INTERNATIONAL ENCRYPTION BRIEF

MAY 2019

The Encryption Debate in Australia

Stilgherrian

The Encryption Debate in Australia

Stilgherrian

For your convenience, this document contains hyperlinked source notes as indicated by teal colored text.

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.

CONTENTS

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 briefing paper 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.

The Encryption Working Group will continue its efforts to study this important issue and plans on releasing further briefings on aspects of the encryption policy debate.

Members of the Encryption Working Group include:

Jim Baker
Former General Counsel, Federal Bureau of Investigation

Katherine Charlet
Program Director, Technology and International Affairs, Carnegie Endowment for International Peace

Tom Donahue
Visiting Fellow, George Mason National Security Institute, and former Senior Director for Cyber Operations, National Security Council, White House

Ed Felten
Robert E. Kahn Professor of Computer Science and Public Affairs, Princeton University

Avril Haines
Senior Research Scholar at Columbia University's Columbia World Projects and former Deputy Director, Central Intelligence Agency

Susan Hennessey
Executive Editor, Lawfare, and Senior Fellow in Governance Studies, the Brookings Institution

Chris Inglis
Managing Director, Paladin Capital Group, and former Deputy Director, National Security Agency

Sean Joyce
US Cybersecurity and Privacy Leader, PwC, and former Deputy Director, Federal Bureau of Investigation

Susan Landau
Bridge Professor of Cyber Security and Policy, Tufts University

Christy Lopez
Distinguished Visitor from Practice, Georgetown Law Center

Alex Macgillivray
Board Member, Data & Society, and former Deputy Chief Technology Officer of the United States

Jason Matheny
Founding Director, Georgetown Center for Security and Emerging Technology, and former Director, Intelligence Advanced Research Projects Activity

Tim Maurer
Co-Director and Fellow, Cyber Policy Initiative, Carnegie Endowment for International Peace

Denis McDonough
Visiting Senior Fellow, Technology and International Affairs, Carnegie Endowment for International Peace, and former White House Chief of Staff

Lisa Monaco
Distinguished Senior Fellow, Reiss Center on Law and Security, New York University School of Law, and former Assistant to the President for Homeland Security and Counterterrorism

Laura Moy
Executive Director, Center on Privacy & Technology, Georgetown Law Center

Michelle Richardson
Director, Privacy and Data Project, Center for Democracy and Technology

Ronald L. Rivest
Institute Professor, Massachusetts Institute of Technology

Ari Schwartz
Managing Director of Cybersecurity Services, Venable LLP

Harlan Yu
Executive Director, Upturn

Denise Zheng
Senior Associate (Non-resident), Technology Policy Program, Center for Strategic and International Studies

Note: This is not a comprehensive list of all members. Some wish to remain anonymous for the time being and to contribute in their personal capacity.

At the end of 2018, Australia gave its intelligence and law enforcement agencies wide-ranging powers to compel communications providers to assist in accessing encrypted communications. This includes giving the attorney general the power to issue a so-called Technical Capability Notice, requiring a provider to create a new interception capability if it is needed to provide future access to encrypted communications that might become subject to a warrant. Assistance may also be demanded of organizations as small as individual website operators.

The driving force for these laws has been the "going dark" problem posed by end-to-end encrypted messaging. While Australia's governing political parties have sold the laws as being necessary for the fight against terrorism and child abuse, law enforcement can also use the laws to investigate relatively minor crimes. Critics have objected to the lack of judicial oversight and the secrecy provisions surrounding any use of the laws.

The laws are framed as part of Australia's contribution to the Five Eyes intelligence alliance. Australia has led the alliance's discussions about the response to encrypted messaging. The laws are controversial, however. They were advanced through public review and parliament in just three months over opposition party and civil society objections, and will continue to be a live political issue as a federal election on May 18, 2019, looms.

Introduction

Late in 2018, the Parliament of Australia passed the most significant changes to the government's communications interception powers in a generation. The 2018 Telecommunications and Other Legislation Amendment (Assistance and Access) Bill, or 2018 Assistance and Access Bill, became law after a divisive fight about its effects on privacy and the legitimate use of encryption.[1] Opponents of the bill condemned the rush to pass it, a lack of transparency, and a poor consultation process, among other problems. The controversy has continued into 2019.

