, making it so that software written in Australia will likely never be used in Europe due to the fear of significant fines by the EU because of a GDPR breach. You might think that s317ZB(5) would mean that Australian software couldn't be backdoored in a way that violates the GDPR ("the law says it, so it must be technically possible"), however the ability to add backdoors to a system that processes private information already increases the risk of a breach that will be punished under the GDPR (being able to add backdoors means that the system is insecure – let alone the insecurity added by the backdoors themselves – and insecure systems get breached very often).

And, as with trust in Australian software developers, trust in Australian *software* will also be eroded for the same reasons. We are already having enough trouble penetrating the international market (Atlassian is one of the only success stories we've had), and this just adds more problems.

It will also result in fewer international software businesses wanting to do business in Australia – because doing business here is now a personal privacy liability (since backdoors that can target Australians can target Europeans or Americans just as easily – and legislative instruments can't protect against an attacker discovering and abusing a backdoor added to a system to "just" target Australians).

One could even make the argument that this legislation would actually make Australian software companies (which claim to be "secure") liable to Australian Consumer Law violation lawsuits (due to backdoored software tautologically not being "fit for purpose" as secure software). And while there are civil immunities granted within this legislation (probably precisely to avoid this sort of problem), it will seriously damage the public's view of such software companies.

V. ITS USE WILL SYSTEMICALLY WEAKEN ENCRYPTION IN AUSTRALIA

Despite all of the word-games around "systemic weaknesses" in this legislation, the primary point that has been entirely ignored by Parliament is that **if it is possible for a secure piece of software to be backdoored due to government pressure, then it is an insecure piece of software**.

Edward Snowden's revelations showed us that the NSA had attempted to subvert the security of various systems around the world (and succeeded)[23,24], and since then many groups of software developers have been working tirelessly to design systems that are resilient to such attacks and are easy for the public to use.

As a thought-experiment, we can envision a system whereby the company which develops the software does not have the ability to silently backdoor it. This could be done by having TPM-resident keys on the device which have to sign all software that runs on the device (this would require the user to agree to all software updates). Updates would have to be cryptographically signed by several developers that are all in different jurisdictions in order for the device to even attempt to install it. All of the software on the device would be FOSS, licensed under the GNU General Public License[7], and would be able to be built reproducibly[8].

Such a device **could not be silently backdoored by the company which developed it** (assuming all the above protections were implemented correctly). In order to make this device backdoor-able, the company would have to have created a fundamental weakness in the security of the device to bypass the above protections. And thus, **any** Technical Capability Notice would either be found unenforceable (which I'm sure won't actually happen – why would ASIO and the ASD push for a law they couldn't use for secure systems) or the company would be forced to create a "systemic weakness" (in the common meaning of the word).

Similarly, many messaging applications exist today (such as Signal[10] and Matrix.org[12]) which have encryption that cannot be broken by the company which develops it[18] – **without fundamentally redesigning their system so that it is insecure** (and note that the source code is available for the secure version – so **anyone can just continue using the secure version**). This is by design, because any other design would be an insecure system – and developers are not interested in developing insecure systems because users wouldn't use them (because attackers would target them).

And, by systemically weakening encryption for our Government, we have now created an extreme incentive for those backdoors to be uncovered by malicious parties. In a world where data breaches are already an existential threat to many electronic services, creating backdoors is just inviting attackers to target Australians and Australian software.

It is already difficult enough to create an encryption system that is secure to attackers (including the Government), and is a skill that takes many years to perfect. Developing a "secure" system that is backdoored, "but

only for the 'good guys' (i.e. the Government)", is something that has **never been shown to be possible** — in fact, several attempts have proven to be broken in the past[25]. If it's not possible for computer scientists to come up with such a system in several **decades** of research, how on Earth can the Government expect that a software developer being coerced (under threat of fines due to non-compliance) to develop such a system securely? **They cannot.** And due to the wording in s317ZG, you would expect that this **fundamental limitation** would mean that *all* Technical Capability Notices would have to be invalid. But ASIO has stated they will use these powers[26], and since **we know it's not technically possible to create such a system securely**, then clearly such backdoors *will have to be insecure*.

