Submission: Comments on The Assistance and Access Bill 2018

Addressed to:
Department of Home Affairs
assistancebill.consultation@homeaffairs.gov.au

10 September 2018

Contributors

This submission was prepared by Dr James Jansson, Drew Wolfendale, Dr Andrea Leong, Andrea Finno and Michael Maroske on behalf of the Science Party. Some of the contents of this submission have previously appeared on the Science Party website.

Contact details

Email: secretary@scienceparty.org.au

Confidentiality

This submission does not need to be kept confidential and may be made public.

Summary of Issues

Assistance and Access Bill 2018 seeks to allow law enforcement agencies to issue “technical assistance notices”, and the Attorney General to issue “technical capability notices”. The former would legally oblige communications providers to assist in decrypting encrypted messages to the extent of their capability. The latter would oblige those providers to build access capabilities to assist in intercepting communications.

While there is no doubt that this law would indeed make it easier for law enforcement to access encrypted communications, this is not a reasonable step to take to ensure the safety of Australians. It is not only disproportionate; it also introduces new, unacceptable risks:

- Device access laws increases national security risks by enabling a broad risk of hacking to all devices.
- This human rights violation is a serious threat to our democracy.
- The government asserts that it can’t force a systemic weakness to be built or maintained, which contradicts the intent of the law.
- This law risks sending innocent people to gaol—for even longer! The only way to be safe from prosecution under this law is to not own any electronic devices whatsoever.

Each of these points is discussed below.

In summary: the Science Party recommends, in the strongest terms, that the capabilities allowed for by the Assistance and Access Bill 2018 be condemned to the scrapheap.

Device access laws increase national security risk by increasing the attack surface for hacking on all devices

The implementation of this law will create one of the world's largest reservoirs of high-value security holes for hackers to take advantage of, in terms of obtaining access to personal devices. It will be hard to control access to exploits and the networks of the Australian Federal Police (AFP), Australian Security Intelligence Organisation (ASIO) and other policing bodies when so much valuable information can be obtained by hijacking a single law enforcement agency.

Security through distributed control is an important part of modern security practices. Placing potential access to all important information in a single location creates an attractive target for international spies and corporate espionage agents.

To suggest that ASIO, AFP and other policing bodies are impenetrable to foreign spies defies history. For example, the blueprints of the new ASIO building were leaked (possibly to or by the Chinese government) before ASIO had a chance to move in[1]. The result of this disclosure of information led to the agency failing to move into the building[2], as it was considered a security risk.

With the introduction of this legislation, mobile phones that are in Australia will be considered to be a security risk by individuals with a high requirement for security. The risk of privacy loss could also render Australia unattractive for non-essential travel. Many ordinary people rely on the security of electronic devices, which means a compromised personal device could mean access to a large organisational or governmental network.

These include:

- Government utilities such as power, water and transport networks
- Private utilities such as telephone and internet networks
- Banking infrastructure
- Major shopping centre chains which have a critical position in terms of the logistics of food supply to our urban centres

This human rights violation is a serious threat to our democracy

There is a chilling effect when people are spied upon. This effect extends to when people know there is even a small possibility that they could be spied upon. This act effectively renders all electronic devices compromised from the perspective of keeping information secret from the current ruling party, or any future ruling party.

The federal government has shown itself to be hostile towards whistleblowers. The Commonwealth Director of Public Prosecutions has pursued a case against East Timor whistleblower Witness K and their lawyer, for conspiring to release information about immoral spying by Australian Secret Intelligence Service (ASIS) to assist the government in oil field negotiations[3]. In a punitive move against Andy Fox, who criticised the government, the government misused Fox's private welfare information by releasing it to the media[4].

[1] http://www.abc.net.au/news/2013-05-27/asio-blueprints-stolen-in-major-hacking-operation/4715960
[2] http://www.abc.net.au/news/2014-07-23/asio-building-in-canberra-remains-empty-a-year-after-opening/5618544
[3] http://www.abc.net.au/news/2018-06-28/witness-k-and-bernard-collaery-charged-intelligence-act-breach/9919268
[4] https://www.theguardian.com/australia-news/2017/feb/27/centrelink-recipients-data-released-by-department-to-counter-public-criticism

The current government wants the Australian people to trust them with their private data and security, but it lacks the credibility needed to make such requests. Any such trust would be misplaced and irresponsible, especially considering this bill's impact on freedom of speech.

The increased difficulty and perceived legal danger associated with reporting illegal activity to media and other policing agencies due to poor whistleblower protections means that such activity will be reported less. This increases the confidence of bad actors in our political system (including convicted criminals and people taking illegal donations that were members of both major political parties), and encourages an increase in illegal activities.

The government asserts that it can't force a systemic weakness to be built or maintained, which contradicts the intent of the law

There is a contradiction between the methods of requesting data and the limitations and safeguards for said requests.

Section 317ZG of the Bill states:

> "Designated communications provider must not be required to implement or build a systemic weakness or systemic vulnerability etc."[5]

In contrast, various sections of the accompanying Industry Assistance Fact Sheet state that no systemic weakness will be mandated, but the explanation of the 'Technical Capability Notice (TCN)' states:

> "If a designated communications provider is ordered to provide assistance under a TCN, they must provide that assistance, including building a capability or functionality to provide that assistance."[6]

Any out-of-band method used to grant access of a user's secure data to a third party has the potential to be exploited by other parties with more malicious intent. Therefore, any of these methods must be interpreted as a "systemic weakness or vulnerability".