Australia has enjoyed a relatively open debate about national security laws, if not the laws that relate to the intelligence agencies. But this is one of the few times that the discussion has moved into the mainstream, beyond just political actors—like civil society lobbying groups, minor political parties, or independent politicians—and the technical arena. Issues of encryption and digital privacy are no longer solely for the specialists.

Australia is a member of the so-called Five Eyes intelligence alliance with the United States, UK, Canada, and New Zealand. Broadly speaking, Australia's security policies have tended to follow those of its senior partners. These new measures are broadly similar to the UK's 2016 Investigatory Powers Act, but 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.

Background

Echoes of the Crypto Wars

In 1996, at the height of the United States' contested policy discussions about the use of encryption—known as the Crypto Wars—the Australian Attorney-General's Department (AGD) commissioned a major encryption policy review, led by Gerard Walsh, a former deputy director general of the Australian Security Intelligence Organization (ASIO).[2] The full, uncensored version was not released officially until 1999.

The Walsh Report framed the conundrum of encryption in terms that are familiar today. Highlighting encryption's broad availability to individual citizens, the report argued that with the advent of widespread encryption, "advantage moves in the citizen's favour." In response, the report said, law enforcement and national security officials emphasized that "loss of access to real-time communications and to data stored electronically would have a significant and deleterious effect on investigative capability."

The Walsh Report's main conclusion was that "major legislative action is not advised at this time," though it did recommend minor changes. One such change was to combine various investigative powers into a proposed Aid to Public Safety Act, which never happened. "The problem, in a substantive sense, still lies ahead of law enforcement and national security agencies but the distance is shortening rapidly," Walsh wrote.[3]

In the twenty years since then, Australia's national security laws have been framed primarily as a response to global terrorism in the wake of the September 11 attacks. As David Martin Jones noted, the federal government enacted fifty-four pieces of anti-terrorism legislation between 2001 and 2011, in addition to legislation at the state level.[4] Yet there was no real focus on encrypted communications.[5]

Two key pieces of legislation covered communications interception, although neither addressed encryption.

First, the 2014 National Security Legislation Amendment Act (No. 1) extended ASIO's powers such that one computer access warrant could "cover a whole computer network, allowing ASIO officers to disrupt the operation of targeted computers and use third party computers to access targeted computers."[6]

Although the Greens and independent members of parliament (MPs) argued that this effectively gave ASIO the power to intercept the entire internet, those powers became law with "network" left undefined. They also argued that the government was rushing the legislation through parliament to capitalize on a period of widespread fears related to terrorism.[7]

Second, the 2015 Telecommunications (Interception and Access) Amendment (Data Retention) Act made it mandatory for telecommunications providers to log certain data relating to customers' use of their services, and retain it for two years. This so-called metadata included the date, time, and duration of all telephone calls; the source address and destination addresses of emails, and the size and format of any attachments; and the internet protocol (IP) addresses allocated to customers at the time of the communication.[8]

The stored data can be accessed by law enforcement and intelligence agencies without a warrant—except in the case of journalists, where a "journalist information warrant" must be sought.

This legislation was highly controversial, with critics claiming it breached fundamental rights to privacy; that warrantless metadata access could reveal more private information than a communication's content, which would require a warrant; and that the stored data would become a target for hackers.

Origins of the 2018 Assistance and Access Bill

The current chapter of Australia's encryption debate was originally driven by AGD. They had been thinking about the problem of encryption since at least 2015.

In emails released under Freedom of Information requests, AGD said it was aware that "both the technology and broader environment has [sic] changed significantly," and had "undertaken some preliminary thinking about the new challenges in the context of broader plans to improve the Telecommunications (Interception and Access) Act 1979."[9]

AGD was also "mindful that recent developments in the UK and US indicate that those jurisdictions have moved away from the idea of backdoor 'skeleton keys' as a solution."

Senator George Brandis, then Australia's attorney general, framed the response to the increasing use of encryption as a Five Eyes matter, and he was eager for Australia to take the lead.

The first clear statement of this intent came in mid-2017, when the Coalition government led by then prime minister Malcolm Turnbull said it would look at changing laws to force telecommunications and technology firms to help authorities decrypt suspect messages.[10]

Brandis commented that the government wanted to make a proposed 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." The government cited end-to-end encrypted messages as the specific problem.

