OPEN LETTER regarding the Assistance and Access Bill 2018

Dear Minister Dutton,

I write to you to ask that you intervene in the inadequate consultation process that is taking place within your department regarding the draft *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* released in August 2018 (The Bill).

This Bill has aroused unprecedented national and international attention and widespread concern, as it has profound implications not only for Australia and Australians but also for the entire global Internet communications system. This is because, in its current form, the draft bill clearly risks creating unintended security vulnerabilities across Australian and global communications networks, together with potentially harming Australia’s entire IT software and goods export sector. It may also damage Australia’s international standing as a positive supporter, and exemplar of human rights.

At the outset, I wish to make plain that Internet Australia accepts that law enforcement and security agencies need to find ways to enhance their capacities for lawful interception of new and emerging communications technologies. However, they must not do so via hastily enacted legislation which fails to consider the legitimate concerns and advice of global technology experts and carries the very clear risk of creating more problems than it solves.

The eyes of the globe are focussed on Australia and on how we balance the challenges experienced by law enforcement with the expectations of security, confidentiality and privacy of the vast majority of legitimate and law-abiding users, and the ongoing development of future secure and trusted methods of communication. This extremely complex legislation must be carefully examined and given enough time in preparation to be drafted properly. The Government must carefully evaluate and heed the advice of local and global technical and policy experts, to ensure the legislation doesn’t form a cure that is vastly worse than the disease it seeks to address.
1 Publication of submissions to date

More than two weeks after the close of submissions in the Department’s inadequately short call for public submissions, your Department has only published around a quarter of submissions – those from submitters with names beginning from ‘A’ to ‘E’, plus a paucity of others. Just this subset numbers over 120 submissions from other government departments, international and local experts, affected stakeholders, and concerned citizens, indicating the total number of submissions may be more than 500.

Submissions from notable international institutions such as the Massachusetts Institute of Technology (MIT), Stanford University and the Internet Architecture Board (IAB), as well as our own submission amongst many others, have still not yet been published by your Department.

This delay in publishing all submissions robs the public, industry and other arms of Government of the opportunity to learn from the analysis of experts and the concerns of the public, and is contrary to a transparent consultation process normally expected of Government.

2 International Concerns and Consequences

This Bill has global implications, and Australia must be exceedingly cautious in looking at these laws and new capabilities. Unintended consequences and hasty implementation of subtly interconnected requirements impacting the security of global systems could harm the future development of Internet trust and e-commerce world-wide, and hamper Australian industry from competing internationally.

Riana Pfefferkorn from Stanford University’s Center for Internet and Society submitted:

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.\(^2\)

And

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.\(^1\)

The Internet Policy Research Initiative expert group within MIT’s Computer Science and Artificial Intelligence Lab noted several examples where past United States actions related to encrypted


\(^3\) Ibid, P6
communications had caused severe weakening of global systems and directly consequential damage, cost and disclosure or theft of sensitive information – not even by mandating a particular action, but by simply prohibiting action of development of improved systems:

It is worth noting that failed cryptographic protocols can cause outsized damage in unexpected ways that last far beyond when they were discovered to be faulty. For example, the FREAK and DROWN exploits were only possible because earlier regulatory mandates to weaken encryption on products exported from the United States left critical systems perpetually vulnerable as Internet servers continued to support out-of-date software exported under the regulation.

...these so-called “export grade encryption” cipher suites resulted in a class of vulnerabilities that caused colossal damage to the internet infrastructure. At one point, roughly 12% of the top million most visited websites were completely interceptable, allowing attackers to gain user credentials, passwords, and other private data.⁴

and

The examples of Heartbleed, FREAK and DROWN highlight how domestic policy decisions have global implications and can introduce vulnerabilities that extend well into the future.⁵

The Internet Architecture Board (IAB), the overall steering committee of the Internet Engineering taskforce (IETF) responsible for the key technology standards that are used on the Internet, submitted that (emphasis added):

While we normally do not review proposed legislation, We are concerned that this proposal might have a serious and undesirable impact upon the Internet and, taken as a model, the sum of similar legislation may result in the fragmentation of the Internet.⁶

and

We understand that Australia intends to develop appropriate oversight mechanisms to avoid misuse or overuse of these instruments within its borders. However, as custodians of the Internet’s architecture, we are required to take a global view. This approach, if applied generally, would result in the Internet’s privacy and security being the lowest common denominator permitted by the actions taken in myriad judicial

⁵ Ibid., P8
contexts. From that perspective, this approach drastically reduces trust in critical Internet infrastructure and affects the long term health and viability of the Internet.

In making these very serious concerns public, we impress upon you that these comments from the IAB are not restricted to the Internet operating in Australia, but are describing serious detrimental impacts on the entire global Internet communications system, and all the many valuable economic applications and platforms enabled by the Internet worldwide.

