INTERNATIONAL ENCRYPTION BRIEF

MARCH 2021

The Encryption Debate in Australia: 2021 Update

Stilgherrian

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

About the Encryption Working Group

The Carnegie Endowment for International Peace and Princeton University have convened a small group of experts to advance a more constructive dialogue on encryption policy. The working group consists of former government officials, business representatives, privacy and civil rights advocates, law enforcement experts, and computer scientists. Observers from U.S. federal government agencies attended a select number of working group sessions. Since 2018, the working group has met to discuss a number of important issues related to encryption policy, including how the relevant technologies and uses of encryption will evolve in the future.

This brief and its companion pieces detailing the encryption debates in a select number of key countries and regions—Australia, Brazil, China, the European Union, Germany, and India—were prepared by local and area experts at the request of the Encryption Working Group. They are designed to shine light on key drivers of the debates in these countries, how they have evolved in the last five years, and the divergent approaches taken by different governments. The briefs do not take a position on encryption policy, rather they provide analysis of how debates about encryption have evolved internationally. The views are the authors' own and do not necessarily reflect the views of Carnegie or the Encryption Working Group.

In 2018, the heads of Australia's law enforcement and intelligence agencies were given broad powers by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018,[1] or TOLA Act, to gain access to encrypted communications.

The aim, as then attorney general, Senator George Brandis, had said the year before, was to create a law "sufficiently strong to require companies, if need be, to assist in response to a warrant to assist law enforcement or intelligence to decrypt a communication."[2] The government cited end-to-end encrypted messages as the specific problem, and continues to do so.

The TOLA Act powers have now been in operation for more than two years. Government oversight agencies, the opposition Labor Party, the Australian Greens, and civil society organizations have all recommended significant changes—none of which have yet been made.

Australia's Encryption Laws as They Stand

The most controversial section of the TOLA Act amended the Telecommunications Act 1997 to create "frameworks for voluntary and mandatory [communications] industry assistance to law enforcement and intelligence agencies."

Three kinds of notices or requests sit at the core the TOLA Act framework:

- **Technical Assistance Requests** (TARs), which are "voluntary" requests for a "designated communication provider" to use a decryption or other data access capability they already have;

- **Technical Assistance Notices** (TANs), which are compulsory notices for a designated communication provider to use a capability they already have; and

- **Technical Capability Notices** (TCNs), which are compulsory notices for a designated communication provider to build a new capability, so that it can fulfil subsequent Technical Assistance Notices and Requests.

The net can in fact be cast very wide indeed. The definition of "designated communication provider" runs for three pages, and includes everyone from the major telecommunications carriers down to an entity that "provides an electronic service that has one or more end-users in Australia," anyone who "develops, supplies or updates software used, for use, or likely to be used, in connection with" such a service, and "manufactures or supplies components for use, or likely to be used, in the manufacture of customer equipment for use, or likely to be used, in Australia."[3]

An agency using this framework might have started with a communications interception or computer access warrant obtained in the usual way from an eligible judge or nominated member of the Administrative Appeals Tribunal (AAT), but cannot access the content of the communication because of encryption or other difficulties. It can then issue a designated communication provider with either a TAR, which the provider could in theory refuse, or a TAN.

The provider might be the telecommunications company through which the intercept was conducted. More likely, however, it's the responsible legal entity for the over-the-top communications provider such as Facebook in the case of Messenger, Apple in the case of iMessage, WhatsApp LLC in the case of WhatsApp, and so on.

In another scenario, the agency might have seized a physical device after executing a search warrant, or otherwise legitimately have it in custody. A TAR or TAN could then be issued to gain access to stored communications, either to the hardware manufacturer such as Apple or Google or Samsung, or the software vendor providing the encryption.

No further warrant or other judicial approval is required. The chief officer of the agency in question must simply satisfy themselves that the assistance would be "reasonable and proportionate," that compliance would be "practicable" and "technically feasible," and a range of other considerations.

Any independent oversight happens after the fact, conducted for intelligence agencies by the Inspector-General of Intelligence and Security (IGIS), and for law enforcement by the commonwealth ombudsman and their state and territory equivalents.

If the communications provider cannot comply with a TAR or TAN because it isn't technically feasible or is otherwise unreasonable, a TCN can be issued by the attorney general with the joint approval of the communications minister.

Every aspect of this process happens in secret. Only totals and some statistical information is reported publicly.