Brandis also noted that given the difficulties with cracking end-to-end encryption during transmission, one possibility would be to increase law enforcement's ability to access messages at their endpoints. He reassured the public that the government would not ask tech companies to "backdoor" their systems.

This set in place one of the key arguments over the proposed law, and one which has yet to be resolved: Is it actually possible to create access methods into protected communications which are not backdoors?

Brandis announced that the use of the internet by terrorists was of "critical concern" to intelligence and law enforcement, and that "Australia will lead the discussion of ways to address this issue; in particular the involvement of industry in thwarting the encryption of terrorist messaging" at the five nations meeting of attorneys general in Ottawa in late June 2017.[11]

The resulting communiqué noted that "encryption can severely undermine public safety efforts by impeding lawful access" but did not preview any impending legislative actions.[12]

Days later, Turnbull delivered a similar message at the G20 meeting in Hamburg, urging G20 leaders to take a strong stand against terrorists on the battlefield and online. "I understand the legal issues," he reportedly told the meeting. "But we need to say with one voice to Silicon Valley and its emulators: 'You have got to find a way to ensure that these wonderful platforms are not used as dark places for criminals and terrorists to hide.'"[13]

In a joint statement on countering terrorism, G20 leaders subsequently agreed (emphasis added):

> We will work with the private sector, in particular communication service providers and administrators of relevant applications, to fight exploitation of the internet and social media for terrorist purposes such as propaganda, funding and planning of terrorist acts, inciting terrorism, radicalizing and recruiting to commit acts of terrorism, while fully respecting human rights. Appropriate filtering, detecting and removing of content that incites terrorist acts is crucial in this respect. We encourage industry to continue investing in technology and human capital to aid in the detection as well as swift and permanent removal of terrorist content. **In line with the expectations of our peoples we also encourage collaboration with industry to provide lawful and non-arbitrary access to available information where access is necessary for the protection of national security against terrorist threats.** We affirm that the rule of law applies online as well as it does offline.[14]

On December 20, 2017, the Australian government restructured itself. A new mega-agency, the Department of Home Affairs (DHA), was created to take on responsibility for national security, law

enforcement, emergency management, border control, immigration, refugees, citizenship, and multicultural affairs. Under departmental secretary Mike Pezzullo, DHA was given responsibility for the soon-to-emerge legislation.

Oversight of ASIO and the Australian Federal Police (AFP) was moved from the attorney general to the new minister for home affairs, Peter Dutton**.**

While the government had been foreshadowing its anti-encryption legislation for two years, the public consultation process was compressed into just three months at the end of 2018.[15] Government ministers said this was because they had engaged in a year-long consultation process with industry.[16] Australian Prime Minister Scott Morrison demanded expeditious passage, saying, "our police, our agencies need these powers now."[17]

DHA released the first exposure draft of what would become the Assistance and Access Bill on August 14, 2018, with the deadline for any public submissions just four weeks later, on September 10.

At the same time, the Five Eyes were fleshing out their views. The attorneys general of all five states met in September 2018 on Australia's Gold Coast. In a "Statement of Principles on Access to Evidence and Encryption," they said that, as law enforcement has fewer means to access data because of encryption, "court decisions about legitimate access to data are increasingly rendered meaningless."[18]

Further, the joint statement argued that information and communications technology vendors and service providers have a "mutual responsibility" to offer "further assistance" to law enforcement agencies. Service providers who "voluntarily establish lawful access solutions" will have "freedom of choice" in how they do it. "Such solutions can be a constructive approach to current challenges."

> Should governments continue to encounter impediments to lawful access to information necessary to aid the protection of the citizens of our countries, we may pursue technological, enforcement, legislative, or other measures to achieve lawful access solutions.

On September 20, just ten days after the close of public submissions on the first draft of the 2018 Assistance and Access Bill, the government introduced a partially revised version in Parliament that did not address much of the criticism of the first draft.

As is usual with any significant legislation, it was then referred to a parliamentary committee for review—in this case, it went to the powerful Parliamentary Joint Committee on Intelligence and Security (PJCIS). It received public submissions and held public hearings in October and November, before delivering a report on December 5.

Key government stakeholders took part in that process, with some agencies giving their evidence in camera: DHA and its minister, ASIO, AFP, the Australian Criminal Intelligence Commission (ACIC), and the Australian Signals Directorate (ASD, which is overseen by the minister for defense). The Australian Secret Intelligence Service (ASIS), overseen by the minister for foreign affairs, did not make any public appearance. One can assume that all these agencies had been providing advice as the legislation was developed.