Illegal access needs to be prosecuted, but likely will not be

Telecommunications metadata was illegally accessed almost as soon as the Telecommunications (Interception and Access) Amendment (Data Retention) Bill came into force. The federal government, after making assurances that appropriate checks and balances were in place to

[5] https://www.homeaffairs.gov.au/consultations/Documents/the-assistance-access-bill-2018.pdf
[6] https://www.homeaffairs.gov.au/consultations/Documents/industry-assistance-factsheet.pdf

protect freedom of speech, was quickly found to have had insufficient protection against unauthorised access of metadata.

In early 2017, an AFP agent accessed the call records of a journalist without a warrant[7] (warrants are required to access metadata in a select few cases, including for journalists, while the vast majority of our metadata can be accessed without one). Commissioner Andrew Colvin said the agent had no "ill will or bad intent". It is good to know that the AFP is hiring nice people. It is deeply concerning however, that the process intended to protect our individual rights (the requirement of a warrant) was so easily thwarted by someone in the AFP incompetent enough to allow illegal access. The curators of this data must be held to a higher standard than that of the average citizen.

Given that the metadata retention laws were freely broken without any consequence for the employees of the organisation that broke it, we can be fairly sure that illegal access made possible by this new law is also unlikely to be punished. Access to devices and the ability to remote control them come with huge responsibility and is of national security importance. There clearly is not sufficient disincentive in organisations like the AFP to prevent agents from accessing information or to prevent systemic access failures.

This law risks sending innocent people to gaol—for even longer!

Extending gaol time for failing to provide secret keys to encrypted data extends an already terrible law. For most practical purposes, an encrypted message is indiscernible from random noise. The only way to distinguish between encrypted content and random noise is to have access to the private key. As such, a person with white noise on their device, or any files not encrypted by them on their device, could be subject to long gaol sentences.

Below we outline four different ways that an innocent person can be prosecuted under this law, by being incapable of producing encryption keys for data in their possession.

1) Being sent encrypted information or white noise

Users are not always explicitly in control of the information that is downloaded and stored on their computer. A demonstration of this is below:

```
rNYUHxeR5yCdIb79d2TYRognDAo9cPQW2autiPO6sdPp=
```

```
sEKFkTCWAdDk/EbN0zcH8TJ6SZZFgcJ9nmWVfTGdzBw=
```

[7] http://www.abc.net.au/news/2017-04-28/afp-officer-accessed-journalists-call-records-in-metadata-breach/8480804

The first string is effectively just random noise (generated by https://random.org). No information can be gathered from this string.

The second string contains encrypted information. The information says, “This law is a bad idea,” and is encrypted using 128-bit AES with the very simple password “password1”, which was simply performed on the website https://aesencryption.net. There are many other sites providing this functionality, and the functionality is in-built in all modern web browsers.

The first string looks very similar to the second string. If we did not include this password to the second string, the reader of this report would not be able to tell if there is information in the second string. In fact it is impossible for the reader (or anyone else, including our best spies) to know if either string contains encrypted information.

Unfortunately, it is impossible to prove that the first random string does not contain information. As such, this report becomes a legal liability for someone likely to be searched and carrying an electronic device with this report stored on its internal storage.

Merely deleting the file will not work. Deleting a file from a device only marks the space as available to be written over. If you have downloaded this as a PDF to your drive, a silent copy can remain on your drive. Terrorists, child exploitation material peddlers and other nefarious people can use this fact to transfer data as “deleted” and use a disk recovery tool to retrieve the information. Likewise, police can also use a disk recovery tool to find the deleted information. If they find this submission by the Science Party, and you cannot provide the encryption key to the first string, you are at risk of going to gaol.

If you are likely to be searched (for example, crossing our border), the only way to ensure that this report doesn’t get you into trouble under this law is to throw out this device and get a new one.

Unfortunately, this will likely be insufficient. Pieces of seeming non-sense are routinely downloaded and stored in the cache on our devices every time we surf the web, all without our knowledge. All of this seemingly random data could hold encrypted information, and ultimately puts you at risk, whether you are crossing the border, or your computer is under investigation for any other reason. The only way to be safe from prosecution under this law is to not own any electronic devices whatsoever.

2) Buying a second-hand computer

As discussed above, deleting a file doesn’t mean that it is gone. The deleted information can still be recovered. If you receive a computer, even one with a fresh install, and do not reformat the hard drive with white noise to replace hidden deleted files, you are at risk of being prosecuted for not providing the encryption key to information on your personal device.

3) Owning a computer with a white-noise cleaned hard drive

That second hand computer we bought above, with which we tried to do the right thing by wiping the hard drive with white noise now suffers from the same problem in point 1) above: white noise and encrypted data are impossible to tell apart.

4) Receiving any image or sound

Steganographic[8] techniques mean all data could contain encrypted information. By taking an image and changing some of the pixels ever so slightly, we can send this new image to a friend with a message inside of it.

The United States Federal Bureau of Investigation (FBI) reported that Russian foreign agents used steganographic techniques to send encrypted information on public networks[9]. As the method simply relies upon similar but slightly different images being sent as a means of communicating cryptographic information, all pictures effectively become a means for storing encrypted information.

If your computer holds a copy of a picture of a dog, and its brightness and contrast of some pixels are slightly different to another version on the internet (which can be caused simply through re-saving an image), an enforcer of this law may find the difference between the two images, and present you with a long string that they could ask you to decrypt. Unfortunately for you, despite the fact that it will look like random noise, there is no way to prove to the law enforcement agent that there is no encryption key for this random noise.

All people are at risk of being punished under a law which fails to take into consideration that encrypted data and white noise is transmitted and stored routinely, and most people have no way of unlocking this data.

For all the reasons detailed above, the Science Party is strongly opposed to the provisions enabled by the Assistance and Access Bill.

[8] https://en.wikipedia.org/wiki/Steganography
[9] https://www.justice.gov/sites/default/files/opa/legacy/2010/06/28/062810complaint2.pdf