In practice, at least up to August 2020, neither the Australian Security and Intelligence Organisation (ASIO) nor any of the law enforcement agencies have used the compulsory notices. Communications providers have acted on the basis of the voluntary requests.[4] One imagines that if they'd declined to cooperate voluntarily then a compulsory notice would soon follow.

According to evidence given before the Parliamentary Joint Committee on Intelligence and Security (PJCIS) at that time, ASIO has issued "fewer than 20" TARs, the Australian Federal Police eight, and the New South Wales Police Force some thirteen.[5]

According to ASIO Director-General Mike Burgess, "There have been points in time where ASIO has come close to issuing a compulsory notice, however our preference will always be to engage as much as possible with industry partners who have also been committed to helping keep Australians safe."

At the time of writing, there has been no reported use of a TCN.

Further subtleties of the TOLA Act powers, and the political processes which led to the Act, are detailed in a previous brief, "The Encryption Debate in Australia."[6]

While similar in intent to the UK's Investigatory Powers Act 2016, Australia's laws go beyond the UK's in two significant ways: explicitly granting the power to require a broad range of communications and service providers to develop new interception capabilities, and attempting to require foreign companies to comply.

Reviews and Proposals for Changing the Encryption Laws

Contrary to almost all expectations, the Liberal-National Coalition government was returned to power in the May 2019 federal election. Since then, the TOLA Act powers have remained untouched, largely because they were scheduled to be reviewed by the PJCIS after operating for eighteen months.

While the encryption debate was a political football before the election, it had until quite recently faded into the background. More immediate political issues have demanded attention, including the government's response to the devastating bushfires of 2019–2020 and the continuing coronavirus pandemic.

Broadly speaking, while the Labor Party has supported the general intent of the Liberal-National Coalition government's proposals, they've questioned their breadth and lack of transparency. The Greens have positioned their objections in their wider argument against government surveillance in general.

Labor has proposed a number of amendments that would address some of the party's more serious concerns. Senator Kristina Keneally, the shadow minister for home affairs and shadow minister for immigration and citizenship, introduced the Telecommunications Amendment (Repairing Assistance and Access) Bill 2019 on December 4, 2019.[7] The proposed legislation retains the TAR/TAN/TCN framework, but all three would now have to be approved by a judge.

The current law prohibits the creation of a "systemic weakness" or "systemic vulnerability" in encryption and other systems of "electronic protection," terms that have proved difficult to define.[8] Under Labor's amendments, providers could not be required to "implement or build a new decryption capability," perform "one or more actions that would render systemic methods of authentication or encryption less effective," or "any act or thing that would or may create a material risk that otherwise secure information would or may in the future be accessed, used, manipulated, disclosed, or otherwise compromised by an unauthorised third party."

The bill would also limit the "acts or things" that agencies can ask for to those specifically listed in legislation, but there would be no change to the range of communications providers or criminal offenses targeted.

That bill is currently on hold in the Senate.

Meanwhile, the PJCIS called for submissions and held public hearings in the usual manner, but also asked for a review by the Independent National Security Legislation Monitor (INSLM) to consider "whether the Act contains sufficient safeguards for protecting the rights of individuals and remains proportionate and necessary."[9]

The INSLM report, published in June 2020, was titled "Trust But Verify."[10] "I consider that there is a greater need for safeguards in the virtual world than in the physical world, for both reasons of trust and the wide and unknown impact of technology," wrote James Renwick. He called for the power to issue TANs and TCNs to be removed from agency heads and the attorney general respectively and given not to judges but to the AAT "in a way which will preserve and protect both classified and commercial-in-confidence material and allow independent rulings on technical questions."

The AAT's role is to conduct independent merit-based reviews of "administrative decisions made under Commonwealth laws."[11] Some of its members already hold the power to issue telecommunications interception warrants in a personal capacity as a *persona designata* under section 6DA of

the Telecommunications (Interception and Access) Act 1979, the TIA Act.[12] Concerns have been expressed, however, that many AAT members are political appointees, and that the AAT in general might be more willing to issue a warrant than a judge.[13]

Renwick also proposed a new statutory office, the Investigatory Powers Commissioner (IPC). "The IPC should be a retired judge who will be appointed to the AAT and have access to technical advice. The IPC will assist in approving the issue of TANs and TCNs," Renwick wrote. The IPC would also monitor the operation of the regime and issue guidelines.

> "The IPC should be 'dual hatted'—the IPC should be appointed as a part-time Deputy President within the AAT and designated as the head of a new Investigatory Powers Division (IPD) of the AAT, with powers and procedures based upon the existing Security Division. One of the first tasks of the IPC, following wide consultations with interested persons, would be to recommend in detail how that system should work."