The tech community engaged primarily through its trade associations and lobby groups, although some larger corporations did make submissions and give evidence to PJCIS—notably Apple, Cisco, Kaspersky Lab, Microsoft, and the major telecommunications companies Telstra and Optus.

Given the compressed timeline as the Assistance and Access Bill was debated, most stakeholders coordinated their public statements with their submissions and evidence to PJCIS. Media coverage largely followed and reflected that process.

At 6:30 a.m. on December 6, the morning after the PJCIS report was released, the government distributed some sixty-seven pages of amendments to the bill, addressing some of the issues raised in the PJCIS inquiry plus some technical matters. Those amendments and then the bill itself were passed with minimal debate. Despite their objections, the opposition Labor party voted for it. By the end of the day, the Assistance and Access Bill had been passed and two days later, on December 8, it received royal assent and became law.

Main Issues

Pressure from Australia's law enforcement and intelligence agencies, which are worried about losing access to the content of intercepted communications, has been the biggest driver of the encryption policy debate in Australia. The government has set the agenda through legislation, with civil society organizations and the tech industry acting in response.

When the government introduced the Assistance and Access Bill, DHA said the growing prevalence of encryption had "significantly degraded" the capabilities of Australia's intelligence and law enforcement agencies to "collect intelligence, conduct investigations into organised crime, terrorism, smuggling, sexual exploitation of children and other crimes, and detect intrusions into Australian computer networks."[19]

References to organized crime in the Walsh Report have largely been replaced by allusions to terrorism and child exploitation, but the underlying fear of going dark remains.

No specific Australian event has been closely linked to a failure to access encrypted messages—at least, none that are known publicly. However, the fear of going dark is brought up every time there has been a terrorism incident or an arrest on terrorism charges.

For example, on November 21, 2018, brothers Ertunc and Samed Eriklioglu and their friend Hanifi Halis were arrested on suspicion of plotting a terror attack in Melbourne. The case will allegedly rely on 17,000 intercepted telephone calls and more than 10,000 text messages. According to Victoria Police Chief Commissioner Graham Ashton: "The trio's use of encrypted communications made it difficult for police and intelligence agencies to track their activities."[20]

Home Affairs Minister Peter Dutton used the occasion to repeat his "going dark" warning. As the debate around the new laws unfolded over the following days, much of the mainstream media ran with the line that the new laws would protect Australians from terrorism.

The Centerpiece: The 2018 Assistance and Access Bill

The 2018 Assistance and Access Bill, as previously mentioned, is a generational change that builds on more than a dozen pieces of legislation.

The most significant and controversial part has been amending the 1997 Telecommunications Act to create "frameworks for voluntary and mandatory industry assistance to law enforcement and intelligence agencies" that help government access the content of encrypted communications.[21]

Under the new laws, Australian government agencies can issue three kinds of notices or requests:

- Technical Assistance Requests (TAR), which are "voluntary" requests for a "designated communication provider" to use an interception or other data access capability they already have;
- Technical Assistance Notices (TAN), which are compulsory notices for a "designated communication provider" to use a capability they already have; and
- Technical Capability Notices (TCN), which are compulsory notices for a designated communication provider to build a new capability, so that it can meet subsequent Technical Assistance Notices and Requests.

"Designated communication provider" is defined broadly. The full list 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."[22]

The "listed acts or things" that can be asked for is similarly broad. It can include removing one or more forms of electronic protection (defined as authentication or encryption) that are or were applied by, or on behalf of, the provider; or providing technical information; or installing, maintaining, testing, or using software or equipment; or even "modifying, or facilitating the modification of, any of the characteristics of a service provided by the designated communications provider," or "substituting, or facilitating the substitution of, a service provided by the designated communications provider" for another; and, of course, "an act or thing done to conceal the fact that any thing has been done covertly."[23]

It is clear that the government's intent was to create technology-neutral legislation, but the result is legislation so broad that it seems to encompass almost any imaginable provider and "act or thing."

The broad, vague set of "listed acts or things," the wide-ranging list of persons who can be issued with a notice, and the secrecy provisions have all caused confusion. Since employees of providers must not disclose TAR/TAN/TCN information, there have even been concerns that employees might be dragooned in secret without notifying their employers, although some legal experts consider that unlikely.[24][25][26] These issues all remain unresolved.

