



12 October 2018

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

Via email: [pjcis@aph.gov.au](mailto:pjcis@aph.gov.au)

**Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018**

ACCAN thanks the Parliamentary Joint Committee on Intelligence and Security for the opportunity to comment on the draft *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*.

The Australian Communications Consumer Action Network (ACCAN) is the peak body that represents all consumers on communications issues including telecommunications, broadband and emerging new services. ACCAN provides a strong unified voice to industry and government as consumers work towards availability, accessibility and affordability of communications services for all Australians.

We strongly support the submission to this consultation made by Internet Australia. In particular the following recommendations:

- That the Government seriously consider the many substantive submissions received by the Department of Home Affairs
- That a more thorough consultation process be conducted, including holding meetings and workshops with key stakeholders
- That there be processes in place such as a consultation period to assist providers when they are issued with a request or notice to understand and meet their obligations
- That there be consideration of including a size threshold for organisations that are going to be subject to the Bill, such as the upper threshold of the ATO's definition of small business
- That there be consideration of including a process for how an organisation can be formally exempted from the requirements of the Bill if they can demonstrate they are unable to facilitate access to encrypted communications
- That component manufacturers and suppliers be removed from the list of 'designated communications providers

Australian Communications Consumer Action Network (ACCAN)  
*Australia's peak body representing communications consumers*

---

PO Box 639, Broadway NSW 2007

Tel: (02) 9288 4000 | Fax: (02) 9288 4019 | Contact us through the [National Relay Service](#)

[www.accan.org.au](http://www.accan.org.au) | [info@accan.org.au](mailto:info@accan.org.au) | twitter: [@ACCAN\\_AU](#) | [www.facebook.com/accanau](http://www.facebook.com/accanau)

- That an agency be established to be a single point of contact for providers for all Requests and Notices under the Bill
- That providers should be able to recover costs expended to meet the obligations of a Request or Notice
- That the Government considers creating adequate guidance documents about systemic weaknesses and vulnerabilities

Further to this, given the complexity and broad scope of the Bill, ACCAN comments relate to the aspects of the Bill that will impact consumers. We also note that ACCAN is part of the 'Alliance for a Safe and Secure Internet', alongside other consumer and human rights organisations, industry representatives, and technology companies and experts. The concerns of the Alliance were voiced in a media release from October 3 2018<sup>1</sup>.

### **The lack of quality consultation**

ACCAN would like to echo the serious concerns expressed by Internet Australia and many others in their submissions made to the Department of Home Affairs regarding the manner in which the consultation for this Bill has been managed. The Bill proposes modifications to nine pieces of legislation and includes a lengthy explanatory document. The four-week timeframe provided by the Department of Home Affairs for public consultation on a very complex Bill that requires reviewing and cross-checking various legislation is completely inadequate.

Further, the lack of transparency that has been afforded to the consultation is highly concerning. The Department of Home Affairs failed to publish all of the submissions it received in a timely manner and only finished doing so three days prior to the PJCIS consultation deadline. ACCAN considers that given the significance of the proposals in the Bill and the serious detriment that would face consumers if adequate changes are not made, this consultation both requires and deserves complete transparency.

We note also that grave concerns have been made by many stakeholders from a range of different sectors, including the telecommunications industry, technology sector, and human rights and consumer organisations, from both within Australia and globally. The first round of consultation to the Department of Home Affairs received hundreds of submissions. These included very notable global stakeholders, including Stanford University, the Internet Architecture Board and the Massachusetts Institute of Technology. All felt compelled to weigh in on the proposed legislation given the wide-reaching ramifications for the global internet and technology sectors. Despite the considerable alarm being raised about the Bill, the Department of Home Affairs made few changes to the draft Bill before submitting it to the Australian House of Representatives.

Given the widespread concern about the Bill, ACCAN strongly recommends that PJCIS ensure this Bill undergoes a more in-depth consultation process. We are pleased that PJCIS has extended the number of days for public hearings on the Bill, and urge that the timeframe for the hearings is adequate to ensure all viewpoints can be heard. Beyond this, as recommended by Internet Australia,

---

<sup>1</sup> Digital Rights Watch 2018: <https://digitalrightswatch.org.au/2018/10/03/slow-down-stop-and-listen-consumers-human-rights-groups-industry-telcos-and-technology-companies-join-forces-to-sound-alarm-at-governments-spyware-legislation/>

consultation for this Bill must include a series of meetings and workshops with industry and relevant sector stakeholders, consumer representatives and the public so that feedback can be properly collated, published, debated and for subsequent iterations of the draft Bill to be considered. This will also allow time to develop case studies and processes to better understand and scrutinise how the Bill could and should work in practice.

