Hardy, Keiran

**Article**

# Australia's encryption laws: Practical need or political strategy?

Internet Policy Review

**Provided in Cooperation with:**
Alexander von Humboldt Institute for Internet and Society (HIIG), Berlin

*Suggested Citation:* Hardy, Keiran (2020) : Australia's encryption laws: Practical need or political strategy?, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 9, Iss. 3, pp. 1-16, https://doi.org/10.14763/2020.3.1493

This Version is available at:
https://hdl.handle.net/10419/224934

INTERNET POLICY REVIEW
Journal on internet regulation

Volume 9 | Issue 3

# Australia's encryption laws: practical need or political strategy?

**Keiran Hardy**
*Griffith Criminology Institute, Griffith University, Brisbane, Australis, k.hardy@griffith.edu.au*

Published on 26 Aug 2020 | DOI: 10.14763/2020.3.1493

**Abstract:** To investigate terrorism, law enforcement and intelligence agencies increasingly require assistance from multinational technology companies including Facebook, Google and Apple. These companies can assist with decrypting secret communications or unlocking personal devices, but not, they maintain, without undermining the privacy and security of all their users. While other western countries continue to debate these issues, Australia legislated quickly to enhance decryption capabilities with little industry consultation. This article examines the encryption laws recently enacted by the Australian federal parliament, which allow law enforcement and intelligence agencies to require technical assistance from 'designated communications providers'. It interrogates the government's justifications for these laws and examines the wider legal and political context in which they were enacted. The analysis confirms that Australia's approach to decryption does not represent sound practice and instead reflects a pattern of rights-infringing lawmaking in response to terrorism.

**Keywords:** Encryption, Counter-terrorism laws, Terrorism, Industry assistance

Article information

**Received:** 23 Aug 2019 **Reviewed:** 07 Feb 2020 **Published:** 26 Aug 2020

**Competing interests:** The author has declared that no competing interests exist that have influenced the text.

**URL:**
http://policyreview.info/articles/analysis/australias-encryption-laws-practical-need-or-political-strategy

**Citation:** Hardy, K. (2020). Australia's encryption laws: practical need or political strategy?. *Internet Policy Review*, *9*(3). DOI: 10.14763/2020.3.1493

# INTRODUCTION

Terrorist groups commonly use encrypted messaging applications to conceal their activities while recruiting new members, spreading propaganda and planning their attacks (Graham, 2016; Smith, 2017). Freely available smartphone applications like WhatsApp, Telegram and Facebook Messenger employ end-to-end encryption, which is so secure that the content of the messages cannot be read by any third parties, including the technology companies that build the

product (Lewis, Zheng, & Carter, 2017). This problem – known as terrorist organisations 'going dark' – poses a major challenge for law enforcement and intelligence agencies, who routinely intercept communications to disrupt terrorist plots and prosecute individuals for terrorism offences (Forcese & West, 2020; Lewis, Zheng, & Carter, 2017). Law enforcement investigations can also be hindered by phone passcodes and other methods of authentication, which cannot be bypassed without undermining the privacy and security of other users. For example, several requests by the United States Federal Bureau of Investigation to unlock criminals' iPhones have been denied by Apple, on the grounds that the data is encrypted locally on the device and cannot be accessed 'without attacking fundamental elements of iOS security' (Brandom, 2020).

Western governments are addressing these challenges by regulating technology companies directly, but there is no consensus as to best practice and some hesitation to legislate too strongly. This is partly due to the difficulties in governments regulating multinational tech giants, as well as concerns about privacy and cyber-security. In the United Kingdom, the Home Secretary can issue technical capability notices under the Investigatory Powers Act 2016 (IPA), which can require 'removal by a relevant operator of electronic protection' (section 253). However, the British government has so far exerted political rather than legal pressure, with threats of stronger regulation but no further legislation (Baker, 2019; Hern, 2017). In 2017, WhatsApp (which is owned by Facebook) reportedly refused to comply with a request by the British government to build a backdoor into the application (Ong, 2017). This suggests either that the IPA scheme lacks teeth or the British government is unwilling to pursue civil claims against large multinationals that refuse to cooperate. In the European Union, the position is even less clear, with France and Germany calling for stronger regulation of encryption but no consensus on how member states will proceed (Baker, 2019; Koomen, 2019; Toor, 2016). The European Commission has so far supported only non-legislative measures in response (European Commission, 2017). In the United States, senior officials continue to disagree on the benefits and risks of regulating encryption, with little resolution in sight (Baker, 2019; Geller, 2019).

The Australian government has not had the same qualms. In 2018, the federal parliament enacted the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Cth), which is known as 'TOLA' or, more commonly in the media, as the 'encryption laws' (Bogle, 2018). The legislation was enacted on a very short timetable, with little public consultation or parliamentary debate (Bogle, 2019). Its extensive powers have been heavily criticised not only by the technology industry, in Australia and globally, but also by a wide range of legal, civil society and human rights organisations (Australian Information Industry Association, 2018; Australian Human Rights Commission, 2018; Digital Industry Group, 2018). The legislation allows law enforcement and intelligence agencies to require technical assistance from 'designated communications providers', a broadly defined term which encompasses the largest social media companies down to small hardware and software suppliers (Telecommunications Act 1997 (Cth), s 317C). It permits an almost unlimited range of technical assistance, extending beyond decryption to include modifying consumer products and services (Telecommunications Act 1997 (Cth), s 317E).