A voluntary TAR can be issued by the directors general of ASIO, ASIS, or ASD, or by the chief officer of the so-called interception agencies: AFP, ACIC, and the state and territory police forces.

A compulsory TAN can be issued by the director general of ASIO, or the interception agencies—ASIS and the ASD have no remit to demand assistance within Australia.

A TCN, requiring the building of a new capability, can only be issued by the attorney general following a request from ASIO or an interception agency, and only with approval from the minister for communications.

The attorney general must also give written notice of the intention to issue a TCN to the communications provider, inviting them to make a submission and respond. Except in a "matter of urgency"—which, in terrorism cases, is likely to be all of them—that process has to run for at least twenty-eight days. The inspector general of intelligence and security (IGIS) must also be notified.

Notices cannot be issued unless they are "reasonable and proportionate," and compliance with the request would be "practicable" and "technically feasible."

The decisionmaker has to take into account equities such as the interests of national security; the interests of law enforcement; the legitimate interests of the designated communications provider; the objectives of the request; the availability of other means to achieve the objectives; whether the request is the least intrusive form of assistance with respect to "persons whose activities are not of

interest"; and "the legitimate expectations of the Australian community relating to privacy and cybersecurity."

An important factor is that the decisionmaker is the chief officer of the agency issuing the notice. There is no independent judicial oversight. However, there must be an underlying warrant to access the communications under the 1997 Telecommunications (Interception and Access) Act, the 2004 Surveillance Devices Act, or their state-level equivalents.

The Matter of Backdoors

The legislation goes to great lengths to dismiss the possibility of agencies asking for so-called backdoors to be created.

Under the Assistance and Access Bill, agencies cannot ask a provider to "implement or build a new decryption capability," "render systemic methods of authentication or encryption less effective," introduce a "selective" vulnerability or weakness that would "jeopardize the security of any information held by any other person," or create "a material risk that otherwise secure information can be accessed by an unauthorized third party."

The key terms defined in the bill are:

- **Systemic vulnerability**, which means a vulnerability that affects a whole class of technology but does not include a vulnerability that is selectively introduced to one or more target technologies that are connected with a particular person. For this purpose, it is immaterial whether the person can be identified.
- **Systemic weakness**, which means a weakness that affects a whole class of technology but does not include a weakness that is selectively introduced to one or more target technologies that are connected with a particular person. For this purpose, it is immaterial whether the person can be identified.

A lengthy definition of "target technology" refers to a service, device, piece of software, "particular update of software," or any type of data processing device that "is used, or is likely to be used, (whether directly or indirectly) by a particular person," whether or not the person can be identified.

How will these definitions work in practice? This has been a major industry concern.[27]

The TAR/TAN/TCN regime applies to "enforcing the criminal law, so far as it relates to serious Australian offences," which is defined as any federal, state, or territory crime "punishable by a maximum term of imprisonment of 3 years or more or for life."[28] This means the law applies to crimes that the general public might consider relatively minor, such as, in various jurisdictions,

graffiti, criminal damage, a menacing phone call, or even a prank. It certainly includes white-collar crime like fraud or criminal negligence, which means that the law covers communication within almost any enterprise software application or service.

Finally, while the law applies to any "electronic service that has one or more end-users in Australia," among other things, can a TAR/TAN/TCN be enforced if the service has no physical or legal presence in Australia?[29]

Other Aspects of the Assistance and Access Act 2018

The 1979 Australian Security Intelligence Organisation Act and four other acts were amended to provide "an additional power for Commonwealth, state and territory law enforcement agencies investigating certain federal offences to obtain covert computer access warrants under the Surveillance Devices Act 2004; and provide additional powers for law enforcement agencies in relation to the use of existing computer access powers."

An electronic device found while executing a warrant can now be moved to another place for analysis for thirty days, up from fourteen days. The Australian Border Force can now seize and examine an electronic device for thirty days, up from seventy-two hours.

Cross-border Considerations

Cybersecurity is one of the Australian government's nine National Science and Research Priorities. Among other things, the Australian Cyber Security Strategy, launched in April 2016, aims to:

> promote Australian cyber security products and services for development and export, with a particular focus on the Indo-Pacific region. . . . Cyber security is one of the fastest growing sectors in many national economies and Australia is well placed to use our home-grown capabilities to develop business opportunities in this increasingly connected world.[30]

Yet the Assistance and Access Bill seems to have been written without reference to the supposed importance of trust in Australia's cyber products. Such issues have only emerged in the very final stages of the current debate, and then only from the industry side.