VI. ITS USE WILL WEAKEN THE SECURITY OF USERS AROUND THE WORLD

One of the more concerning (and political) aspects of the legislation is that it is explicitly designed with the 5-Eyes spying alliance in mind.

s317T(3)(b) states that a "relevant objective" of a Technical Capability Notice can be to assist the enforcement of criminal laws in a foreign country (though only for "serious foreign offences"). As was revealed by Edward Snowden, one of the primary uses of the 5-Eyes spying alliance is to circumvent domestic laws, by using the spying apparatus of member states to spy on their own citizens[27]. This capability of the legislation was clearly designed with this purpose in mind – to allow other 5-Eyes countries to outsource their illegal spying of their citizens to Australia.

The fact of the matter is that technology does not care what your jurisdiction is, and thus a backdoor introduced in order to spy on Australians can just as easily be used to spy on political activists in dictatorships (and it can spy on ordinary citizens just as easily as it can spy on suspected terrorists). That which is *legal* is not necessarily *moral*, and some decisions (such as allowing for the unfettered violation of a person's privacy) should require moral determinations, not just legal ones.

VII. TECHNICAL CAPABILITY NOTICES HAVE NO JUDICIAL OVERSIGHT

This legislation has no judicial oversight to decide whether implementing a backdoor is "reasonable and proportionate". There is no review process in front of a judge about whether a Technical Capability Notice is "reasonable and proportionate" nor any of the other requirements under s317ZAA. Instead, there is an arbitration system that only requires a *former* judge to preside as an assessor under s317YA. And while there is a 28-day consultation period under s317W (which means that Australians mathematically were not able to be "kept safe over Christmas" using this legislation), there is no *judicial* oversight over such consultation. Not only that, but the Minister that approves the Technical Capability Notice only needs to have "regard" to any possible concerns – which is just frankly not any limitation or oversight on these powers.

This is an affront to the fundamental purpose of our judicial system – to ensure there is an impartial check and balance on the powers of law enforcement. Instead, this legislation has made is so that "designated communications providers" are compelled to either act, or defy the notice in order to get judicial oversight through civil court proceedings. This is completely backwards – in order for the notice to have effect, it should go through judicial review *first*, not after-the-fact.

VIII. IT WILL VERY LIKELY INCREASE IN SCOPE OVER TIME

Three years ago, Parliament passed a law mandating metadata retention of Australian communications[28]. Just as with this law, it was originally claimed that it would help catch serious criminals. And just like this law, the set of agencies that could use it was very limited – but over time, "authority creep" has set in[29]. And just like this legislation, there was no need for a warrant to gain access to such data.

A recent example of an abuse of the metadata retention legislation is that a local Sydney council wanted phone records to fine residents for minor infringements like littering[30]. By 2016, the number of government agencies using this warrant-less power to invade people's privacy had almost tripled and included several State racing and gambling authorities[31] – and it's quite likely the list has grown since then. The Communications Alliance recently stated that there are approximately 1000 warrantless metadata requests **per day**[29].

There is absolutely no reason to believe that this law will not exhibit this same "authority creep", given that the same assurances were given (and broken) with previous laws. Not to mention that once a backdoor has been implemented, it's not clear to me whether other agencies could request to use the backdoor using an ordinary warrant (this might be a violation of s317ZF but I'm really not sure). A backdoor cannot differentiate between different reasons for access – it's just a security weakness that can be exploited by the Government (or anyone who figures out how the backdoor works) for any purpose.

The ASD's defence of the law[32] almost entirely depends on the claim that the powers given by the law are incredibly limited at the moment (even though it isn't — it's the first law of it's kind in the entire world) and are only given to a very limited list of agencies. Given our previous experiences with privacy-violating laws passed by the Australian Government, I'm sure you'll understand why we might not take such defences very seriously. The ASD statement has a few other issues, such as pretending that the law being "highly targeted" somehow translates to the underlying backdoor being equally targeted (and I debunked this in section V) – but the above is their core defence. And it's not a very good one.

IX. RECOMMENDATION

All in all, this legislation is completely unacceptable. It **will not fulfill its goals**, it will damage trust in Australian software and software developers, and gives effectively no checks and balances before a notice can be given. This legislation *will* result in the atrophy of the Australian technology industry, because *users expect secure software* and will not accept software that could be backdoored by the Australian government.