In this article, I explain and interrogate the reasons why TOLA was enacted. In section 1, I explain the powers in their current form and assess whether there are meaningful limits to their scope. In section 2, I explore the political and parliamentary process by which these laws were enacted, including the government's claims for urgency and the role of the Labor Party in opposition. In section 3, I explore the wider legal and political context, including Australia's previous responses to terrorism and a lack of enforceable human rights protection. From this

analysis, it becomes clear that Australia's encryption laws reflect a pattern of highly politicised responses to terrorism within a permissive constitutional environment. They increase the impact of Australia's existing counter-terrorism laws on human rights by generating further risks to privacy, free speech and freedom of the press.

## SECTION 1: AUSTRALIA'S ENCRYPTION LAWS

Australia's encryption laws, also known as TOLA, created a tiered regulatory scheme by which law enforcement and intelligence agencies can request or require technology companies to provide them with technical assistance. The scheme was inserted into the Telecommunications Act 1997 (Cth) ('Telecommunications Act') in early December 2018. There are three tiers of notices: technical assistance requests (TARs), technical assistance notices (TANs), and technical capability notices (TCNs). Each of these provides immunity from civil liability for companies which act in accordance or good faith with the terms of a notice (Telecommunications Act, ss 317G, 317ZJ). The requests or requirements in each notice must be reasonable, proportionate, practicable, and technically feasible (Telecommunications Act, ss 317JAA, 317P, 317V).

TARs request voluntary assistance and can be issued by the head of a law enforcement or intelligence agency for wide purposes relating to the functions of those authorities. This includes enforcing serious crimes, safeguarding national security, protecting Australia's foreign relations or national economic well-being, and maintaining the security of electronic information (Telecommunications Act, s 317G).

TANs require mandatory assistance and set higher standards for approval. They can also be issued by the head of a law enforcement agency, but only with the approval of the Commissioner of the Australian Federal Police (AFP). Alternatively, they can be approved by the Director-General of the Australian Security Intelligence Organisation (ASIO), Australia's domestic intelligence agency (Telecommunications Act, ss 317, 317LA). TANs cannot be issued by Australia's foreign intelligence agencies. The purposes for issuing TANs are also narrower than those triggering TARs: they are available only to enforce serious criminal offences or safeguard national security (Telecommunications Act, ss 317). A company that fails to comply with a TAN fines of up to AUD$ 10 million (Telecommunications Act, s 317ZB).

TCNs also involve mandatory assistance, but they can require companies to develop new technical capabilities. As such, an added layer of protection applies. TCNs are available for the same purposes as TANs but they can only be issued by the Commonwealth Attorney-General on request by the Director-General of Security or the head of a law enforcement agency (Telecommunications Act, s 317T). The same penalty for non-compliance applies.

There are no clear limits to the types of technology companies that could be issued with a TOLA notice. A notice can be issued to any 'designated communications provider' (DCP), a broadly defined term that encompasses 15 company types. These include telecommunications service providers, internet hosting services, software and hardware suppliers, any company that 'operates a facility', and, at its broadest, any company that 'provides an electronic service that has one or more end users in Australia' (Telecommunications Act, s 317C). In this respect, the scheme extends far beyond regulating major multinationals such as Facebook and Apple, which have been the focus of global debates surrounding encryption. Notices can be issued to national telecommunications and internet service providers (such as Telstra, Vodafone and Optus) and even small software and hardware companies. The definition of a DCP could also extend to

banks, universities, insurers, retailers and other businesses that offer online services to Australian end-users. Many of the categories mentioned above also include activities that facilitate, or are ancillary or incidental to, the main activity. This could plausibly include marketing companies, distributors and retailers.

The types of technical assistance that can be required under the legislation are similarly broad (Telecommunications Act, s 317E). They include:

- removing one or more forms of electronic protection;
- installing, maintaining, testing or using software or equipment;
- assisting access to facilities, customer equipment, data processing devices, carriage services, or other electronic services;
- assisting with the testing, modification, development or maintenance of a technology or capability;
- modifying any of the characteristics of a service;
- substituting part of a service; and
- concealing the fact that anything has been done under the scheme

Only the first of these – removing electronic protection – relates directly to the problem of end-to-end encryption. DCPs can be required to provide many other types of assistance, such as installing software or modifying consumer products and services. For example, Apple argued in a parliamentary inquiry on the Bill that it could be required to install eavesdropping capability in its home speakers (Apple Inc., 2018). It is unlikely that ASIO or the AFP would ever require this, and amendments introduced into the final version of the Bill (explained further below) prevent the scheme being lawfully used for large-scale surveillance. However, the types of assistance available certainly extend beyond decryption to a wide range of unknown tasks.

These are extraordinary powers with few protections. Some additional accountability is provided by the requirement that law enforcement TANs be approved by the AFP Commissioner rather than the head of a state police force, although higher approval for TANs need not be sought by ASIO. The requirement that TCNs be approved by the Attorney-General is more rigorous again, although ministerial warrants still do not entail the same degree of independence as authorisation by a judge or magistrate. This contrasts with the IPA scheme in the UK, where technical capability notices must be approved through a 'double-lock' process involving both a judicial commissioner (an appointed former judge) and the Home Secretary (Investigatory Powers Act 2016 (UK), s 254).