According to the tech industry, the viability of Australian businesses overseas is being threatened, as is the appeal of Australian industry as an investment. Some claim to already be losing customers. This is being seen as an incompatibility with those innovation and cybersecurity strategies.[31]

Again, the law applies to international companies doing business in Australia, raising concerns about Australians being denied access to certain services or hardware. Vendors might decide that

Australia's relatively small market of 25 million people isn't worth developing compliant products and internal processes.

Similar issues arose in the development of the UK's 2016 Investigatory Powers Act, particularly in relation to foreign companies being forced to remove encryption from communications. The consensus was that "this legal duty cannot be imposed on overseas companies, such as Apple, that use a form of encryption which they say they cannot themselves breach."[32]

The main cross-border issues raised by the government have been about cooperation in law enforcement, and in particular speeding up what Brandis described in 2017 as "the rather prolonged procedure of mutual legal assistance treaties [MLAT]." Little specific has been said in the public domain, however.

Related Issues

End-to-end encrypted messaging has most vexed Australia's law enforcement and intelligence agencies. Device encryption has not emerged as a subset of the debate, as it has in the United States.

ASIO can obtain a computer access warrant from the attorney general, which can include authority to access "any other computer or a communication in transit to access the relevant data," and "if necessary to achieve that purpose—adding, copying, deleting or altering other data in the computer or the communication in transit," and doing "any thing reasonably necessary to conceal the fact that any thing has been done under the warrant."[33] The use of any such warrants would fall under the usual secrecy provisions of ASIO's activities.

The extent to which these warrants are used, and what specific actions might be taken, is unknown. Not even a total number of warrants issued is reported.

With the passage of the Assistance and Access Bill, a computer access warrant may now also be used in the investigation of "certain federal criminal offences" rather that purely national security matters. ASIO can now also "require a person with knowledge of a computer or a computer system to provide assistance that is reasonable and necessary to gain access to data on a device that is subject to an ASIO warrant."

This again raises the concern that a software engineer or systems administrator could be asked to do something by ASIO on company systems but ordered not to tell their employer. The legislation does not offer any clarity.

Computer access warrants could thus be used to access unencrypted communications on endpoint devices.

There is also a broadly worded provision in the 1997 Telecommunications Act that outlines the responsibilities of telecommunications carriers and carrier or carriage service provider. Section 313 requires them to do their "best to prevent telecommunications networks and facilities from being used in, or in relation to, the commission of offences against the laws of the Commonwealth or of the States and Territories." They must give government officers and authorities "such help as is reasonably necessary" to enforce the criminal law and laws imposing pecuniary penalties and well as international criminal laws, protect the public revenue, or safeguard national security.[34]

Section 313 powers have been used for a wide variety of tasks. It is fair to say that one goal of the Assistance and Access Bill was to strengthen these powers and extend the responsibilities beyond telecommunications carriers to the rest of the communications ecosystem.

The 1996 Walsh Report did spend some time discussing the location and management of key and data storage, but this has not been part of the public debate since that era.

Outlook

The main force shaping what happens next, at least in the short term, will continue to be Australian party politics.

In the final days before the Assistance and Access Bill vote in December 2018, the debate became highly contentious, with the government using any attempts by the opposition as a political wedge to portray them as soft on national security.

The opposition Labor party had tried to delay the vote so that advice and amendments could be given more consideration. Government ministers responded by accusing Labor of "running a protection racket for terrorists" and of being "quite happy for terrorists and organised criminals to chat on WhatsApp, leaving our security agencies in the dark."[35]

Since then, a PJCIS review of those sixty-seven pages of amendments recommended nothing more than properly funding IGIS and the Independent National Security Legislation Monitor to conduct their reviews.[36] The government has fulfilled its promise to return the legislation to the Senate for further review, but there has been no debate yet.

