THE DELICATE BALANCE BETWEEN NATIONAL SECURITY AND PRIVACY

The 4A Framework: Stronger Protections for Stronger Powers

By Simon Liu and Mike Trovato

January 2024

The Delicate Balance Between National Security and Privacy

A Delicate Balance, Rather Than a Trade-Off

There is a greater need to revisit the interplay between privacy and security, in an era of 'polycrisis' where multiple conflicts occur at the same time. Resolving the perennial tension between maintaining national security while preserving privacy is an ongoing challenge.

Our views are coloured by the impacts of the September 11 attacks in New York City and the 2014 Lindt Café siege in Sydney, as we both witnessed, that forever shaped our understanding of extremism and how a single event like this can be so destructive to a city, country, industry, and people. National security threats are of upmost concern, but can we still preserve the freedoms of privacy that we all need? This is not a trade-off between the two, but rather, a delicate balance.

In 2020, there was a parliamentary inquiry into the controversial *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* ('the TOLA Act') which allowed law enforcement, security, and intelligence agencies to compel communication and technology companies to intercept and monitor encrypted communications. In practice, at least until August 2020, 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 also 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 threat environment "remains complex, challenging, and changing".

Australian Signals Directorate (ASD) Director-General Rachel Noble shares this sentiment. In the same year, in a 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].

As part of the 2023-2030 Australian Cyber Security Strategy, the government will continue to deliver ASD's Project REDSPICE that will triple Australia's offensive cyber capabilities [3]. Even though the details of the project remain classified, ASD has asserted that they remain committed to transparency about their rights and obligations under the respective powers. However, there has been no further public demonstration or documentation of this commitment.

In light of proposals to give agencies more intrusive powers in the name of national security whilst claiming the protection 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 (OAIC) as the 4A framework [4] – that has resolved such issues in the past. Here's how we can do it again today.

The 4A Framework

Analysis

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

- Define the problem – taking care to be calm, objective, and framing it in the right way.
- Be clear about the values that you would like to preserve and uphold – for example, respect for individuals, due process, etc.
- Choose the most suitable option with the least privacy impact on balance – for example, confirming 18+ proof of age (rather than collecting every information on an ID card), introducing a sunset clause to enabling legislation, establishing a reasonable cause requirement, etc.
- Ensure that you are conducting the analysis while keeping in mind the other A's 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 proposal to expand the use of facial recognition by law enforcement agencies. In its review of the Identity-matching Services Bill 2019, the Committee 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].

Following changes, the Parliament introduced the Identity Verification Services Bill 2023 for consideration in 2023, highlighting the PJCIS report and what was mentioned in that review. The Bill was passed by both Houses and gained Royal Ascent in December 2023.

Authority

Next, we need the right authority for law enforcement and national security agencies to do their job properly. There needs to be a careful and delicate 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 and oversight arrangements was adequate [6]. This is a fine point of judgment that is very controversial given the new powers that the agencies are seeking.

The Delicate Balance Between National Security and Privacy

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 as their powers are frequently exercised in difficult decisions that often have irreversible impact. As Noble explains 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, whistle-blower 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:

- First, 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.
- Second, they are allowed to operate without undue political or outside influence.
- Third, we must provide them with sufficient resources in order to do their job effectively. Having all the legal mandate in the world is futile 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 ASD. However, despite IGIS's clear remit, there appears to be ongoing challenges with the ability to carry out its extensive responsibilities.

One major issue is that of resourcing. The outgoing Inspector-General Margaret Stone at the time 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.

One consequence is that the extent to which the IGIS can effectively exercise oversight over the relevant agencies has been 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 "[t]he [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 which means the threat landscape changes. New tools and powers wielded by law enforcement and national security agencies inevitably have both intended and unintended effects.

Hence the last of the 4A's: 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 since the enactment of the TOLA Act in 2018, which circles back to an analysis of what needs to be done about it.

An example of appraisal is the 2020 inquiry that the PJCIS conducted into the TOLA Act. Companies and civil society groups voiced a number of concerns and it was reported that none were likely to be in favour of the anti-encryption laws [10]. However, the report that was due to be released in September 2020 was only issued in December 2021, and the list of recommendations failed to take into oversight of the anti-encryption concerns of the Australian people.

It seems unlikely that the Australian government has given priority to appraisal of national security laws, powers, and practices that impact privacy. This is understandable – hardly anyone does appraisal well, be they organisations or individuals. However, appropriate appraisal is more important in today's context than ever.

A False Dichotomy

"Give me privacy, or give me security?"

It is not a trade-off; a careful and delicate balance between the two is required. Let's all move beyond this false dichotomy and have a conversation based on facts, sound judgment, and an appreciation of our past successes.

Bibliography

[1] Sydney Morning Herald, 'Encryption Powers Not Used by ASIO, Police as Tech Companies Volunteer Help' (7 August 2020), <https://www.smh.com.au/politics/federal/encryption-powers-not-used-by-asio-afp-as-tech-companies-volunteer-help-20200807-p55jhl.html>.

[2] Australian Signals Directorate, 'Director-General ASD Speech to the National Security College' (1 September 2020), <https://web.archive.org/web/20201105175859/https://www.asd.gov.au/publication/speech-transparently-secret-asd>.

[3] Department of Home Affairs, '2023-2030 Australian Cyber Security Strategy' (22 November 2023), <https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf>.

[4] Office of the Australian Information Commissioner, '4A Framework – A Tool for Assessing and Implementing New Law Enforcement and National Security Powers' (July 2011), <https://www.ag.gov.au/sites/default/files/2020-05/Office%20of%20the%20Australian%20Information%20Commissioner%20Annexure%20A.PDF>.