The major limitation on the TOLA powers is that DCPs cannot be required to build a 'systemic weakness' or 'systemic vulnerability' into a product or service (Telecommunications Act, s 317ZG). In the original version of the Bill, these terms were left undefined, and while there is now some statutory guidance, significant confusion remains. The clearest definition available is that any assistance provided should not 'affect a whole class of technology' (Telecommunications Act, s 317B). In addition, companies cannot be required to develop new decryption capabilities or take action that would 'render systemic methods of authentication or encryption less effective' (Telecommunications Act, s 317ZG). This seemingly undermines the main purpose of the legislation, which was to allow greater access to encrypted communications. However, requests for decryption are still possible in individual cases, provided that the company already has the technical capability to unscramble the content. This is clear as a vulnerability can be 'selectively introduced to one or more target technologies that are connected with a particular person' (Telecommunications Act, s 317B). However, it remains doubtful whether this is technically possible without creating risks to other users (Apple Inc., 2018; Digital Industry Group, 2018). This remains a sticking point for other countries seeking to

regulate encryption (Baker, 2019), and it is doubtful that the Australian approach solves this problem.

TOLA also includes reporting requirements. The issuing of any notice must be reported to the Commonwealth Ombudsman (for law enforcement) or the Inspector-General of Intelligence and Security (IGIS) (for intelligence agencies). The IGIS is an independent statutory authority that has oversight of Australia's intelligence agencies and conducts inquiries into their operations as well as regular inspections (Hardy & Williams, 2016b). Reporting to the IGIS is an important inclusion that will enhance accountability, although most of the details in IGIS's annual reports remain classified, so the public must largely trust rather than know that the agencies are being held to account (Hardy & Williams, 2016b). The Home Affairs Minister must produce a public report on TOLA usage, but this only includes the raw numbers for how many times the powers were used by law enforcement in relation to which types of offences (Telecommunications Act 1997, s 317ZS). ASIO must also include the number of TOLA notices issued in its annual report (Australian Security Intelligence Organisation Act 1979 (Cth), s 94), but again these are raw numbers only. In its latest report, the entire appendix containing those numbers was redacted (ASIO, 2019).

These limited reporting requirements mean there are very scant details about the use of TOLA in practice, and that this is likely to remain the case over time. This is further enforced by a disclosure offence, punishable by five years' imprisonment, which prohibits DCP employees (and law enforcement or intelligence officers) from revealing anything about the use of the powers (Telecommunications Act, s 317ZF). This offence is likely to stifle any meaningful public discussion that could contribute to subsequent reviews and amendments by parliament.

## SECTION 2: POLITICAL AND PARLIAMENTARY PROCESS

TOLA was passed very quickly by the federal parliament following a truncated committee inquiry. Draft legislation was released for public consultation on 14 August 2018 and the Bill was introduced into the House of Representatives on 20 September 2018. When he introduced the Bill, Peter Dutton, the Minister for Home Affairs, explained that encryption is 'eroding the capacity of Australia's law enforcement and security agencies to investigate serious criminal conduct and protect Australians' (Dutton, 2018). He cited the November 2015 terrorist attacks in Paris as an example of terrorist groups using encrypted messaging services to conceal their activities from authorities while planning a mass-casualty attack (Dutton, 2018). With regard to Australia, he explained that 90 percent of ASIO's priority cases, and the same percentage of AFP data intercepts, are impacted by encryption (Dutton, 2018). It was not clear from this statement whether he meant end-to-end encryption, the most secure kind which generated the need for new powers, or any type of encryption, such as passwords for email accounts, which are commonly bypassed by authorities. Given that he referred to encryption 'in some form' (Dutton, 2018), the latter seems more likely. It is more plausible that 90 percent of intercepted communications employ some type of encryption, with some smaller (unspecified) percentage employing the stronger end-to-end variety. Otherwise, nearly all of the telecommunications data intercepted by the AFP would be unreadable.

After Dutton's second reading speech, the bill was referred immediately to the Parliamentary Joint Committee on Intelligence and Security (PJCIS). The PJCIS is a bipartisan committee which examines Australia's counter-terrorism laws, reviews listings of proscribed terrorist organisations, and oversees the financing of Australia's intelligence agencies. In contrast to

similar committees in the UK and US, the PJCIS does not have oversight of intelligence agency operations; its role is largely limited to making law reform recommendations (Intelligence Services Act 2001 (Cth), s 29).

The PJCIS conducted hearings on the Bill in October and November of 2018, after receiving more than 100 written submissions from law reform and human rights organisations, digital rights organisations, and technology companies based in Australia and overseas. These groups have diverse motivations, and at other times can be opposed on rights-based issues. For example, human rights groups have advocated for stronger regulation of social media companies to prevent hate crime and other online abuse (Amnesty International, 2020). Social media and technology companies have business interests at heart and shareholders to think of, which represents a very different starting point to a rights-based organisation when thinking about platform regulation. Nonetheless, with regard to the encryption laws, there was a notable consensus amongst otherwise strange bedfellows. Across these groups, the submissions identified many similar concerns with the Bill (Apple Inc., 2018; Australian Human Rights Commission, 2018; Australian Information Industry Association, 2018; Australian Information security Association, 2018; Cannataci, 2018; Digital Industry Group, 2018; Law Council of Australia, 2018; Mozilla, 2018). The major issues raised in the submissions included:

- Vagueness and overbreadth as to the types of companies to be targeted, devices affected, and assistance provided;
- The absence of statutory definitions as to when a company would be introducing a 'systemic weakness' or 'systemic vulnerability' into a product or service;
- Additional risks to privacy and cyber-security if vulnerabilities are introduced to assist with decryption, which could be exploited by malicious actors;
- Technical difficulties in complying with the scheme in individual cases, without weakening encryption for all users;
- Limited transparency and a lack of judicial oversight in the approval of notices;
- A likely economic impact on technology companies, both locally and globally, as consumer trust in their products and services would be undermined; and
- Potential for significant conflict of laws across jurisdictions

In his written submission, the United Nations Special Rapporteur on the right to privacy offered a thorough, scathing critique (Cannataci, 2018). He believed the safeguards in the bill were 'illusory rather than substantive', and offered this dressing-down of the government's approach:

In my considered view, the Assistance and Access Bill is an example of a poorly conceived national security measure that is equally as likely to endanger security as not; it is technologically questionable if it can achieve its aims and avoid introducing vulnerabilities to the cybersecurity of all devices irrespective of whether they are mobiles, tablets, watches, cars, etc., and it unduly undermines human rights including the right to privacy (Cannataci, 2018).

