NATIONAL SECURITY OR PRIVACY?

BY MICHAEL TROVATO, MANAGING DIRECTOR AND LEAD SECURITY ADVISOR, INFORMATION INTEGRITY SOLUTIONS AND AISA BOARD MEMBER; CHONG SHAO, SENIOR CONSULTANT, INFORMATION INTEGRITY SOLUTIONS; AND SARAH BAKAR, ASSISTANT CONSULTANT, INFORMATION INTEGRITY SOLUTIONS

The 4A framework: stronger protections for stronger powers.

A perennial conflict in the technology and policy space is the apparent trade-off between privacy and security. The issue has resurfaced in Australia in the law enforcement and national security space. My views are coloured by the impacts of 9/11. I was in New York that day – my country, city and industry were attacked by a truly malevolent extremist organisation, and I believe threats like those must be a priority. Can we do that and still preserve the freedoms we all need?

During a recent parliamentary inquiry into the controversial *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (the TOLA Act) – which allows security agencies to compel tech companies to decrypt information – the Australian Security and Intelligence Organisation (ASIO) Director-General Mike Burgess revealed that ASIO has only issued voluntary requests for assistance, and it has not had to use the compulsory powers under the Act.[1] Burgess stated that the agency's preference is to work with industry partners, although it has 'come close' to issuing a compulsory notice, and that the treatment environment 'remains complex, challenging and changing'.

Australian Signals Directorate (ASD) Director-General Rachel Noble shares this sentiment. In her recent speech to the National Security College, she defended the need for secrecy in ASD's operations because authorities are in a 'near impossible game' to keep Australia safe and 'the threat to our way of life is more real today than at any time I have known in my career'.[2] This speech was made not long after Minister for Home Affairs Peter Dutton confirmed that that the powers of the ASD will be expanded to enable the targeting of serious criminal activity within Australia as part of the government's new cyber security strategy.[3]

In light of proposals to give agencies more intrusive powers in the name of preserving national security while claiming the mantle of operational secrecy, it is even more important that this is matched with countervailing safeguards.

Fortunately, we have a well-established approach – which is known in the Office of the Australian Information Commissioner as the 4A framework[4] – that has resolved such difficult issues in the past. Here's how we can do it again today.

1. *https://www.smh.com.au/politics/federal/encryption-powers-not-used-by-asio-afp-as-tech-companies-volunteer-help-20200807-p55jhl.html*
2. *https://www.asd.gov.au/publication/speech-transparently-secret-asd*
3. *https://www.theguardian.com/australia-news/2020/aug/06/peter-dutton-confirms-australia-could-spy-on-its-own-citizens-under-cybersecurity-plan*
4. *https://www.ag.gov.au/sites/default/files/2020-05/Office%20of%20the%20Australian%20Information%20Commissioner%20Annexure%20A.PDF*

4A FRAMEWORK

Analysis

The first thing we need to get right is analysis. This involves a series of steps:

1. Define the problem, taking care to be calm, objective and frame it in the right way.
2. Be clear about the values that you would like to preserve and uphold – for example, respect for individuals, due process, et cetera.
3. Choose the most suitable option with the least privacy impact on balance – for example, confirming 18 years of age and older (rather than collecting everything on the ID card), introducing a sunset clause to enabling legislation, establishing a reasonable cause requirement, et cetera.
4. Ensure that you are conducting the analysis while keeping in mind the other As, as well.

Analysis should be an iterative process. For law enforcement and national security powers that have the potential to significantly intrude on privacy, analysis should encompass public consultations and parliamentary scrutiny.

The Parliamentary Joint Committee on Intelligence and Security (PJCIS) played an important role in halting the government's proposal to expand the use of facial recognition by law enforcement agencies. In its review of the Identity-matching Services Bill 2019, the PJCIS unanimously found that there was insufficient privacy and transparency safeguards in the Bill, and took the uncommon step of requesting that it be redrafted.[5]

Authority

Next, we need the right authority for law enforcement and national security agencies to do their job properly. As with everything, there needs to be a careful balance. Where privacy is likely to be affected, the power should be granted expressly by legislation setting out in objective terms what kinds of information can be collected, for how long, and in what circumstances.