Therefore, **I strongly recommend that Schedule 1 be repealed** (given that it simply cannot fulfill its goals, let alone the many other practical problems that will happen as a result of this legislation having been enacted), and that there be a lengthy discussion with the information technology and information security community about how law enforcement can effectively investigate sophisticated criminals. In addition, I hope that the wider Australian community will push for a dialogue over how few human rights protections (such as privacy) we have in Australia – and how we might need to have significant legislation or even an amendment to the Constitution in order to protect the people.

However, the purpose of this review is to *amend* the legislation, so I imagine that "repeal Schedule 1 immediately" might not be seen as a useful comment. I would – as a minimum – request that all of the following amendments (1 through 8, inclusive) be made to the legislation.

1. Permitting the disclosure of far more information about Technical Capability Notices (so long as no reference is made to particular users being targeted) so that other users of the service can be aware of whether the service they are using is still secure enough for their legitimate needs. Aggregated statistics do not provide sufficient information to users about whether they should trust a particular provider. In addition, there is an incentive for some providers to simply lie about how many notices they have received – and users have no way of knowing if they have been mislead as consumers (thus there should be either mandatory reporting, or require that reporting of aggregated statistics be made truthfully or not at all).

2. A more accurate explanation of what a "systemic weakness" is, with an understanding that there exist technologies which simply cannot be secretly backdoored by the company that developed them (instances include free software projects where the source code is publicly published). The laws of mathematics really do trump the laws of Australia in this context. The proposed Senate amendment to do this seemed like a good first step, but it should still be far more explicit — since this is one of the most fundamental limitations in this legislation.

3. Judicial overview over Technical Capability Notices, to ensure that a request is actually valid **before** the notice has been given. Ideally this judicial overview would allow the "designated communications provider" to be present and argue their case.

4. The Government must also provide the aggregated statistics under s317ZF(13), for each "designated communications provider". This would improve the transparency (and trustworthiness) of such statistics – since as far as I know there isn't a restriction against lying about how many notices you've received (within a 6-month window).

5. An explicit statement that an employee cannot be considered to be a "designated communications provider" under s317C in the context of their work as an employee of a "designated communications provider" under the same section. This would massively re-assure people that if a company develops a product then the entire company will receive a notice, and not individual employees. This would mean that companies (especially foreign companies) would no longer be concerned that their employees may become saboteurs.

6. s317C (especially item 6, as well as the scope of "electronic service") should be massively curtailed, as it currently (according to my non-lawyer reading) would include a large number of individuals and companies involved in the software industry. If the purpose of this legislation is to be used for communications software, then that restriction in the scope of targets (for notices) should be clearly present in the legislation.

7. A sunset clause (expiring in 2021) which would require future Parliaments to re-approve this legislation in the future (thus allowing for more public debate of the issue in the future). And by that point, the various agencies requesting these powers must give concrete evidence that the concerns I raised in section II and section V were not justified.

8. If it is necessary for this power to exist, then it should also be given to government anti-corruption commissions, for the express purpose of furthering investigations into corruption within the Government. Though I wouldn't like to start the process of "authority creep" (section VIII) myself, the reason for this proposal is effectively "if we want this power to exist for investigation of the people, it should also be usable for investigations of the Government." After all, if the Government expects the public to eschew their privacy then government officials should lead the way.

By building the mechanism for the Government of today to create backdoors in critical information systems that are used by the vast majority of developers, you are opening yourself to the Government of tomorrow to abuse that power. Laws should be written to not just give power to the Government, but also to protect the people. Hurrying overly-broad legislation through Parliament simply cannot lead to legislation that protects the public sufficiently.

There has been a switch in the past few decades, where now many conversations that would have happened in person now happen using communications software – and

thus the balance of privacy has shifted. Just because technically the communications are now being transmitted through computer networks and not through air vibrations doesn't change the ethics of violating the privacy of the public (law enforcement should be able to do it, but the difficulty of doing it should be proportional to how brazen the privacy violation would be).

Quite contrary to how the Government has painted us, software developers that are developing secure software are not trying to stop the Government from doing investigations. We do want to protect users from malicious adversaries though, and this consideration is more important than making investigations simple. There are far more innocent people than criminals, and thus making software insecure for the majority to be able to catch the few is not (in my view) a reasonable trade-off — especially when there are plenty of methods that law enforcement could employ to catch such people without backdooring encryption systems.