Alongside other major players from the technology industry, including Apple, Facebook and Amazon (Apple Inc., 2018; Digital Industry Group, 2018), Mozilla went so far as to say that the powers 'could do significant harm to the Internet' (Mozilla, 2018).

It was obvious, then, that the legislation to be debated by parliament had significant structural problems, both principled and practical. Despite these fundamental issues, the PJCIS inquiry was expedited and the Bill passed in a single day in essentially its original form. The enacted version did incorporate a long list of amendments introduced by the government, including most of the 17 changes recommended by the PJCIS (2018). As discussed in Section 1, these included approval of law enforcement TANs by the AFP Commissioner, additional reporting requirements, and improved definitions of 'systemic weakness' and 'systemic vulnerability'.

However, the other changes were largely cosmetic and none addressed the most fundamental concerns, including the breadth of possible technical assistance and a lack of judicial oversight.

The truncated timetable for the PJCIS inquiry and approval by parliament was due to government intervention. On 22 November, Dutton contacted the committee to say 'there was an immediate need to provide agencies with additional powers and to pass the Bill in the last sitting week of 2018' (PJCIS, 2019). He cited a recent terrorist stabbing in Melbourne and an increased threat of terrorism over the Christmas and New Year period:

I am gravely concerned that our agencies cannot rule out the possibility that others may also have been inspired by events in Melbourne to plan and execute attacks … This is particularly concerning as we approach Christmas and the New Year, which we know have been targeted previously by terrorists planning attacks against Australians gathered to enjoy the festive season …

For these reasons I ask that the committee accelerate its consideration of this vital piece of legislation to enable its passage by the parliament before it rises for the Christmas break (PJCIS, 2019).

The committee accepted the Minister's advice but later commented that the 'expedited consideration … precluded the Committee from incorporating a detailed presentation of the evidence informing its recommendations' (PJCIS, 2019). The inquiry was completed and the committee's recommendations largely accepted by government, but in major respects the most significant opportunity to review the controversial new laws was left unfinished.

The TOLA legislation was approved by both Houses of Parliament on 6 December, on the last sitting day of Parliament before the end of the year. The Labor opposition had initially opposed the bill, with Shadow Attorney-General Mark Dreyfus declaring that the bill was 'unworkable and potentially weakens Australia's security' (Duckett, 2018c). However, after being accused by senior Liberal Party members of being soft on national security – even 'running a protection racket for terrorists' (Duckett, 2018a) – Labor capitulated at the eleventh hour, withdrawing amendments it had proposed in the Senate and allowing the bill to pass (Worthington & Bogle, 2018). In explaining Labor's backdown, then Opposition Leader Bill Shorten told the public, 'Let's just make Australians safer over Christmas (Duckett, 2018b). The Labor Party claimed it would pursue amendments to the bill in the coming year or if it was elected to government (Duckett, 2018b; Seo, 2019), but it remains in opposition and no substantive changes to the powers have since been made.

Further reviews into TOLA have been conducted by the PJCIS and the Independent National Security Legislation Monitor (INSLM, 2020). The INSLM is an independent statutory office, based on the UK's Independent Reviewer of Terrorism Legislation, which examines Australia's counter-terrorism laws to determine if they are proportionate, effective, necessary, and compatible with human rights (Independent National Security Legislation Monitor Act 2010 (Cth), s 6). At the time of writing, the PJCIS is yet to publish its findings. The INSLM (2020) has recommended that TANs and TCNs, which require mandatory assistance, be subject to judicial approval by a new Investigatory Powers Division of the Administrative Appeals Tribunal, rather than executive approval by the Attorney-General or head of an agency. In addition, he recommended that an Investigatory Powers Commissioner and Commission, similar to those found in the UK, be created to enhance oversight of the regime (INSLM, 2020). Finally, he offered a tighter, singular definition of systemic weakness and vulnerability, focusing on whether the modification creates a material risk of data being accessed by a third party (INSLM,

2020). It remains to be seen whether these recommendations will be taken up by the federal government.

## SECTION 3: LEGAL AND POLITICAL CONTEXT

Across a wide range of technology companies and civil society actors, both locally and globally, TOLA is recognised as adopting a highly problematic approach. This begs the question, if the laws were so obviously problematic, why were they allowed to pass? Were they justified in the Australian context as an urgently needed response to terrorism?

Australia has enacted a significant body of counter-terrorism laws since 9/11, including many more recently in response to Islamic State and the threat of returning foreign fighters (Hardy & Williams, 2016a). At last count, the federal parliament alone had enacted more than 80 separate pieces of legislation in response to terrorism (McGarrity & Blackbourn, 2019). These counter-terrorism laws have created extensive criminal offences and powers, including detention and supervision orders and expanded surveillance warrants. Despite this, until TOLA there was no legal mechanism allowing authorities greater access to encrypted communications. There were a variety of powers available, both to law enforcement and intelligence agencies, to intercept communications between persons of interest (McGarrity & Hardy, 2020), but none of these addressed the problem of terrorist organisations 'going dark' through end-to-end encryption. In this respect, some legal response to the encryption issue was justified. However, this does not excuse the specific powers that were created, or the timeframe in which they were enacted.