We ask you to reflect for a moment on the existence of these submissions from international groups. That these bodies have such serious concerns to have taken the time to make submissions on an Australian legislative process is surely reflective of serious, and widespread global concerns about the potential dangers of the Australian draft legislation.

3 Violation of Human Rights

The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion, David Kaye, wrote from Geneva:

*I also wish to bring to the attention of the Department some of the provisions of the draft Bill that, if adopted, would severely impinge on the rights to privacy and freedom of expression and association, as provided by articles 17 and 19 of the International Covenant on Civil and Political Rights (“the Covenant”), ratified by Australia on 13 August 1980...*

*...I am concerned that the draft Bill is inconsistent with Australia’s obligations under Article 17 and 19 of the Covenant. I am particularly concerned that the draft Bill gives virtually unfettered discretion to agencies to compel providers to modify digital security standards or take other action that would effectively weaken encryption. I urge the Department to reconsider the draft Bill in line with the human rights standards outlined below, as well as my recommendations based on these standards.*

These concerns are shared by the Australian Human Rights Commission, which submitted:

*38. Any improved ability of the Government to conduct digital surveillance, intercept digital communications and collect personal data in a manner that is disproportionate or unnecessary to a legitimate objective risks a ‘chilling effect’ on the enjoyment of human rights, in particular the rights to freedom of expression and privacy.*

---

7 Ibid., P2
9 Ibid., P2
39. The Commission considers that further consideration and refinement of the draft Bill are required to ensure its compatibility with human rights.\(^{10}\)

## 4 Consultation Period is Insufficient

A great many submissions have highlighted that the four weeks provided for comment by the Department after the initial draft was made public was manifestly inadequate for the complexity and vast scope of the Bill.

The Australian Human Rights Commission noted:

> 4. In light of the short timeframe for the preparation of submissions in this consultation process, and the length and complexity of the draft Bill, this submission is not exhaustive. Rather, it draws attention to the key human rights concerns identified by the Commission to date.\(^{11}\)

And its first recommendation was:

> The Australian Government ensure that further and adequate time is afforded for public consultation, review and reform of the draft Bill, to enhance human rights compatibility.\(^{12}\)

The UN Special Rapporteur urged:

> As a threshold matter, given the seriousness of the issues being considered and the length and complexity of the draft Bill, I urge your Excellency’s Government to extend the deadline for comments\(^{13}\)

Internet Australia’s own submission highlighted:

> We consider the four week period provided for review of these papers to be wholly inadequate for such a complex issue with such wide and global ramifications.

> This consultation alone required the review of over 150 pages of explanatory material, and a 174-page draft legislation paper that modifies 9 other items of legislation, requiring the new provisions to be cross-checked against those other documents.

---


\(^{11}\) Ibid., P3

\(^{12}\) Ibid., P8

\(^{13}\) UN Special Rapporteur, Mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, P1, online at https://internet.org.au/images/MediaReleases/OL-AUS-5-2018.pdf
Four weeks is not sufficient to perform such a review comprehensively, so this submission is necessarily incomplete, with other substantive issues likely to be found following deeper review.

Despite these comments, and the huge volume of substantial submissions, the Government tabled the legislation in Parliament largely unchanged just one week after the close of submissions. This suggests to us that, in such a short timeframe, it is very unlikely that serious consideration was given to the many issues raised in the hundreds of submissions received. Furthermore, now the PJCIS review process is similarly hobbled, with a short time for submissions and only a single day allocated for public hearings.

Allocating just a single day for public hearings is extremely short-sighted and, in our view, ill-advised, given the high interest and volume of submissions to the original Department of Home Affairs consultation. The PJCIS will not know how many submissions it will receive or requests to appear at public hearings until at least 2nd October and probably later—only then will the PJCIS be able to assess how many days of hearings it will need to hear from all stakeholders. The process is far too short to enable the many international experts from institutions such as MIT, Stanford and the Internet Architecture Board to plan travel to Australia to appear.

It is also telling that the single scheduled hearing day is only one week after the close of submissions, leaving insufficient time for the Committee to read and fully evaluate all the submissions it is likely to receive - this will in turn reduce the value of the public hearings in assisting the Committee to delve into the many substantial issues, concerns and profound implications raised about the proposed legislation.

This manifestly inadequate consultation period carries with it very real dangers of inadequate preparation and development of appropriate legislation that would give effect to the Government’s oft-stated objective that the requirements of this legislative framework should be “proportionate and reasonable”. It also enhances the very real dangers of unintended consequences that endanger the security and privacy of all Australians. If you rush this legislation, you are very likely to get these things wrong.

