From: Justin Clarke
To: Assistance Bill Consultation
Subject: Targeted Surveillance vs Mass Surveillance
Date: Monday, 10 September 2018 9:44:21 PM

Dear fellow citizen,

When it comes to state surveillance **targeted surveillance** with appropriate judicial oversight is reasonable, proportionate and in fact *unavoidable*.

World-leading security researchers regularly make statements which assert that when state actors want to target an individual it is essentially impossible to avoid this surveillance:

* the underlying mobile phone protocol Signalling System No. 7 can be exploited
* the mini-computer running on a SIM card can be exploited
* regularly discovered 0-day exploits (software vulnerabilities) can be exploited

These vectors all allow state actors to hack, monitor and capture target communications.

There is naturally a higher operational cost to undertake this surveillance, but ASIO and other entities *already* have this power.

Edward Snowden's revelations about NSA and GCHQ capabilities have confirmed this in detail.

Encrypted communication does not protect against any of the above vulnerabilities.

However what we have proposed here is *potentially* a new form of **mass surveillance**.

Any change in the power dynamic between citizens and governing institutions should very carefully consider all reasonable threats.

The consultation paper mentions terrorism as a threat, and any committee discussion should seriously consider the future risk of state terrorism in the form of future authoritarian abuse of technology systems that could be enabled by this proposed legislation.

History suggests that no matter how unlikely that scenario appears to be today, tomorrow offers no guarantees.

Any discussion which limits consideration of this threat to merely acknowledging the existence of some form of judicial oversight and vague tests of 'reasonableness' in the bill is not good enough.

We have a far more sophisticated understanding of how to analyse systems from a game theoretic perspective: modelling numerous scenarios to understand how bad actors, both inside and outside a system, can exploit weaknesses and cause unintended consequences.

Unless the committee is provided with an example technology system architecture that would be birthed under this bill, so that outside technical experts and security researchers can evaluate it and report on systemic weaknesses, then exactly no-one has a full and complete understanding of the consequences of this bill.

As Edward Snowden has observed: 'No system of mass surveillance has existed in any society, that we know of to this point, that has not been abused.'

Considering state actors can already undertake **targeted surveillance**, it is reasonable to assume that these proposed changes may in some way enable **mass surveillance**.

The focus on requesting or forcing communications and technology providers to build new software to satisfy this is suggestive of a hoped-for industry engineering effort to enable fast, scalable surveillance: the type of dragnet / firehose / indiscriminate data capture the NSA engaged in but argued was not illegal if it was only stored, and not accessed.

That ASIO's US equivalent took such a flexible attitude to existing US laws in undertaking mass surveillance is illustrative of the legal contortions that intelligence agencies can engage in in the quest to stockpile national data.

This illustrates another issue with any abuse of legislation to surveil populations at scale: the collected data is a honeypot for a wide array of actors, both criminal and state, national and foreign, who are not bound to any legislative protections once they seize the data.

To satisfy the public that the proposed legislation will not be used for **mass surveillance**, additional safeguards, modifications, restrictions and explicit directives should be considered.

But beyond that, **one public metric, updated regularly, is essential: the number of individual citizens who have been affected by actions under the bill.**

With this one simple metric, rigorously enforced, we can as a society have a good handle on the scale of surveillance occurring in our society to have a better sense about what type of society we are, and whether the powers under the bill are getting closer to being abused to enable mass surveillance.

Regards,
Justin Clarke.

From: Justin Clarke
To: Assistance Bill Consultation
Subject: Questionable examples
Date: Monday, 10 September 2018 10:17:14 PM

Dear fellow citizen,

The example used in the discussion paper to illustrate the need for additional powers illustrates the reverse:

A high risk Registered Sex Offender (RSO) was placed on the register for raping a 16 year old female, served nine years imprisonment and is now monitored by Corrections via two ankle bracelets whilst out on parole. Victoria Police received intel that he was breaching his RSO and parole conditions by contacting a number of females typically between 13 and 17 years of age. Enquiries showed that he was contacting these females and offering them drugs in return for sexual favours. The suspect was arrested and his mobile phone was seized but despite legislative requirements he refused to provide his passcode. Due to an inability to access his phone as well as the fact that he used encrypted communication methods such as Snapchat and Facebook Messenger, Victoria Police was unable to access evidence which would have enabled them to secure a successful prosecution and identify further victims and offences. These are high victim impact crimes that are being hindered by the inability of law enforcement to access encrypted communications.

The commercial services mentioned: Snapchat and Facebook, can be configured to encrypt communications, but the connected graph (users you are connected to) **is not encrypted** and available.

Considering a number of victims were identified, it would have been possible for police to determine the suspect's Snapchat and Facebook username(s) from their devices, if not already known, and through other technical means otherwise.

Based on this information it would be possible for law enforcement to request all users the suspect was connected to, allowing an investigation to contact other potential victims parental guardians to seek endpoint access and communication history.

A few questions:

Why were these existing methods of access either not pursued or not mentioned in the draft example?

How does the bill solve this particular case when applied? Assuming the bill does not weaken encryption, that only leaves the possibility the bill will enable automatic disabling of passcodes on any phone. How would this work without weakening national security at scale?

Regards,
Justin Clarke.