In pushing for the laws to be enacted before the end of parliament's sitting year, the government cited an urgent threat of terrorism (PJCIS, 2019). To some extent, this might have justified imperfect laws and a truncated timetable, if lives would be saved as a direct consequence of bypassing more extensive consultation. However, and while the exact details of TOLA usage remain classified, there is sufficient reason to doubt the government's claims of urgency. As discussed in Section 1, the Home Affairs Minister claimed that 90 percent of ASIO and law enforcement investigations are impacted by encryption (Dutton, 2018), but this figure (if accurate) more likely captures all types of encryption rather than the stronger end-to-end variety. The figure also suggests that encryption raises systemic, longstanding issues for terrorism investigations, which could be resolved over a longer timeframe. The Minister did cite a recent terrorist stabbing in Melbourne and a heightened threat over Christmas (PJCIS, 2019), but neither of these indicated that a specific terrorist plot could be averted or that lives could be saved by enacting the laws before the end of the year. The Director-General of ASIO, Duncan Lewis, explained there were 'cases afoot at the moment where this legislation will directly assist', and that ASIO would take advantage of the powers within 10 days of being enacted (Karp, 2018). However, he also conceded that there was no specific intelligence of an imminent threat (Karp, 2018).

Based on Australia's previous experience in enacting counter-terrorism laws, it is more likely that the government relied on a generalised threat terrorism over the Christmas and New Year period to quicken TOLA's passage through Parliament with minimal scrutiny. With few exceptions, Australia's counter-terrorism laws have been passed on truncated timetables with minimal time for public and parliamentary debate (Hardy & Williams, 2016a; Lynch, 2006). For example, the government's major response to the threat of foreign fighters was a 160-page bill that amended nearly 30 federal acts. An eight-day period was allowed for public consultation and it took one day in each House of Parliament for the laws to be approved (Hardy & Williams,

2016a). Viewed in this context, there is nothing especially unusual about the passage of TOLA through the Australian Parliament, except that the powers have generated controversy amongst a wider global audience.

A strikingly similar example is the passage of counter-terrorism laws through the federal parliament in 2005, following the London bombings in July that year. Lynch (2006) interrogated the Liberal party's claims of urgency surrounding those laws, which were enacted in almost identical circumstances to those surrounding TOLA. The 2005 laws included technical amendments relating to terrorism offences, as well as control orders and preventative detention orders (PDOs), two of Australia's most controversial and rights-infringing responses to terrorism (Burton, McGarrity, & Williams, 2012; Tyulkina & Williams, 2016). The package also included controversial sedition offences, which were widely recognised to undermine freedom of speech (Australian Law Reform Commission, 2006; Nette, 2006). In introducing these laws in parliament, the Prime Minister and Attorney-General claimed there was an urgent need to pass the laws before Christmas – an urgency, Lynch (2006) argued, that 'was of the government's own making'. He reached this conclusion based, among other factors, on the fact that the government knew about the need for the technical amendments for a much longer period, and that the new powers were not used until at least nine months after their passage through Parliament (Lynch, 2006). Confirming his analysis, the control order powers were used only twice and PDOs not at all until nearly a decade later in response to Islamic State (Hurst, 2014; Tyulkina & Williams, 2016).

Other features of the 2005 process directly resemble the passage of TOLA. At that time, too, the support of the Labor opposition was secured after senior members of the Liberal Party government accused them of being soft on national security and 'anti-Australian' (Lynch, 2006). The sedition offences were also widely recognised as being problematic (Nette, 2006) but were agreed to by Labor on the basis that they would be reviewed immediately after enactment by the Australian Law Reform Commission (2006). This is strikingly similar to how the Liberal government secured Labor's support for TOLA, on threats of endangering national security and a vague promise that the laws would be improved following reviews by the PJCIS and INSLM (Seo, 2019). In both cases, Labor MPs were pressured into supporting laws that they recognised as overtly problematic.

Viewed in this light, the passage of TOLA through the Australian Parliament was highly problematic but neither exceptional nor unusual. Rather, it reflects problematic patterns of counter-terrorism lawmaking that have become commonplace in the Australian political landscape. Likely, the passage of TOLA could have been delayed for days, weeks or perhaps even months without any significant impact on national security. The Home Affairs Minister later concluded that TOLA 'played a role, and a very positive role, in a number of investigations' (SBS News, 2019). While the full details of these benefits will never be known, it is hardly the kind of report card that could justify such perfunctory consultation.

That the government's urgency was doubtful is supported by two additional factors. First, discussions about regulating encryption in Australia started at least as early as 2015 (Stilgherrian, 2019), several years before the need to pass TOLA arose apparently in a matter of days. Second, to the extent that information on TOLA usage is currently available, the powers have not been used by law enforcement in relation to any terrorism offences. The only law enforcement notices to date have been issued in relation to cybercrime, homicide, organised crime, telecommunications offences and theft (Department of Home Affairs, 2019). It is possible that the powers have been used by ASIO to gather intelligence on domestic terrorism, but the

numbers in the agency's most recent annual report were redacted (ASIO, 2019).