The 2019 federal election will be held on May 18, 2019. Based on current polling, the Liberal-National Coalition government is anticipated to lose.[37]

The Labor party, currently in opposition, has pledged to amend the bill. At its national conference on December 16, 2018, Labor condemned the "appallingly inadequate process" in relation to the

Assistance and Access Bill, and called upon its own MPs to "further engage and work with industry and civil society and economic regulators" in outstanding issues such as the security and safety of the internet, the impact on Australian industry and businesses relying on encryption, and civil liberties and transparent public reporting.[38]

In March 2019, Labor's spokesman on the digital economy, Ed Husic, committed the party rewriting the laws if it wins. "This is as much about national security as it is about economic security," he said.[39] He also committed to attempting to rewrite the laws from opposition, should the Coalition retain control of the government.

In the medium term, law enforcement agencies are free to continue using the new legislation. AFP says it has already done so, although DHA is "still consulting with industry" on how to implement the new powers.[40]

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 for more than a decade.

The author would like to thank Fergus Hansen, Tom Uren, and another expert for their review of the manuscript.

Notes

1 *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, Australian Parliament. https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22legislation/billhome/r6195%22

2 *Review of policy relating to encryption technologies*, Gerard Walsh, 10 October 1996. https://www.efa.org.au/Issues/Crypto/Walsh/walsh.htm

3 Walsh, paragraph 1.2.1.

4 "Intelligence and the management of national security: the post 9/11 evolution of an Australian National Security Community", David Martin Jones, *Intelligence and National Security*. Volume 33, 2018. https://www.tandfonline.com/doi/full/10.1080/02684527.2016.1259796

5 "All of Australia's national security changes since 9/11 in a timeline", Nick Evershed & Michael Safi, *The Guardian*, 19 October 2015. https://www.theguardian.com/australia-news/ng-interactive/2015/oct/19/all-of-australias-national-security-changes-since-911-in-a-timeline

6 "Explainer: What do the new anti-terrorism laws involve and how will they will be rolled out?", Emma Griffiths, ABC News, 28 May 2015. https://www.abc.net.au/news/2014-09-22/new-anti-terrorism-laws-explained/5761516

7 "Parliament passes law to let ASIO tap entire internet", Allie Coyne, *iTnews*, 1 October 2014. https://www.itnews.com.au/news/parliament-passes-law-to-let-asio-tap-entire-internet-396365

8 "Revised Explanatory Memorandum on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015", Australian Parliament, 19 March 2015.

http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fems%2Fr5375_ems_ac4732e1-5116-4d8f-8de5-0ead3828012c%22

[9] "Australia's semantic sleight of hand on encrypted messaging revealed", Stilgherrian, *ZDNet*, 13 June 2018. https://www.zdnet.com/article/australias-semantic-sleight-of-hand-on-encrypted-messaging-revealed/

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

[11] "Australia will lead Five Eyes discussions to 'thwart' terrorist encryption: Brandis", Chris Duckett, *ZDNet*, 26 June 2017. https://www.zdnet.com/article/australia-will-lead-five-eyes-discussions-to-thwart-terrorist-encryption-brandis/

[12] "Five Country Ministerial 2017: Joint Communiqué", Ottawa, 27 June 2017. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/fv-cntry-mnstrl-2017/index-en.aspx

[13] "Turnbull targets online terror at G20", SBS News, 7 July 2017. https://www.sbs.com.au/news/turnbull-targets-online-terror-at-g20

[14] "The Hamburg G20 Leaders' Statement on Countering Terrorism", G20, 7 July 2017. http://www.g20.utoronto.ca/2017/170707-counterterrorism.html

[15] "How government haste is ruining its own anti-encryption law", Stilgherrian, *ZDNet*, 25 November 2018. https://www.zdnet.com/article/how-government-haste-is-ruining-its-own-anti-encryption-law/

[16] Rohan Pearce, "Alarm over government's encryption bill rush," *ComputerWorld,* September 20, 2018. https://www.computerworld.com.au/article/647056/alarm-over-government-encryption-bill-rush/

[17] Chris Duckett, "Australian PM insists on encryption-busting Bill being passed in next sitting fortnight." *ZDNet,* November 22, 2018. https://www.zdnet.com/article/australian-pm-insists-on-encryption-busting-bill-being-passed-in-next-sitting-fortnight/

[18] "Statement of Principles on Access to Evidence and Encryption", Australian Government Department of Home Affairs, 2018. https://web.archive.org/web/20180925154820/https://www.homeaffairs.gov.au/about/national-security/five-country-ministerial-2018/access-evidence-encryption