[5] iTnews, 'Govt Told to Rewrite Facial Recognition Bills' (24 October 2019), <https://www.itnews.com.au/news/govt-told-to-rewrite-facial-recognition-bills-532885>.

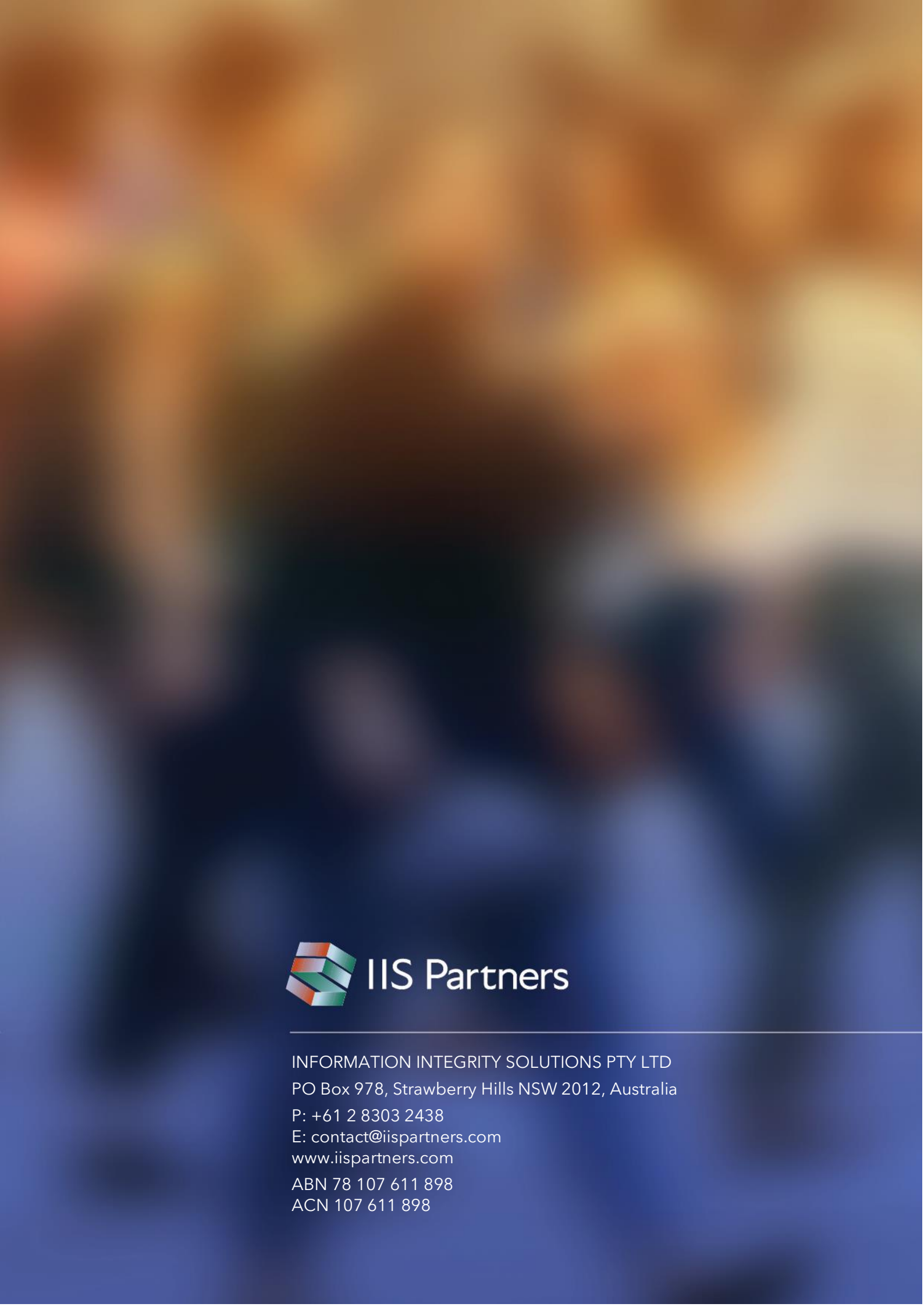
[6] Sydney Morning Herald, 'Encryption Powers Not Used by ASIO, Police as Tech Companies Volunteer Help' (7 August 2020), <https://www.smh.com.au/politics/federal/encryption-powers-not-used-by-asio-afp-as-tech-companies-volunteer-help-20200807-p55jhl.html>.

[7] Australian Signals Directorate, 'Director-General ASD Speech to the National Security College' (1 September 2020), <https://web.archive.org/web/20201105175859/https://www.asd.gov.au/publication/speech-transparently-secret-asd>.

[8] ZDNET, 'IGIS Still Calling for More Staff to Provide Oversight of ASIO's Encryption-Busting Powers' (9 August 2020), <https://www.zdnet.com/article/igis-still-calling-for-more-staff-to-provide-oversight-of-asios-encryption-busting-powers/>.

[9] ABC News, 'Spy Watchdog Dismisses Secret Prisoner Witness J's Claims of Mental Health Neglect' (1 September 2020), <https://www.abc.net.au/news/2020-09-01/witness-j-mental-health-neglect-spy-watchdog-inspector-general/12611580>.

[10] InnovationAus, 'Encryption Inquiry is Out of Hibernation' (22 July 2020), <https://www.innovationaus.com/encryption-inquiry-is-out-of-hibernation/>.



IIS Partners

INFORMATION INTEGRITY SOLUTIONS PTY LTD
PO Box 978, Strawberry Hills NSW 2012, Australia
P: +61 2 8303 2438
E: contact@iispartners.com
www.iispartners.com
ABN 78 107 611 898
ACN 107 611 898