The final piece of this puzzle, to explain why TOLA was enacted despite its evident problems, is to recognise that Australia lacks enforceable human rights protection. Australia sits alone among democratic nations in having no constitutional or statutory Bill of Rights at the federal level (Williams & Reynolds, 2017). Human rights legislation exists in some states, but there is no mechanism by which the High Court could strike down legislation enacted by the federal parliament on the basis that it infringes privacy or another fundamental right. A government securing the passage of laws speedily through parliament would be aware that the laws could later be struck down by the High Court only on structural grounds, such as infringing the separation of powers (which, incidentally, cannot be at issue with TOLA because the judiciary plays no role in its operation). There are some limited rights in the Australian Constitution, including to trial by jury and an implied freedom of political communication, but nothing that would be of any assistance in a human rights challenge against the encryption laws.

This lack of human rights protection has allowed the enactment of many counter-terrorism laws in Australia that would be constitutionally impermissible elsewhere. These include the possible detention of non-suspects by ASIO for up to a week for coercive questioning (Burton, McGarrity & Williams, 2012), and incommunicado detention for up to two weeks under PDOs to prevent a terrorist attack (Tyulkina & Williams, 2016). Sadly, the encryption laws are simply the latest example in a long line of exceptional counter-terrorism laws passed urgently through the federal parliament, in a constitutional setting that permits rights-infringing legal responses to terrorism.

In particular, the encryption laws compounded extant risks to freedom of speech and freedom of the press. Currently in Australia, freedom of the press remains a topic of significant public debate, with several ongoing prosecutions of high-profile whistleblowers and journalists (Byrne, 2019; Khadem, 2020; Knaus, 2020). The encryption laws exacerbated these risks by enhancing the possibility that journalists' confidential sources could be accessed by law enforcement and intelligence agencies. Prior to the encryption laws, the enactment of Australia's mandatory metadata retention regime, combined with other national security disclosure offences, had generated significant backlash from Australian media organisations (Hardy & Williams, 2015). As a result of those laws, journalists looked to encrypted messaging to protect the identity of their sources (Digital Rights Watch, 2019), but then the encryption laws meant this technique no longer provided a guarantee of security.

The possibility that the encryption laws could be used to identify journalists' confidential sources, combined with the additional disclosure offence found in the encryption laws, has further contributed to a low point for free speech and freedom of the press in Australia. This is a cause of concern not only for journalists who wish to report on the scheme, but also for technology company employees, who may feel compelled to speak out in the public interest if the powers are misused by their employers or government agencies.

# CONCLUSION

TOLA remains a feature of public discourse in Australia, and the issues it raises reflect wider concerns about evolving surveillance technologies, including metadata and facial recognition (Bogle, 2020; Churches & Zalnieriute, 2019). The overwhelming consensus amongst technology companies and human rights organisations, despite the otherwise contrasting motivations of

these groups, is that the laws are highly problematic. The powers are vague and broadly drafted and they lack transparency and judicial oversight. According to many industry experts, the use of the powers will endanger privacy and cyber-security by allowing law enforcement and intelligence agencies to introduce vulnerabilities that can be exploited by malicious actors (Apple, Inc., 2018; Digital Industry Group, 2018). It is clear that the Labor opposition shares many of these concerns, despite allowing the laws to pass (Duckett, 2018b; Worthington & Bogle, 2018). It is also widely acknowledged that the time allowed for parliamentary debate was inadequate, and that more extensive consultation, particularly with smaller Australian companies, was needed (Bogle, 2019).

Civil society and the technology industry will be playing close attention to the upcoming report from the PJCIS and whether the federal government supports the INSLM's recommendations. They should not, however, be optimistic that the government will introduce substantive changes as a result. Once counter-terrorism laws are on the statute books in Australia, it becomes very difficult to wind them back (Ananian-Welsh & Williams, 2014). Some of Australia's most controversial counter-terrorism laws include sunset clauses as expiry dates, reflecting their original intention as an emergency power, but these have been renewed time and again in their original form (McGarrity, Gulati, & Williams, 2012). There is even less reason for the current government to amend the encryption laws, which were written into the statute books as permanent measures. In any case, the current COVID-19 crisis means that the political attention on counter-terrorism laws and the appetite for winding them back will be lower than at other times.

Most likely, some small changes may be made to improve accountability, but the overall shape of the scheme is likely to remain. One small amendment for significant benefit would be to reduce the scope of the disclosure offence, so that it applies only to those who intentionally harm national security or an ongoing law enforcement or intelligence operation. Alternatively, it could include a defence or exemption for DCP employees who reveal information in the public interest. As it stands, DCP employees who reveal any information about a notice face five years in prison (Telecommunications Act, s 317ZF). If some limited information about the use of TOLA notices could be made public, there may be sufficient groundswell of opinion against the laws to force the government's hand. More significant changes, for example to address the lack of judicial oversight, might then have a greater chance of succeeding. In the meantime, such an amendment would reduce the impact of the encryption laws on freedom of speech and protect the ability of media organisations to hold government agencies accountable for any future misuse of the scheme.

During this review process, the Labor party will play a crucial role in opposition. If it bows once more to government pressure for bipartisanship, it will lose further credibility. Bipartisanship on national security matters is important to communicate a message of strength and direction to the general public, but not if it leads to poorly drafted laws that affect the privacy and security of all technology users. By allowing TOLA to sail through Parliament before Christmas, the Labor party missed an important opportunity to communicate to the Australian public that it will hold the government to account. In the absence of constitutional safeguards, protecting Australians' human rights through legislation is crucial: not only to reviews of the encryption laws, but also when regulating any other emerging technologies. The encryption laws are a significant test case for whether the Australian government can strike an appropriate balance between security and human rights when regulating digital platforms. So far, such a balance has not been achieved.