[19] *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* Explanatory Memorandum, 20 September 2018, paragraphs 3–5. https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r6195_ems_1139bfde-17f3-4538-b2b2-5875f5881239/upload_pdf/685255.pdf;fileType=application%2Fpdf (PDF)

[20] "Melbourne terror attack plot suspects arrested in police raids over mass shooting fears", *ABC News*, 21 November 2018. https://www.abc.net.au/news/2018-11-20/three-men-charged-with-planning-a-terrorist-act-in-melbourne/10513328

[21] "What's actually in Australia's encryption laws? Everything you need to know", Stilgherrian, *ZDNet*, 10 December 2018. https://www.zdnet.com/article/whats-actually-in-australias-encryption-laws-everything-you-need-to-know/

[22] *Assistance and Access Bill 2018* as passed, section 317C.

[23] *Assistance and Access Bill 2018* as passed, section 317E.

[24] *Assistance and Access Bill 2018* as passed, section 317ZF.

[25] "Submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018", Communications Alliance et al, 22 January 2019, p.13. https://www.commsalliance.com.au/__data/assets/pdf_file/0006/62475/190122_Submission-to-PJCIS_Assistance-and-Access-Bill-Review-2019_SUBMITTED.pdf

[26] "Australia's encryption laws are 'highly unlikely' to dragoon employees in secret", Stilgherrian, *ZDNet*, 17 December 2018. https://www.zdnet.com/article/australias-encryption-laws-are-highly-unlikely-to-dragoon-employees-in-secret/

[27] "Australia's encryption laws will fall foul of differing definitions", Stilgherrian, *ZDNet*, 11 December 2018. https://www.zdnet.com/article/australias-encryption-laws-will-fall-foul-from-differing-definitions/

[28] *Assistance and Access Bill* as passed, section 317B.

[29] *Assistance and Access Bill 2018* as passed, section 317C(b)4 etc.

[30] "Growth and Innovation", Australian Cyber Security Strategy. Accessed 4 January 2019. https://cybersecuritystrategy.homeaffairs.gov.au/sgrowth-ands-innovation

[31] "Atlassian leads encryption law revolt as Peter Dutton stands firm", Paul Smith and Bo Seo, *Australian Financial Review*, 11 February 2019. https://www.afr.com/technology/web/security/atlassian-leads-encryption-law-revolt-as-peter-dutton-stands-firm-20190207-h1ayk2

[32] "UK surveillance powers explained", *BBC News*, 5 November 2015. https://www.bbc.com/news/uk-34713435

[33] *Australian Security Intelligence Organisation Act 1979*, Section 25A Computer access warrant. http://www6.austlii.edu.au/cgi-bin/viewdoc/au/legis/cth/consol_act/asioa1979472/s25a.html

[34] *Telecommunications Act 1997*, Section 313 Obligations of carriers and carriage service providers. http://www6.austlii.edu.au/cgi-bin/viewdoc/au/legis/cth/consol_act/ta1997214/s313.html

[35] "Govt piles on encryption pressure in final week", Ry Crozier, *iTnews*, 3 December 2018. https://www.itnews.com.au/news/govt-piles-on-encryption-pressure-in-final-week-516411

[36] Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018, Parliamentary Joint Committee on Intelligence and Security. https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/ReviewofTOLAAct/Report

[37] "BludgerTrack: 51.9-48.1 to Labor", William Bowe, *The Poll Bludger*, 2 May 2019. https://www.pollbludger.net/2019/05/02/bludgertrack-51-9-48-1-labor-2/

[38] "Politics Live: Labor vows to restore penalty rates and address gender pay gap – as it happened", *The Guardian*, 18n December 2018. https://www.theguardian.com/australia-news/live/2018/dec/18/labor-national-conference-day-three-politics-live?page=with:block-5c187a23e4b08a19177b1429#block-5c187a23e4b08a19177b1429

[39] "Labor will rewrite encryption laws", James Riley, *InnovationAus*, 27 March 2019. https://www.innovationaus.com/2019/03/Labor-will-rewrite-encryption-laws

[40] "AFP says new encryption laws have helped coerce suspects into unlocking devices", Paul Karp, *The Guardian*, 4 February 2019. https://www.theguardian.com/australia-news/2019/feb/04/afp-says-new-encryption-laws-have-helped-coerce-suspects-into-unlocking-devices

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

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

CarnegieEndowment.org