Table of Contents

Submission
Author: Paul Wilkins
Date: 12 Feb 2019

Distinction of Police from Security / Intelligence Powers

The Act, as passed, established an equivalence of the remit of police powers and those of the security/intelligence services. All party to this accepted that the Act as passed was an expedient, and that in passing the Act, poor framing of the powers granted, and in their requisite accountabilities, were a necessary risk that would be dealt with when sufficient time for due consideration allowed. Obviously time now affords sober consideration of the clear overreach of powers granted under the Act, and so the time has come to reign in the scope of the sweeping and arbitrary police powers granted under the Act. One of the accepted risks at the time of the Act's passing was that the powers granted under the Act could go beyond requirements of necessity and proportionality, and indeed, the greater parts of industry and the wider public expressed views that this was the case. Such is the case where it comes to granting police Exceptional Access powers, which is entirely unnecessary.

When considering the proportionality of powers granted under the Act, it's a clear error to equate the missions and responsibilities of the police forces, with those of the security/intelligence services. A more deliberate drafting of the Act would have treated with police powers and security/intelligence powers differently. The rushed drafting of the Bill conflated the need for Exceptional Access for the security/intelligence services, with those of the police services, which require only Legal Intercept powers.

When granting Exceptional Access, one needs to consider the reach of the powers granted, and the purposes they will be put to. Exceptional Access, as embodied within the Act, grants the power to read, write, modify, delete data as required. This is an exceptionally broad remit, and reflects the need for security/intelligence agencies to conduct intelligence missions, up to and including engaging in cyber warfare with the foreign security services and their agents. So for intelligence agencies to have EA powers is both necessary and proportional to their mission and responsibilities.

However, police forces have neither the need nor the remit to conduct intelligence missions. Police powers granted under the Act should, indeed must be, limited to necessary and proportional police powers, for the purposes of law enforcement - to recognise crime, identify the perpetrators, and bring them to justice, along with such evidence of wrong doing as they have collected. Nothing in this brief requires any requirement to write, modify, or delete data, conduct espionnage, or conduct cyber warfare. The powers granted under the Act to police should extend only to Legal Intercept, that is, police powers under the Act should be limited to read data. No write/modify/delete powers should be granted to the police under the Act.

Once there is allowance for differentiation in Police vs Intelligence Services powers, there should similarly be differentiation for the threshhold of the seriousness of crimes to exercise powers.

The current threshold of 3 years embodied in the Act is in the right region for the exercise of Legal Intercept. For one thing, cyber stalking attaches a penalty of 3 years.

Police powers should be limited to Legal Intercept only. The security/intelligence services, should be granted both EA and Legal Intercept powers, but given the more intrusive nature of EA vs Legal Intercept, there should be a higher bar for the Intelligence Services to exercise the EA powers (something in the region of 10 to 20 years).

Pending Labor Amendments

The Labor amendments pending in the Senate are welcome and critical for:

Requirements for judicial review of TCNs/TARs, and avenue of judicial appeal for service providers
Strengthened requirements for necessity and proportionality
Definitions of system vulnerability and systemic weakness (which preclude mass deployment of patched code)

These amendments are necessary and reasonable. However the following concerns remain still to be resolved:

Separation of TCN and TAN

It's still not clear that anything doable under a TCN, cannot be compelled under a TAN's write/modify data powers. Hence, there ought to be specific exclusion of a TAN's powers from compelling the implementation of a capability for which a TCN can be issued.

Mass Surveillance via Metadata

Nowhere are TCN/TAN/TARs disallowed from serving as "authorisation" under s280 / s313 of the Telecommunications Act 1997, sufficient to demand mass access to carrier metadata/ metadata datastreams. There is also lawful disclosure of mass metadata under s177 of the Telecomms Interception and Access Act 1979. If the police and/or intelligence services get access to metadata

streams, they will integrate this with their other metadata projects, including CCTV and facial recognition databases. Which is obviously something some in Law Enforcement are advocating for, though I think most citizens would regard this as an alarming move towards mass surveillance and a police state.

Single Agency to Act as Warrant/Notice Clearing House

Having one agency act as a clearing house for notices and warrant data, is still a preferable framework to access by multiple agencies, and would provide advantages for economy, efficiency, governance, and the secure custody of both warrant data and service provider confidential information.

Provision for Journalists and Public Interest to have Standing to Oppose TCN/TAN/TARs

Journalists and media organisations ought to be able to mount a public interest defense against the issue of TANs.

Any citizen ought to have standing to mount a public interest defense against the issue of a TCN.

Audit Trail

An audit trail should be required for all TAN/TAR actions. Any TCN which specifies TAN capabilities should include a requirement that the use of the capability generate an audit trail.

Free/Open Source Software

The Act permits the insertion of arbitrary code at many points in the supply chain for free / open source software. Where a project is the collaboration of multiple authors, any of them may be targeted by a TAN requiring source code modifications or the insertion of arbitrary source code. Where those projects are then bundled into software distributions, those distributors may be targeted by TANs requiring either source modifications, or the insertion of arbitrary unauditable binary “blobs”. Downstream redistributors of free/open source software distributions may similarly be targeted.

One would expect the intelligence services would generally want to foster collaborative relationships with software develops. The Act will have very much the reverse effect. If/when free software developers are directed to modify code under a TAN, the response from the open source community is going to be predominantly hostile. Many FOSS advocates dislike “big state” and many are privacy evangelists. But looking beyond those working in FOSS whose idealogy leaves them with entrenched prejudice against the state intruding to any degree into data privacy, there are still deep concerns in reasonable thinking people that the powers of the Act are intrusive to a degree that represent less the necessary police powers of a Liberal Democracy, and more those of Big Brother Police State. More than likely, FOSS authors subject to the Australian jurisdiction, will either relocate, or discontinue their projects, rather than comply.