Among Renwick's thirty-three recommendations, the INSLM also recommended giving state and territory anti-corruption commissions TOLA Act powers; tightening the range of applicable crimes to "serious Australian offence" and "serious foreign offence'" to align with section 5DA of the TIA Act; amending definitions in a similar way to Labor's bill; and a range of improvements to the reporting and oversight arrangements.

The PJCIS inquiry was due to report by September 30, 2020, but at the end of March 2021 it still has yet to do so.

In a separate development, in December 2020 the government finally released the report "Comprehensive Review of the Legal Framework of the National Intelligence Community," although it had in fact been completed in December 2019.[14]

According to the reviewer, Dennis Richardson, a former diplomat, public servant, and one-time ASIO director general, Australia needs a whole new Electronic Surveillance Act (ESA). The legislative framework that governs Australia's intelligence community is "unnecessarily complex," he wrote. It leads to "unclear and confusing laws" for the intelligence officers who have to interpret and follow them.

"Technological change and convergence has resulted in telecommunications interception, covert access to stored communications and computers, and the use of optical and listening devices . . .

becoming functionally equivalent," he wrote, but at the moment these activities are subject to "inconsistent limits, controls and safeguards" across the TIA Act, the Surveillance Devices Act 2004, and the Australian Security Intelligence Organisation Act 1979.

Richardson sees developing a new ESA as a five-year project, warning: "It would also be possible for government to continue making *ad hoc* amendments to address individual challenges, as they arise. But kicking the can down the road will only make the reform exercise that much bigger and more complex when the time comes, as it surely will."

More broadly, Richardson also recommended not strengthening judicial oversight of intelligence activities, but weakening it. "Ministers should continue to authorise ASIO and Intelligence Services Act agency activities. These authorisations should not also be subject to judicial or other independent authorisation," he wrote.

In its formal response, the government agreed with almost everything Richardson had to say—including the reduction in oversight.[15] Ministerial authorizations and subsequent oversight by the IGIS would be sufficient.

The Law Council of Australia has expressed "grave concern," saying this would "reinforce Australia's status as a major outlier within the Five Eyes Alliance." All of the Five Eyes nations—the United States, the UK, Canada, Australia, and New Zealand—currently require judicial authorization for their "intrusive intelligence collection-powers."[16]

In this context it's worth noting ASIO chief Burgess's response to the INSLM proposal for judicial approval of TARs and TANs in his PJCIS evidence previously cited. "I don't have a problem with the double lock. I just believe that the existing approval process and oversight arrangements we have today are adequate. Of course, in the TCN space, the technical capability notice actually requires two ministers to enable it to be delivered, so I'm satisfied with what we've got," he said. "I know I'm not the person who needs to be satisfied. I don't have, and I would not present, an argument opposed to the oversight that is being proposed here, but I don't believe it is needed."

How the Encryption Debate Might Unfold

In a nutshell, then, the key issues around Australia's encryption laws are oversight and the scope of the laws. Opposition parties and the INSLM want more oversight and a narrower scope. Intelligence agencies are happy with what they have, but they wouldn't object to having less oversight.

The next steps for the government are to release the PJCIS review and their formal response, decide what *ad hoc* changes they might make, if any, and launch into Richardson's five-year project for a new Electronic Surveillance Act.

The government hasn't been moving quickly on these matters though, and the PJCIS already faces a solid stream of work.

Apart from the delays already noted, the PJCIS inquiry into Australia's mandatory telecommunications data retention regime was due to report by April 13, 2020, but that report didn't appear until October 28. An inquiry into "the impact of the exercise of law enforcement and intelligence powers on the freedom of the press" originally due to report in 2019 didn't do so until August 2020.

Still in the pipeline are a review of the Telecommunications Legislation Amendment (International Production Orders) Bill 2020, which is all about exchanging telecommunications data with other countries such as under the U.S. CLOUD Act; a review of the Telecommunications Sector Security Reforms (TSSR), which are all about "a regulatory framework to manage the national security risks of espionage, sabotage and foreign interference to Australia's telecommunications networks and facilities"; and a new Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020, which aims to create a data disruption warrant, a network activity warrant, and an account takeover warrant.[17]

The government seems unlikely to give this legislation a high priority. When it does eventually come up for debate, with so many potential amendments, and with the current close balance of power in both the House of Representatives and the Senate, the exact details are likely to be subject to political horse trading.

