Dr James Renwick,
Independent National Security Legislation Monitor

2020-03-05

Dr Renwick,

Thank you for the opportunity to speak with you on Thursday regarding TOLA. I'm very happy to see this legislation being reviewed with such dedication and rigour.

In particular, I am encouraged by your emphasis on finding a way to include impartial review in the process and by the inclusion of technical advisors in the process. It is critical that a truly neutral arbiter review any orders and that the necessary expertise is available to those involved.

Based on my reflections on the hearing and the discussions that emerged from it, I wanted to share some further thoughts. In addition to the formal submission that Mozilla has already made to your office, I hope you will take these recommendations into consideration as you prepare your report.

- **Secrecy should not be the only choice.** I know that you were not particularly receptive to the notion that TCNs be made public in all circumstances. If you are unwilling to consider a recommendation to abolish TCNs (as would be ideal), you might consider a recommendation that agencies request and justify secrecy when requesting a TCN. The independent review process can then decide whether secrecy is necessary.

  Secrecy around TCNs carries risks. As I mentioned in evidence, wide public review of security-critical mechanisms is an important part of the process of validating the designs that keep us safer online. Secrecy deprives DCPs access to and participation in these public conversations. Furthermore, complex interdependencies in systems might mean that a flaw in one component could affect large parts of the system, often in ways that are impossible to know ahead of time. Secrecy makes it even more difficult to secure technology and comes with greater risk.

  Secrecy also reduces the degree to which the agencies are accountable to the public. Enabling public debate about agency powers is the best means of ensuring accountability.

For a TCN, a request for secrecy should be justified to the independent decision maker and the risk of compromise and the diminution of public awareness of agency powers be considered. TCNs need not be tied to a specific target, operation, or investigation, so the need for restrictions on disclosure that might exist for a TAN or TAR do not apply in the same way.

Limitations on secrecy for TCNs might go a long way to alleviating concerns raised by industry and civil society about the risks of creating accidental flaws in systems.

These concerns about justifying secrecy also apply to use of a TAN. However, as a TAN is more likely to be related to an ongoing operation, it seems likely that secrecy would be easier to justify, at least in the short term.

Affected parties should be notified, either immediately or once the conditions justifying secrecy for a TAR, TAN, or TCN end. This would greatly improve accountability.

- **Abolish TARs in favour of TANs.** I was convinced by the arguments by Lucie Krahulcova from Access Now about the lack of protections for the interests of individuals in this process. While TARs are voluntary, we should expect that they may frequently be used given the friendly relationships that exist between many DCPs and the government. However, this voluntary cooperation offers few protections for the interests of affected users and businesses.

  TARs lack any opportunity for independent review and should be removed.

- **Require destruction of coincidental information that might be gathered.** As was discussed during the hearing, there are cases where information gathered under the auspices of one of these provisions might be unrelated to the investigation. This information should be destroyed once it is clear that it is not material to the investigation. We heard that police routinely retain all information they gather, no matter its apparent import, often with the expectation that it might be useful in other investigations. While we can't insist on agents forgetting what they learn, we can insist that this information be deleted if its collection was not directly authorized by the independent body.

  To give an example, an ICAC could acquire the private communications of a member of parliament in an investigation. This investigation might turn up details of unrelated activities of them and their friends, colleagues, and family, including minors. While the ICAC should obviously be able to retain whatever records are needed for the investigation and prosecution of the MP, retaining information unrelated to that case would violate the rights of those affected to privacy and due process.

Requiring that material unrelated to the investigation be removed might help ensure that the collected information be - in the terms of the law - the least intrusive.

- **Expressly prohibit retention and use of any credentials that are revealed.** In the course of an investigation, agencies may incidentally collect credentials which enable access to other systems that are not in scope of the investigation. The government should be required to delete any credentials.

  Access to a personal device might result in revealing passwords or credentials for multiple other systems and devices. To give a concrete example, a search of my personal device might reveal the keys that I use to authorize the changes I make to Firefox.

  To use an offline analogue, if the police get a warrant to search my house, and in the process of doing so they find keys to my office, they should not be able to copy those keys just in case they want access to my office to investigate a Mozilla employee in the future.

  Credentials might be used to access devices that do more than process information. One trend we did not discuss at length is the way in which controls for physical systems are increasingly online. I seem to recall you touched on this with a comment about “going kinetic”. Some devices can be very simple to the extent that they lack access control systems that can discriminate between providing information and enabling control. For example, access to information about the location and speed of a car might use the same credentials as the controls for steering, acceleration, and braking.

  There should be explicit prohibitions on use of any credentials that might be obtained as part of an investigation. In particular, use of a credential to cause a physical effect should be specifically proscribed.

One final thought is the importance of capturing limitations to agency powers in the statute itself.

What I heard in the testimony of Mr. Mike Burgess, as Director-General of ASIO, was in effect “trust me” when it came to the potential for the introduction of systemic weakness or vulnerability. It is good to hear that the Director-General does not want to weaken security. Nevertheless, expressions of sentiment are not a sufficient basis for a system of law.

Though it is unnecessary, I remind you that the primary purpose in constructing a system of accountability and limitations on power is to reduce the degree to which we are required to confer trust in individuals. Indeed, this is exactly the principle that I described being used to protect our password manager, that motivates the deployment of end-to-end encryption, and that underpins many of the systems that provide online security.

The system that TOLA enables must have multiple defenses against accidental or malicious subversion. I have no reason to assume malice on the part of any of those involved in this process (quite the contrary in fact), but that does not diminish the significance of proper controls and oversight. This system depends on the formulation of strong legislation. That would make it possible for the Australian people to place their trust in the system itself.

Again, thank you for your work and I hope that these suggestions will be taken in the spirit in which they are offered. That is, with the intent to find the best outcome for the Australian people.

Respectfully,

Martin Thomson
Distinguished Engineer, Mozilla Corporation