From: [redacted]
To: Assistance Bill Consultation
Subject: Opposition to Assistance and Access Bill 2018
Date: Sunday, 9 September 2018 10:56:14 PM

I am strongly opposed to the invasive, dangerous, ambiguous and unnecessary powers proposed in the Assistance and Access Bill 2018.

I recognise a need for law enforcement and intelligence agencies to intercept and monitor communications and electronic devices belonging to individuals convicted or credibly suspected of serious criminal activity. I accept that such activities, while invasive are carried out in the interests of ensuring public safety. But government agencies already have tools to access devices. Both Android and Apple mobile phone systems are already susceptible to commercial level spyware marketed and sold to corporations and the public, such as the software packages offered on spycity.com.au and spousebusters.com.au. The Sydney morning herald reports that Agencies including the Australian Federal Police, the Department of Defence and the Australian Securities and Investments Commission have previously been confirmed to use phone intrusion technologies developed by Cellebrite technology.

The FBI was also able to access an encrypted apple device during investigation into the San Bernardino incident. I find it hard to believe the US, a fellow member of the five eyes network, has not shared that capability, or technical knowledge gained from their efforts with Australia. If mobile phone and computer keylogging and screen capture software is available to civilians in Australia, the same (if not more powerful tools) are already used by our government agencies.

Framing this bill as a necessary response to empower outmatched law enforcement and intelligence agencies seems disingenuous and ignorant to the intricacies of the subject matter at best and deceptive at worst. While the contents of certain encrypted messaging services themselves may be beyond the reach of law enforcement when in transit the devices used to compose, send, receive, read, store and ultimately use them remain accessible to anyone using currently available methods and tools.

The powers in this bill are a dangerous and invasive over-reach in their current draft form. Parties subject to an order under this proposed legislation are forbidden from discussing it under heavy penalty. Parties also cannot be subject to any civil legal action as a result of complying with an order. When complying with a requirement to create or modify tools or systems to allow access to information or communications results in unauthorised access, release, dissemination or theft of private information by a criminal party (be it a an individual, organised group or foreign state actor) how can individuals be warned or notified? How will disenfranchised individuals or groups be able to seek recourse and compensation if companies are protected as a result of this bill?

Will the government foot the bill if they are ultimately responsible for ordering the process that enabled access? Will the government be required to report such breaches? Will they do so voluntarily? When invasive surveillance is carried out, there should be clear guidelines, codes of conduct and repercussions for breaching those guidelines.

Article 12 of the universal declaration of human rights, Which Australia has a commitment to upholding states “No one shall be subjected to

arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."
Installing or creating access points in technology to more easily survey a few people threatens the cyber security and privacy of every user of that technology, unnecessarily imposing on the right to privacy.

Again I strongly oppose this draft legislation along with many other individuals, experts and interest groups. I also call on the government for greater honesty, transparency and communication around the intersection of law enforcement, legislation, encryption and technology matters

Tom – a concerned citizen