The enactment of the TOLA Act is a welcome step in ensuring that agencies have the authority to gain access to encrypted information. A subsequent review of the legislation by the Independent National Security Legislation Monitor (INSLM) recommended that the two most intrusive powers be authorised by an independent body (a separate arm of the Administrative Appeals Tribunal headed by a retired judge); however, Burgess considered that the existing approval process was adequate.[6] This is a fine point of judgment that is very controversial given the new powers that the agencies are seeking.

5. *https://www.itnews.com.au/news/govt-told-to-rewrite-facial-recognition-bills-532885*
6. *https://www.smh.com.au/politics/federal/encryption-powers-not-used-by-asio-afp-as-tech-companies-volunteer-help-20200807-p55jhl.html*

Accountability

The third thing we need to get right is accountability: making sure that power is, and is seen to be, exercised in the right way. This is especially important in the law enforcement and national security space – their considerable powers are frequently exercised in a corrosive environment, in difficult situations, and against vile people. As Noble put it, 'Not all Australians are the good guys'.[7] In such a context, misuse and abuse of authority can and does happen – no-one is infallible.

We already have laws and institutions that provide for accountability mechanisms, such as access to information, prohibition on classifying or withholding information about violations of law, whistleblower protection, and monitoring and review of power-wielding agencies.

The real challenge is to ensure that in practice, our accountability bodies are able to function effectively now and in the future. This requires that:

1. they have the necessary scope to operate, enshrined in legislation. No agency or activity should escape scrutiny, and there should be strong powers of evidence gathering
2. they are allowed to operate without undue political or outside influence
3. we must provide them with sufficient resources in order for them to do their job effectively. Having all the legal mandate in the world is useless without the money and personnel to carry it out.

In the national security space, the Inspector-General of Intelligence and Security (IGIS) is the independent statutory office holder charged with reviewing the activities of the major Commonwealth intelligence agencies, including ASIO and the ASD. Despite the IGIS's clear remit, however, there appears to be ongoing challenges with its ability to carry out its extensive responsibilities.

One major issue is that of resourcing. Outgoing Inspector-General Margaret Stone recently told the PJCIS that her office required five additional personnel to meet the workload that has arisen out of the TOLA Act.[8] Furthermore, she agreed with one senator's summary that the office cannot sustain the demand of its current legislative oversight roles.

A consequence is that the extent to which the IGIS can effectively exercise oversight over the relevant agencies is being questioned. The IGIS recently investigated complaints by a former intelligence officer (Witness J) against his former employer and cleared the agency of wrongdoing. Witness J rejected this finding and claimed that '[IGIS] was not taken seriously when I was in the agency...'.[9]

The IGIS plays a crucial role in holding national security agencies accountable. There are proposals to expand its oversight even further to cover four additional agencies, including the Australian Federal Police and the Department of Home Affairs; however, the accountability of these agencies will be significantly weakened unless lawmakers do more to secure the power and resources for the IGIS to do its job.

Appraisal

Finally, as we have seen, technology changes, the threat landscape changes, and powers become stronger. Hence, the last of the 4As: appraisal. We need to monitor the new measures and evaluate whether they are working as expected. We need to ask whether the circumstances have changed, which circles back to an analysis of what needs to be done about it.

A good example of appraisal taking place is the recent inquiry by the PJCIS into the TOLA Act. Companies and civil society groups have voiced a number of concerns, and it has been reported that none are likely to be in favour of the anti-encryption laws.[10] The PJCIS's report – which will be informed by the INSLM report – will likely make recommendations that rebalance privacy and security considerations, and address the issues that have arisen in the TOLA Act's first two years of operation.

Give me privacy, or give me security? Let's all move beyond this false dichotomy and have a conversation based on facts, sound judgment and an appreciation of our past successes. •

7. *https://www.asd.gov.au/publication/speech-transparently-secret-asd*
8. *https://www.zdnet.com/article/igis-still-calling-for-more-staff-to-provide-oversight-of-asios-encryption-busting-powers/*
9. *https://www.abc.net.au/news/2020-09-01/witness-j-mental-health-neglect-spy-watchdog-inspector-general/12611580*
10. *https://www.innovationaus.com/encryption-inquiry-is-out-of-hibernation/*