## REFERENCES

Amnesty International. (2020). *Toxic Twitter—The solution* [Report]. Amnesty International. https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-8/

Ananian-Welsh, R., & Williams, G. (2014). The new terrorists: The normalisation and spread of anti-terror laws in Australia. *Melbourne University Law Review*, *38*(2), 362–408. https://law.unimelb.edu.au/__data/assets/pdf_file/0008/1586987/382Ananian-WelshandWilliams2.pdf

Apple, Inc. (2018). *Submission to the Parliamentary Inquiry into the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*. Apple, Inc.

Australia, L. C. (2018). *Submission to the Parliamentary Inquiry into the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*. Law Council of Australia.

Australian Human Rights Commission. (2018). *Submission to the Parliamentary Inquiry into the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*. Australian Human Rights Commission.

Australian Information Industry Association. (2018). *Submission to the Parliamentary Inquiry into the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*. Australian Information Industry Association.

Australian Information Security Association. (2018). *Submission to the Parliamentary Inquiry into the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*. Australian Information Security Association.

Australian Law Reform Commission. (2006). *Fighting words: A review of sedition laws in Australia* (Report No. 104). Australian Law Reform Commission. https://www.alrc.gov.au/publication/fighting-words-a-review-of-sedition-laws-in-australia-alrc-report-104/

Australian Security Intelligence Organisation (ASIO). (2019). *ASIO Annual Report 2018-19*. Australian Security Intelligence Organisation. https://www.asio.gov.au/asio-report-parliament.html

Baker, S. (2019, September 20). How long will unbreakable commercial encryption last? [Blog post]. *Lawfare*. https://www.lawfareblog.com/how-long-will-unbreakable-commercial-encryption-last

Bogle, A. (2018). 'Outlandish' encryption laws leave Australian tech industry angry and confused. *ABC News*. https://www.abc.net.au/news/science/2018-12-07/encryption-bill-australian-technology-industry-fuming-mad/10589962

Bogle, A. (2019). Encryption laws developed after little consultation with Australian tech companies, FOI documents reveal. *ABC News*. https://www.abc.net.au/news/science/2019-07-10/dutton-encryption-laws-australian-tech-sector-not-consulted-foi/11283864

Bogle, A. (2020). Australian Federal Police officers trialled controversial facial recognition tool Clearview AI. *ABC News*. https://www.abc.net.au/news/science/2020-04-14/clearview-ai-facial-recognition-tech-australian-federal-police/12146894

Brandom, R. (2020). The FBI has asked Apple to unlock another shooter's iPhone. *The Verge*. https://www.theverge.com/2020/1/7/21054836/fbi-iphone-unlock-apple-encryption-debate-pensacola-ios-security

Burton, L., McGarrity, N., & Williams, G. (2012). The extraordinary questioning and detention powers of the Australian Security Intelligence Organisation. *Melbourne University Law Review*, *36*(2), 415–469. https://law.unimelb.edu.au/__data/assets/pdf_file/0018/1700172/36_2_3.pdf

Byrne, E. (2019). Afghan Files leak accused David McBride faces ACT Supreme Court for first time. *ABC News*. https://www.abc.net.au/news/2019-06-13/abc-raids-afghan-files-leak-accused-court-canberra/11206682

Cannataci, J. (2018). *Mandate of the Special Rapporteur on the right to privacy (OL AUS 6/2018))*. United Nations Human Rights Special Procedures.

Churches, G., & Zalnieriute, M. (2019, December 10). Unlawful metadata access is easy when we're flogging a dead law. *The Conversation*. https://theconversation.com/unlawful-metadata-access-is-easy-when-were-flogging-a-dead-law-127621

Department Home Affairs. (2019). *Telecommunications (Interception and Access) Act 1979* (Annual Report No. 2018–19). Department of Home Affairs. https://www.homeaffairs.gov.au/nat-security/files/telecommunications-interception-access-act-1979-annual-report-18-19.pdf

Department of Home Affairs. (2018). *Submission to the Parliamentary Inquiry into the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*. Department of Home Affairs.

Digital Industry Group. (2018). *Submission to the Parliamentary Inquiry into the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*. Digital Industry Group.

Digital Rights Watch. (2019, June). *Digital security for journalists*. Digital Rights Watch. https://digitalrightswatch.org.au/2019/06/10/digital-security-for-journalists

Duckett, C. (2018a). *Labor will not back full encryption Bill as it offers interim deal again*.

Duckett, C. (2018b, December 2). Australian government accuses Labor of backing terrorists on encryption-busting Bill. *ZDNet*. https://www.zdnet.com/article/australian-government-accuses-labor-of-backing-terrorists-on-encryption-busting-bill/

Duckett, C. (2018c, December 6). Australia now has encryption-busting laws as Labor capitulates. *ZDNet*. https://www.zdnet.com/article/australia-now-has-encryption-busting-laws-as-labor-capitulates/

Dutton, P. (2018). *Commonwealth, Parliamentary Debates*. House of Representatives.

