From: John Mifsud
To: Assistance Bill Consultation
Subject: Critique of The Assistance and Access Bill 2018
Date: Monday, 10 September 2018 10:54:21 PM

Greetings Honourable Members,

I am a active professional in the Information Technology industry for 30 years, I offer a critique of the The Assistance and Access Bill 2018 herein "this Bill".

The first and most obvious contradiction is that this bill cannot achieve its intended objection of monitoring paedophiles and terrorists because there is nothing to stop these parties from writing their own software. There is nothing extra-ordinary about exchanging media and messages and this is not difficult software to create. This would also apply to organised crime, there is very little from stopping them from developing their own software to exchange messages. Attempting to police this act is effectively a limitation on the innovative engines of our economy that drives business, the creation of software.

So whilst it is clear the Bill is attempting to enable access to communications for law enforcement and intelligence agencies, there is questionable benefit if it is unenforceable or ineffective for its legislative purpose.

The premise for not introducing "backdoors" and vectors for attacking systems is very shallow. Instead it is clear from 317C and 317D that any and all computer infrastructure deployed in Australia will have to have governmental monitoring subsystems installed in them, possibly by multiple government agencies. None of these clauses will stop, capture or decode messages by anyone determined enough to send them.

Consequently, criminal actors will now have a well defined target that they know exists and only has to be found for it to be used, making their task of covertly capturing data on average Australian citizens much easier. Criminals certainly won't be concerned about breaking laws if they already are. For those reasons once the infrastructure this Bill implies is established and deployed it will put the honest person and businesses at a disadvantage when they comply because the governmental monitoring subsystems will be a known target within their infrastructure.

Cyber crime, identity theft and other fraud against Australians are more likely to succeed with the taxation dollars from ordinary Australians used to build the means to defraud them of assets and income. I am very concerned that passing this Bill will lead to increased fraud against the average everyday Australia who is trying to use the internet to do everyday tasks and save time. No one will be spared, the Honourable Members themselves still have to interact in our society and will be exposed at some level.

There are much better ways for achieving law enforcement's objectives than with obtuse and overt access clauses as the main issue with deploying any kind of technology is unexpected side effects. The obvious unexpected side-effect of the government's proposed initiative is how they will be used against those companies who co-operate. If deployed world wide, which I see is something our government is championing, I cannot help but seeing it lead the world to some sort of digital feudalism broken down into virtual fifedoms.

I urge the government and all honourable members not to hand organised crime a weapon against our citizenry as powerful as this one. The intention of these laws is clearly for gathering data, which is exactly the goal of cyber-criminals. Instead the government could

seek to protect its citizens by implementing technology laws that protect us from cyber-crime and fraud, in ways that lead to intelligence outcomes. Laws that use encryption technology to reduce opportunities for fraud against Australians as opposed to increasing them.

Thank you for taking the time to read this.

Regards
John Mifsud