About the Author

Stilgherrian is an Australian freelance journalist, commentator, and media producer with a background in computing science and linguistics. He has been covering Australia's internet policy since 2007.

Notes

1 Stilgherrian, "What's Actually in Australia's Encryption Laws? Everything You Need to Know," ZDNet, December 10, 2018, https://www.zdnet.com/article/whats-actually-in-australias-encryption-laws-everything-you-need-to-know/; and "Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (TOLA Act)," via AustLII, http://www.austlii.edu.au/cgi-bin/viewdoc/au/legis/cth/num_act/taolaaaa2018643/.

2 David Wroe, "How the Turnbull Government Plans to Access Encrypted Messages," *Sydney Morning Herald*, June 10, 2017, https://www.smh.com.au/politics/federal/how-the-turnbull-government-plans-to-access-encrypted-messages-20170609-gwoge0.html.

3 TOLA Act, section 317C.

4 Anthony Galloway, "Encryption Powers Not Used by ASIO, Police as Tech Companies Volunteer Help," *Sydney Morning Herald*, August 7, 2020, https://www.smh.com.au/politics/federal/encryption-powers-not-used-by-asio-afp-as-tech-companies-volunteer-help-20200807-p55jhl.html.

5 Official Committee Hansard, Parliamentary Joint Committee on Intelligence and Security, "Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018," August 7, 2020, https://www.aph.gov.au/Parliamentary_Business/Hansard/Hansard_Display?bid=committees/commjnt/30904d8b-7cfb-4ef0-99fb-fba2299b57bf/&sid=0000.

6 Stilgherrian, "The Encryption Debate in Australia," Carnegie Endowment for International Peace, May 30, 2019, https://carnegieendowment.org/2019/05/30/encryption-debate-in-australia-pub-79217.

7 "Telecommunications Amendment (Repairing Assistance and Access) Bill 2019," Parliament of Australia, December 4, 2019, https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fbillhome%2Fs1247%22.

8 Stilgherrian, "Australia's Encryption Laws Will Fall Foul of Differing Definitions," ZDNet, December 11, 2018, https://www.zdnet.com/article/australias-encryption-laws-will-fall-foul-from-differing-definitions/.

9 Review into "Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 and Related Matters," Independent National Security Legislation Monitor, July 9, 2020, https://www.inslm.gov.au/reviews-reports/telecommunications-and-other-legislation-amendment-act-2018-related-matters.

10 James Renwick, "Trust But Verify: A Report Concerning the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 and Related Matters," Independent National Security Legislation Monitor, June 2020, https://www.inslm.gov.au/sites/default/files/2020-07/INSLM_Review_TOLA_related_matters.pdf.

11 "About the AAT," Administrative Appeals Tribunal, accessed November 5, 2020, https://www.aat.gov.au/about-the-aat.

12 "Telecommunications (Interception and Access) Act 1979, Sect 6DA Nominated AAT Members," via AustLII, http://www.austlii.edu.au/cgi-bin/viewdoc/au/legis/cth/consol_act/taaa1979410/s6da.html.

13 Karen Middleton, "Exclusive: Police Bypass Courts for Warrants," *Saturday Paper*, August 3–9, 2019, No. 264, https://www.thesaturdaypaper.com.au/news/politics/2019/08/03/exclusive-police-bypass-courts-warrants/15647544008536.

14 Dennis Richardson, "Comprehensive Review of the Legal Framework of the National Intelligence Community," December 2019, https://www.ag.gov.au/national-security/publications/report-comprehensive-review-legal-framework-national-intelligence-community.

15 "Government response to the Comprehensive review of the legal framework of the National Intelligence Community," Commonwealth of Australia, December 4, 2020, https://www.ag.gov.au/national-security/publications/government-response-comprehensive-review-legal-framework-national-intelligence-community.
16 "Richardson Review: Law Council Deeply Concerned by Recommendation to Cut Judiciary Out of Warrant Approval," Law Council of Australia, December 4, 2020, https://www.lawcouncil.asn.au/media/media-releases/richardson-review-law-council-deeply-concerned-by-recommendation-to-cut-judiciary-out-of-warrant-approval.
17 Stilgherrian, "Australia's Tangle of Electronic Surveillance Laws Needs Unravelling," ZDNet, January 19, 2021, https://www.zdnet.com/article/australias-tangle-of-electronic-surveillance-laws-needs-unravelling/.

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

1779 Massachusetts Avenue NW | Washington, DC 20036 | P: + 1 202 483 7600

CarnegieEndowment.org