European Commission. (2017). *Communication from the Commission to the European Parliament, the European Council and the Council: Eleventh progress report towards an effective and genuine Security Union*. European Union. https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-

security/20171018_eleventh_progress_report_towards_an_effective_and_genuine_security_union_en.pdf

Geller, E. (2019, June 27). Trump officials weigh encryption crackdown. *Politico*. https://www.politico.com/story/2019/06/27/trump-officials-weigh-encryption-crackdown-1385306

Graham, R. (2016). How terrorists use encryption. *Combating Terrorism Center Sentinel*, *9*(6), 20–25. https://ctc.usma.edu/how-terrorists-use-encryption/

Hardy, K., & Williams, G. (2015). Special intelligence operations and freedom of the press. *Alternative Law Journal*, *41*(3), 160–164. https://doi.org/10.1177/1037969X1604100304

Hardy, K., & Williams, G. (2016a). Australian legal responses to foreign fighters. *Criminal Law Journal*, *40*(4), 196–212. http://hdl.handle.net/10072/172846

Hardy, K., & Williams, G. (2016b). Executive oversight of intelligence agencies in Australia. In Z. K. Goldman & S. J. Rascoff (Eds.), *Global Intelligence Oversight: Governing Security in the Twenty-First Century*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780190458072.003.0013

Hurst, D. (2014, October 9). Federal police lobby to relax rules on control orders under terrorism laws. *The Guardian*. https://www.theguardian.com/australia-news/2014/oct/10/federal-police-lobbying-to-relax-rules-on-obtaining-control-orders-under-terror-laws

Independent National Security Legislation Monitor. (2020). *Trust but Verify: A Report Concerning the Telecommunications and Other Legislation Amendment (Assistance and Access* [Report]. Australian Government, Independent National Security Legislation Monitor. https://www.inslm.gov.au/sites/default/files/2020-07/INSLM_Review_TOLA_related_matters.pdf

Intelligence, P. J. C., & Security. (2018). *Advisory Report on the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*. Parliamentary Joint Committee on Intelligence and Security (PJCIS).

Karp, P. (2018, November 26). ASIO says it urgently needs powers forcing telcos to help break phone encryption. *The Guardian*. https://www.theguardian.com/australia-news/2018/nov/26/asio-says-it-urgently-needs-powers-forcing-telcos-to-help-break-phone-encryption

Khadem, N. (2020, July 3). Commonwealth dumps 42 charges against ATO whistleblower Richard Boyle but threat of prison looms. *ABC News*. https://www.abc.net.au/news/2020-07-03/charges-against-ato-whistleblower-richard-boyle-dropped-dpp/12419800

Knaus, C. (2020, July 10). Witness K lawyer Bernard Collaery to appeal against secrecy in Timor-Leste bugging trial. *The Guardian*. https://www.theguardian.com/australia-news/2020/jul/10/witness-k-lawyer-bernard-collaery-to-appeal-against-secrecy-in-timor-leste-bugging-trial

Koomen, M. (2019). *The encryption debate in the European Union*. Carnegie Endowment for International Peace.

Lewis, J. A., Zheng, D. E., & Carter, W. A. (2017). *The effect of encryption on lawful access to communications and data*. Center for Strategic and International Studies.

Lynch, A. (2006). Legislating with urgency: The enactment of the Anti-Terrorism Act [No 1] 2005. *Melbourne University Law Review*, *30*(3), 747–781.

McGarrity, N., & Blackbourn, J. (2019). Australia has enacted 82 anti-terror laws since 2001. But tough laws alone can't eliminate terrorism. *The Conversation*.

McGarrity, N., Gulati, R., & Williams, G. (2012). Sunset clauses in Australian anti-terror laws. *Adelaide Law Review*, *33*(2), 307–333.

McGarrity, N., & Hardy, K. (2020). Digital surveillance and access to encrypted communications in Australia. *Common Law World Review*. https://doi.org/10.117/1473779520902478.

Mozilla. (n.d.). *Submission to the Parliamentary Inquiry into the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*. Mozilla.

Nette, A. (2006). A short history of sedition laws in Australia. *Australian Universities Review*, *48*(2), 18–19.

News, S. B. S. (2019). *Dutton says encryption laws help terror cops*.

*Parliamentary Joint Committee on Intelligence and Security (PJCIS)*. (2019). https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security

Seo, B. (2019). Labor attacks 'broken promise' on encryption bill. *Australian Financial Review*.

Smith, L. (2017). Messaging app Telegram centrepiece of IS social media strategy. *BBC Monitoring*.

Stilgherrian. (2019). *The encryption debate in Australia* [Encryption Brief]. Carnegie Endowment for International Peace. https://carnegieendowment.org/2019/05/30/encryption-debate-in-australia-pub-79217

Tillett, A. (2018, November). Encryption laws threaten $3b cyber security industry, tech firms warn. *Australian Financial Review*. https://www.afr.com/politics/encryption-laws-threaten-3b-cyber-security-industry-tech-firm-senatas-warns-20181112-h17shh

Toor, A. (2016, August 24). France and Germany want Europe to crack down on encryption. *The Verge*. https://www.theverge.com/2016/8/24/12621834/france-germany-encryption-terorrism-eu-telegram

Tyulkina, S., & Williams, G. (2016). Preventative detention orders in Australia. *University of New South Wales Law Journal*, *39*(2), 738–755. http://www.unswlawjournal.unsw.edu.au/wp-content/uploads/2017/09/38-2-4.pdf

West, L., & Forcese, C. (2020). Twisted into knots: Canada's challenges in lawful access to encrypted communications. *Common Law World Review*. https://doi.org/10.1177/1473779519891597.

Williams, G., & Reynolds, D. (2017). *A charter of rights for Australia* (4th ed.). NewSouth Press.

Worthington, B., & Bogle, A. (2018). Labor backdown allows federal government to pass controversial encryption laws. *ABC News*. https://mobile.abc.net.au/news/2018-12-06/labor-backdown-federal-government-to-pass-greater-surveillance/10591944?pfmredir=sm