### **Consumer privacy**

Consumer use and reliance on telecommunications, the internet and their technology devices has grown significantly in recent years. Telecommunications is now an essential service and most consumers take for granted their ability to quickly communicate with others using the phone and internet. Consumers use the internet to conduct business, banking and finances, shopping, research, to engage with government, access entertainment, book travel, and much more. Consumers also assume and trust that when using their devices and the internet, their activities are private and secure and their personal safety and privacy is protected through robust safeguards such as strong encryption, sophisticated software systems, and privacy laws.

These safeguards must continue to work in favour of consumers, protect their privacy and promote personal freedom. Consumers place great importance on privacy and are now more than ever wary about how their personal data is being stored, used and in some cases exploited by large corporations and governments. The Cambridge Analytica case<sup>2</sup> earlier in 2018 illustrated the ease at which companies are able to collect information about millions of consumers without their knowing and then potentially use that information for their own or government interests.

Research by the University of New South Wales illustrated the risks that come with an increasingly connected world. Internet of Things (IoT) devices mean that almost every aspect of our lives can be connected to the internet. It was estimated that in 2017 the average Australian household had 13 devices connected to the internet and that this will more than double by 2021<sup>3</sup>. Unfortunately there are also risks with these levels of connectivity. It makes it possible for both device providers to collect personal data about consumers on an unprecedented level, and for hackers to break into systems and steal personal data<sup>4</sup>. Identity theft is also a very real concern. Research by IDCARE found that consumers are at risk of identity theft when using social media, the telephone, and online accounts<sup>5</sup>.

Whilst ACCAN supports the government's endeavours to provide strong national security and the need to adapt legislation and technology to intercept certain communications and data, to access consumer communications and data by law enforcement agencies must be underpinned by an appropriate balance between security and privacy. Striking this balance must be done delicately and with adequate consideration given to consumer interests as well. Consumers need to know that when the government conducts surveillance activities, it is also ensuring their privacy and safety is protected.

---

<sup>2</sup> <http://www.abc.net.au/news/2018-03-18/cambridge-analytica-suspended-by-facebook/9560272>

<sup>3</sup> UNSW 2017, Inside job: Security and privacy threats for smart-home IoT devices: [http://accan.org.au/files/Grants/UNSW-ACCAN\\_InsideJob\\_web.pdf](http://accan.org.au/files/Grants/UNSW-ACCAN_InsideJob_web.pdf), p.3

<sup>4</sup> Ibid., p.5

<sup>5</sup> IDCARE & ANU 2016: [http://accan.org.au/files/Grants/ANU%20ID%20theft/ANU%20ID%20theft%20infographic\\_ICT.PDF](http://accan.org.au/files/Grants/ANU%20ID%20theft/ANU%20ID%20theft%20infographic_ICT.PDF)

ACCAN believes that the proposals in the *Assistance and Access Bill* would act to significantly erode consumer privacy and safety. Current regulatory arrangements for accessing or intercepting encrypted communications and data are underpinned by the need to protect people's privacy and safeguarded by adequate judicial oversight. The proposals in the *Assistance and Access Bill* however would increase the ability for the government to obtain access to consumers' encrypted data and devices. It will enable a much higher level of government surveillance over citizens and enable governments to harvest people's data without their knowing.

The proposals in the legislation will act to weaken encrypted systems by forcing technology companies to develop tools that make it easier to access encrypted data. Whilst the purpose of this is to assist government in law enforcement activities against criminals and terrorists, it will also enable criminals easier access too. This unintended consequence poses far too great a threat to consumer privacy and personal safety. ACCAN is also greatly concerned about the lack of transparency and judicial oversight for orders made to technology companies to facilitate government access to such data.

Privacy is a basic human right that must be respected and given due regard when developing legislation such as the *Assistance and Access Bill*. Consumers experience significant detriment and feel violated, exploited and a loss of security when their privacy is breached. As such, ACCAN strongly recommends that the PJCS take adequate time to consider, amend and ensure the Bill properly balances consumer privacy and national security interests.

## **Conclusion**

Reliance on devices and the internet is integral to daily life and consumers must be able to trust that their privacy is protected without concern that government is creating backdoors to enable greater surveillance and storage of their data, whilst also enabling easier access for terrorists and cyber criminals.

The *Access and Assistance Bill* is wading into relatively uncharted territory, with only the UK having developed similar legislation. Australia must get this right as it will set a precedent on the global stage with many other countries likely to follow suit. As such, if amendments are not made that ensure consumer privacy and security are safeguarded against criminal activity, the detriment to consumers will be felt on a much greater scale.

Sincerely



Teresa Corbin

ACCAN CEO