5 Effect on Australian export markets.

In August this year the Australian government banned companies “likely subject to extrajudicial directions from a foreign government that conflict with Australian law”15 from participating in Australian future telecommunications infrastructure, and in particular from 5G mobile networks. This ban was largely interpreted and confirmed by Huawei and ZTE as primarily aimed at Chinese-
controlled equipment providers. This ban follows the Australian government’s intervention to prevent Huawei Marine building an undersea cable between Australia and the Solomon Islands, also reportedly on national security concerns.

The ban was reportedly driven by concerns that companies with strong Chinese links are subject to Chinese government control and requirements to act under direction of Chinese intelligence agencies.

This Bill will put in place a regime where Australian companies will be subject to the same suspicions, and effectively viewed by international markets as subject to the very same concerns around undisclosed surveillance and surreptitious bypassing of security and privacy functions at the request or direction of the Australian government. Australian manufacturers of communications hardware, developers of Australian communications software systems, every Australian telecommunications provider active in a foreign country, and in fact every Australian website involved in ecommerce to international markets could be suspected to be insecure by international markets. Under the current structure of the Bill, these concerns and suspicions will arise just by virtue of the legislation existing, even if the legislation is not used.

As the IAB puts it:

*This risk might cause some infrastructure providers to relocate, reduce service or even block service to Australian users. Such fragmentation of the Internet is one of the primary concerns we have today as it reduces the value of a global, highly-connected Internet.*

*The ability to compel compromises to the mechanisms that provide security, privacy, and trust on the Internet erodes trust in the Internet as a whole. That erosion, multiplied by the number of political and judicial contexts in which similar approaches might be adopted, represents an existential threat to both the Internet’s security and its integrity.*

MIT makes a similar point regarding US-based suppliers:

*The marketplace of global technology users, both institutions and individuals, has become sensitized to the risk that national governments may seek to weaken the security of widely-used infrastructure. In the wake of the Snowden disclosures,*

---


companies in the United States faced severe scepticism from non-US buyers and increased regulatory pressure from European governments out of a belief that the US national security agencies had compromised the security infrastructure of major US Internet providers.\(^{20}\)

Statistics from Austrade indicate the value of Australian IT and telecommunications exports in 2016-17 was over AUD$3.2billion\(^{21}\), and the value of other exports and commerce enabled by Australian websites is incalculable.

It would be a national tragedy if Australian exporters of IT systems and software were harmed by international bans and security concerns for precisely the same reasons Australia has chosen to ban foreign IT companies from our telecommunications projects. This harm is a very real risk arising from this Bill through your Department being considered in its current form.

### 6 Call for your action

Minister Dutton, this entire process by your Department of railroading a single draft Bill, inadequate consultation, and lack of any effective engagement with the technical and policy expert community and stakeholders needs to be corrected. This manifestly inadequate consultation process and rushed introduction risks Australia’s international reputation as well as many billions of dollars of IT “smart economy” exports, the very type of “smart, high-value, export-focussed industries” the Government identified it wishes to support in its 2016-17 Budget\(^{22}\).

I call on you to intervene and:

1. Require your Department to accelerate the publication of all the remaining submissions to its enquiry, to inform the community and now the PJCIS members of the range of submitters and their concerns.
2. Allow the PJCIS the time it will require to properly evaluate all the submissions it will receive, and schedule as many public hearing days as it needs to become fully informed of the consequences and dangers for the public and for the global communications infrastructure if this Bill proceeds unchanged.
3. Require your Department to consult publicly and transparently over multiple rounds, and to institute a series of meetings and workshops with affected industry bodies to consolidate feedback and further review of future drafts, similar to the extensive consultation process that occurred with the introduction of metadata retention requirements and the Telecommunications Sector Security Reforms legislation.


4. Commence a multistakeholder process of engagement with national and international experts in policy, technology, communications systems engineering, and human rights in the workshops and rounds of document revision, to ensure the best chance of achieving balanced, world-class legislative outcomes.

5. Be mindful of the risks advised by local and global experts of profound damage to global Internet operations and communications systems, and to proceed slowly and cautiously with developing this currently dangerous and unworkable Bill into active legislation.

About Internet Australia
Internet Australia is the not-for-profit organisation representing all users of the Internet. Our mission – “Helping Shape Our Internet Future” – is to promote Internet developments for the benefit of the whole community, including business, educational, government and private Internet users. Our leaders and members are experts who hold significant roles in Internet-related organisations and enable us to provide education and high level policy and technical information to Internet user groups, governments and regulatory authorities. We are the Australian chapter of the global Internet Society, where we contribute to the development of international Internet policy, governance, regulation and technical development for the global benefit.

Yours Sincerely

Dr Paul Brooks
Chair – Internet Australia
chair@internet.org.au