From: Moshe Reuveni
To: Assistance Bill Consultation
Subject: Assistance and Access Bill 2018 Feedback
Date: Thursday, 6 September 2018 6:19:03 PM

Dear sir/madam,

I would like to express my objection to the proposed Assistance and Access Bill 2018 (The Bill). As I will outline below, The Bill demonstrates deep misunderstanding of contemporary telecommunications, The Bill will jeopardise the security of Australians as well as the rest of the world, and The Bill runs the risk of turning Australia from a society of free thinkers into a society of East Germany like people worried about their every move.

To start, the explanations provided in support of The Bill on The Bill's internet page itself (see https://www.homeaffairs.gov.au/about/consultations/assistance-and-access-bill-2018) demonstrate the government's lack of understanding in the areas it is aiming to regulate so aggressively through the proposed Bill.
For example, the page cites a sex offender whose use of Snapchat and Facebook Messenger prevents the Victoria Police from collecting evidence on the case. However, in real life that will not be the case: Snapchat is probably one of the least secure popular messaging platforms, and should allow the police to easily retrieve all communicated data using existing procedures (e.g., a warrant). Given court approval, a police appointed hacker will have no problems retrieving message data, although it should be even easier for the police to acquire the data from Snapchat itself.
Similarly, Facebook Messenger should not pose much of a problem to the police, either. By default, Facebook Messenger does not use end-to-end encryption. Further, Facebook collects messages' metadata, which it will serve the police when issued with a warrant, therefore allowing the police to connect the dots even if encrypted messaging was put to use. And let us not ignore the fact the police can already collect most, if not all, of the evidence it requires from the victim's phone.
To summarise the point, there is nothing in the single example cited in support of The Bill that cannot be achieved, and easily so, using legal methods currently available to the police. This example not only demonstrates lack of understanding in matters of technology on behalf of the government proposing The Bill, it actually demonstrates quite effectively the rather redundant nature of the proposed Bill when it comes to crime fighting.

Further, I - as well as all cybersecurity and encryption experts, who are unanimous on this - argue that the proposed Bill will harm the cybersecurity of Australians rather than improve it. In actual fact, it would harm the cybersecurity of all the citizens of the world, since we all rely on the same technology and mathematics to protect our banking, commerce, private messaging, and even nude photos that we would prefer to keep to ourselves. (I know nude photos do not sound like much in comparison with commerce and banking, but they do seem to carry a lot of significance with a large proportion of the population.)
The reason The Bill will be harmful to the security of Australians and the rest of the world is that its implementations would create backdoors into otherwise private online interactions. While The Bill claims it will not create a backdoor, that is exactly what it will create: there is no other way to break the encryption algorithms in current use other than a backdoor; it is mathematically impossible. The only point of contention remains the exact definition of the term "backdoor", but semantics aside, a backdoor by any other name is still a backdoor.
The problem with such backdoors is that, once created, we cannot prevent them from being used only by "the good guys". Nor can we prevent their abuse, which is likely to be high given the complete absence of oversight offered by The Bill and the oppressive measures it

will enforce on those informing the public of its application (measures that might befit Putin's oligarchy, but certainly have no place in Australia).
For example, if Apple develops a way for Australia to hack into iPhones, that same method can be used by Russia, China, and the entire collection of criminal hackers who would love to put their hands on the sensitive data we all store on our smartphones these days. There is simply no other way about it, which is exactly why The Bill would be harmful to the interests of Australia's citizens and put Australian businesses at a disadvantage against their international competition. It is obvious international companies would prefer to avoid the potential scrutiny of the Australian government.
Eventually, the proposed Bill would put the entire world at risk. Examples for the problematic way in which government backdoors can go wrong include the famous WannaCry, which was originally developed by the NSA as a backdoor. WannaCry then fell into the hands of people on the wrong side of the fence, probably North Koreans, and shut down the UK's health services for a while. It still continues to harm the world economy, putting all manufacturing at Taiwan's TSMC, the world's largest computer chip manufacturer, to a halt just the other month (refer to https://www.bankinfosecurity.com/chipmaker-tsmc-wannacry-attack-could-cost-us170-million-a-11285 for details). I am thus very much puzzled by an Australia that seeks to walk down the same path and put the world's cybersecurity at risk: if the NSA with its multibillion dollar budget, the biggest and mightiest in the world, can fail to protect its trade secrets, what chance does Australia stand?

Lastly, I will argue the proposed Bill stands against the core values of Australian society. The values that make Australia the great country it is, a society of free thinkers, where entrepreneurship is encouraged, and individual initiative is highly regarded.
Do we really want to subdue the free spirit of our society by creating, instead, a country where people know every form of communication they have with their fellow citizens is monitored and surveilled by others (be it government agencies, but also - as previously noted - foreign governments and criminals?).
Science has already told us people behave differently when they know they are being observed (refer to the Observer Effect or the Hawthorne Effect, https://en.wikipedia.org/wiki/Hawthorne_effect). Australians do not need to experiment on ourselves to know what a society of mass government surveillance would be like: we need only look at China. China's internet resembles the one our Bill aspires to create: an internet where no one can keep a secret from the state through the abduction of all form of privacy. All this has been achieved by delegalising all manner of encryption.
Let there be no doubt about it: these days, removing the means with which people can securely and privately communicate electronically amounts to removing people's core freedom; electronic communications are where the bulk of today's communications lie. For some people it represents the entirety of their communication with the world at large.
We therefore need to ask ourselves: Do we want to become another China? I think that is a rhetorical question. I doubt any Australian would prefer to live in China over Australia; similarly, Australia is often cited as one of the best countries in the world to migrate to, whereas I am yet to hear of anyone who seeks to migrate to China.

I therefore urge for the Assistance and Access Bill 2018 to be dropped. As I have demonstrated, it has been wrongfully raised in the first place; it will put Australians at a disadvantage; and it will actively harm Australians as well as the rest of the world.
Let us keep Australia as one of the best places in the world to live at. Let us not imitate the East German Stasi ideal. Let's stop this bill and keep Australians free.

Sincerely,
Moshe Reuveni

Melbourne