

Adam Nelson  
[REDACTED]

Re: The Assistance and Access Bill 2018

Good morning or Afternoon

I am Adam. I am an experienced IT Service Professional with over 8 years' experience working for government, telecommunication and private sector.

I run things, fix and protect things. Sometimes, I write about things and provide written advice about those requested things to engage governments as shareholder rather than retweeting or like it. Rather than alternative where nobody says something and everyone Complains.

This is my second submission to the Australian government on matter relating to privacy, security and general internet

I write to express my concerns over the draft legislation titled 'The Assistance and Access Bill 2018', Some people are calling this the 'Ass Bill'. Because this just smell bad and rotten smell come from those inside the local Australian government, enforcement agency, local and international intelligence services; whom want to undermine citizen right to privacy protections and general freedoms of internet/app usage

These same people made you write a law about covering your government mistakes. Such as

- Providing warrantless access to data without a judge,
- Where access, abuse, misuse to this data isn't punishable offence. Local law enforcement have already demonstrated some incompetence
- If you report on our mistakes. At the government discretions you, your lawyer, or media person can go to Jail for embarrassing the government or making us look evil.

Imagine that first conversation with a cell mate charged with murder or domestic violence. "What you hear for?" and your answer is "Reporting or commenting on the news online...."

As many other have raised concerns on how this bill should be implemented or

#### 1. This Bill would harm cybersecurity

This Bill would require companies to provide information about how their systems work. It would allow more people physical access to networks. It would require organisations to test and install new functionality built by the government. These measures would undoubtedly introduce new threats and vulnerabilities into the systems that we all use each day.

#### 2. This Bill would lead to an increase in government hacking

This Bill grants government officials power to both compel organisations to reveal information about their systems and to make changes to those systems. Combined with the government's new ability to issue warrants to seize information directly from devices, this would empower Australian government agencies to develop and grow their hacking capacities without vital and necessary protections. Any government hacking must come with strong safeguards given the high risk of harm. While the orders issued under this authority must be reasonable and proportionate, there is nearly no limitation to ensure that the government would not use any vulnerabilities it uncovered around the world or share that information with its allies.

#### 3. This Bill could create a backdoor into end-to-end encryption despite assurances to the contrary

Whilst the Bill does specifically prohibit the government from mandating a systemic weakness in an encrypted system, the ambiguity in the use of the term "systemic" will highly likely be exploited, and will result in less trust in technologies deployed in Australia. It may be that a company could be compelled to use its software update mechanism to interfere with the system of a specific user. Such a function would undermine faith in software updates, leading users not to update. That means more unpatched systems and overall harm to cyber-security.

#### 4. This Bill is a huge overreach into the fundamental workings of our digital world

What is next? Everytime you bring out a new surveillance power you try to adapt the laws to changing technology with little understanding how your making this worse for yourself. Your creating a feedback loop. What a feedback loop? To quote wikipedia

**Feedback** occurs when outputs of a system are routed back as inputs as part of a chain of cause-and-effect that forms a **circuit** or **loop**. The system can then be said to feed back into itself.

You create a new law. Someone find a workaround, This upsets law enforcement whom cry wolf everytime and ask for a new law. New laws are drafted because law enforcement find that don't already have enough powers. You can see we get stuck in a feedback loop and lack of consultation with industry stakeholders who have general concerns around privacy and freedoms

The Tech companies who dare to innovate and protecting those important freedoms of internet or those whom have a right privacy. These companies are being fair, balanced democracy and allow reporting on the news or making youtube videos without the fear of being prosecuted.

As drafted, this Bill would authorise vast new powers to authorities with almost no understanding of the limitations, the implications, or oversight mechanisms. Encryption protocols are the backbone of the digital economy, facilitating every single transaction online. Any attempt to weaken these will be a risk that no other democracy is taking. Strong encryption is essential to the modern Australian economy, and it would be a mistake to deliberately weaken it.

The access bill can be used with other laws as advantage. But can be seriously abused and misused in unreasonable way that is proportionate

Warrantless access to data whether be encrypted or unencrypted is dangerous without audit or federal, state employee and international partners punishment whom do the wrong thing. May you look to example in QLD Police; Where Queensland police computer hacking: no action taken in nearly 90% of cases.

To quote the guardian

<https://www.theguardian.com/australia-news/2018/aug/02/queensland-police-computer-hacking-no-action-taken-in-nearly-90-of-cases>:

Renee Eaves, a social justice advocate, found out through a right to information request in 2016 that her personal information had been accessed 1,400 times since 2008. She does not have a criminal record

I urge the government to consider how this Bill, in its current draft form, could damage the way that I, and many other Australians, use digital communications on a daily basis. I am also concerned about the impact on my rights - particularly the right to privacy.

Thank you

Adam Nelson

Heres a picture of a cat for those whom are reading this