X. REFERENCES

[1] "Telecommunications and other legislation amendment (assistance and access) act," https://www.legislation.gov.au/Details/C2018A00148 (2018).
[2] "Australia's anti-encryption law is so unpopular, there was only 1 comment in support and 342 against," https://www.businessinsider.com.au/australia-spy-chief-is-defending-tola-act-an-unpopular-anti-encryption-law-2018-12 (2018).
[3] "Australia's human rights record attacked in global report for 'serious shortcomings'," https://www.theguardian.com/law/2018/jan/18/human-rights-watch-attacks-australias-serious-shortcomings (2018).
[4] "Human rights watch: Australia," https://www.hrw.org/world-report/2018/country-chapters/australia (2018).
[5] "Un slams australias human rights record," https://theconversation.com/un-slams-australias-human-rights-record-87169 (2017).
[6] G. Williams, "The federal parliament and the protection of human rights," https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/rp9899/99rp20 (1999).
[7] "Gnu general public license (version 3)," https://www.gnu.org/licenses/gpl-3.0 (2007).
[8] https://reproducible-builds.org/.
[9] https://www.gnu.org/proprietary/proprietary-back-doors.en.html ().
[10] https://signal.org/.
[11] https://www.gnupg.org/ ().
[12] https://matrix.org/.
[13] B. Pogorelov and M. Pudovkina, "Properties of the transformation semigroup of the solitaire stream cipher," Cryptology ePrint Archive, Report 2003/169 (2003), https://eprint.iacr.org/2003/169.
[14] B. Schneier, "The solitaire encryption algorithm," https://www.schneier.com/academic/solitaire/.
[15] N. Stephenson, *Cryptonomicon* (Avon, 1999).
[16] A. Kaminsky, "Elsiefour: A low-tech authenticated encryption algorithm for human-to-human communication," Cryptology ePrint Archive, Report 2017/339 (2017), https://eprint.iacr.org/2017/339.
[17] "What's actually in australia's encryption laws? everything you need to know," https://www.zdnet.com/article/whats-actually-in-australias-encryption-laws-everything-you-need-to-know (2018).
[18] "Setback in the outback," https://signal.org/blog/setback-in-the-outback/ (2018).
[19] "Does australia's access and assistance law impact 1password?" https://blog.1password.com/does-australias-access-and-assistance-law-impact-1password/ (2018).
[20] "Tech companies slam new australian law allowing police to spy on smartphones," https://edition.cnn.com/2018/12/07/tech/australia-encryption-law-passes-intl/index.html (2018).
[21] "Here's why labor voted for the encryption laws the party said were flawed," https://www.buzzfeed.com/joshtaylor/labor-this-encryption-law-is-flawed-also-labor-we-voted-for (2018).
[22] "Security experts have cloned all seven tsa master keys," https://techcrunch.com/2016/07/27/security-experts-have-cloned-all-seven-tsa-master-keys/ (2016).
[23] "Inside the nsa's war on internet security," http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html (2014).
[24] "Attacking tor: how the nsa targets users' online anonymity," https://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity (2013).
[25] "What the government shouldve learned about backdoors from the clipper chip," https://arstechnica.com/information-technology/2015/12/what-the-government-shouldve-learned-about-backdoors-from-the-clipper-chip/ (2015).
[26] "Asio says it urgently needs powers forcing telcos to help break phone encryption," https://www.theguardian.com/australia-news/2018/nov/26/asio-says-it-urgently-needs-powers-forcing-telcos-to-help-break-phone-encryption (2018).
[27] "What is the five eyes intelligence alliance?" https://www.businessinsider.com/afp-what-is-the-five-eyes-intelligence-alliance-2017-3 (2017).
[28] "Telecommunications (interception and access) amendment (data retention) act," https://www.legislation.gov.au/Details/C2015A00039 (2015).
[29] "Metadata laws under fire as 'authority creep' has more agencies accessing your information," https://www.abc.net.au/news/2018-10-19/authority-creep-has-more-agencies-accessing-your-metadata/10398348 (2018).
[30] "Councils pry into residents' metadata to chase down fines," https://www.smh.com.au/business/consumer-affairs/councils-pry-into-residents-metadata-to-chase-down-fines-20181114-p50fxr.html (2018).
[31] "List of agencies applying for metadata access without warrant released by government," https://www.abc.net.au/news/2016-01-18/government-releases-list-of-agencies-applying-to-access-metadata/7095836 (2016).
[32] https://www.asd.gov.au/speeches/20181212-tola-act-statement.htm (2018).