LECA

Law & Economics Consulting Associates

The Economic Impact of Laws that Weaken Encryption

By

George Barker, William Lehr, Mark Loney, and Douglas Sicker

5 April 2021

Contact Personnel: Dr George Barker (LECA)
Email: George.Barker@cleconsult.com

Commissioned by Internet Society

Table of Contents

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

1. Executive Summary[1]

In December 2018, the Parliament of Australia passed the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (better known as TOLA)[2] which expanded government authority and capabilities to circumvent digital data protections. TOLA created a framework by which law enforcement and intelligence agencies, or LEIAs,[3] could request or require information technology providers, or in the terminology of TOLA – Designated Communications Providers (DCPs) – to provide assistance in accessing the content of encrypted data, which may involve sharing of confidential company information or the development of new capabilities.

The focus of this report is to assess the available evidence of the impact of TOLA on the Australian and global economies. Our analysis leads us to conclude that *TOLA has the potential to result in significant economic harm for the Australian economy and produce negative spillovers that will amplify that harm globally*. By significant, we mean economic harms measurable in the multiple *billions of dollars* that are broad-based and likely to be (primarily) realised in coming years.

There are numerous mechanisms by which TOLA may impose economic harms. For example, TOLA increases business uncertainty. Studies completed by the US National Institute of Standards and Technology (NIST) in 2001 and 2018 concluded that government-sponsored interventions that reduced uncertainty about digital security resulted in aggregate benefits worth many billions of dollars.[4] By increasing uncertainty among digital market participants as to the best ways to secure digital information, TOLA may forego the realisation of analogous benefits.

Second, TOLA can harm the brand image of DCPs with operations in Australia that are vulnerable to the threat TOLA poses for the digital security of their products and services. Customers, which includes both enterprise and mass market Internet users, concerned that their data may be rendered less secure due to TOLA may opt to take their business elsewhere. Such responses can reduce DCP revenues and increase DCP operating costs as DCPs adopt work-around strategies to offset the TOLA-related threats. These direct effects need not be limited to DCPs that receive TOLA notices: they may be incurred by DCPs in anticipation of receiving a TOLA notice or by other entities concerned about the impact of TOLA. Those entities need not be limited to DCPs but may include their customers. In aggregate, these direct and indirect effects are likely to be broad-based and accumulate over time as effects ripple through the economy.

---

[1] Acknowledgement: We are grateful to the Internet Society for financial support for this research. The views expressed in this paper however, and any errors, are ours alone.

[2] Otherwise known as the Encryption Act or the Assistance and Access Act, https://www.legislation.gov.au/Details/C2018A00148/Download

[3] LEIA stands for Law Enforcement and Intelligence Agencies, which includes government agencies lawfully empowered to request government access to data.

[4] See NIST (2015, 2018), discussed further below and referenced in Notes 110, 112 *infra*.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

Third, perhaps the single biggest source of adverse economic effects is the indirect threat that TOLA poses for trust in digital services, including the Internet. We are in the midst of a global transition to a digital economy in which eCommerce and networked digital information play an ever-larger role, impacting all countries, all sectors, and all businesses. If the services and networks that support this activity are trusted (e.g., the DCPs), then the economic growth prospects are bright. Reduced trust in data security is expected to depress aggregate demand across the digital economy and induce firms to incur higher costs in attempts to offset the harms resulting from the reduction in trust.[5] Moreover, since digital technology is used throughout the entirety of the economy, these effects are economy-wide and impact all aspects of how modern businesses operate. Consequently, even small threats to cybersecurity, or equivalently, digital trust, have the potential to have large adverse costs. One study shows how threats to digital trust may translate into global harms on the order of a trillion dollars or more.[6] Measuring, attributing, and quantifying such an adverse impact on digital trust to TOLA is not feasible with the available data. Moreover, since these effects will mostly occur in coming years, estimating the impact depends on formulating appropriate forecasts for what would happen with and without TOLA. Any such forecasts will depend on a wide range of modelling assumptions that are likely to be contentious.

Although we can identify multiple vectors through which TOLA's harms may propagate, the evidence does not allow us to provide a more precise quantification of the likely economic harms that TOLA presents. There are multiple reasons for this that are discussed more fully in the report, but those include:

- Estimating the economic impact of TOLA is inherently complex and challenging. TOLA may impose adverse economic impacts both directly and indirectly in multiple ways. Some are easier to trace and estimate than others, but to capture the full effects, it is important not to focus just on what is readily observable;
- To date TOLA use has been limited. Since its passage, multiple reviews and various stakeholders have raised concerns about the potential for TOLA to result in significant economic harms and have called for amendments to reduce that threat. The short time since TOLA's passage and concerns over how best to respond to TOLA opposition may account for the limited empirical evidence of TOLA-attributable costs being incurred; and,
- Access to TOLA-relevant data for use in estimating economic impacts is severely constrained by the lack of transparency and non-disclosure provisions that are part of TOLA. Those data gaps pose a threat to effective oversight, including the ability of analysts attempting to develop theoretically and empirically sound estimates of TOLA impacts.

Moreover, although the focus here is on the potential costs of TOLA, consideration of the potential benefits suggests that they would be even more difficult to estimate. It is

[5] In 2019, 18% of those who distrust the Internet responded that they make fewer online purchases (see https://www.internetsociety.org/wp-content/uploads/2019/06/CIGI-Ipsos-Trust-User-Privacy_Report_2019_EN.pdf).

[6] For example, see the Zurich Insurance Group (2015) study, Note 105 *infra*.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

unclear whether TOLA has improved or will improve LEIA access to digital data and enhance their operational effectiveness. Furthermore, it is generally accepted that one of the most important ways to promote cybersecurity is to promote wider adoption of end-to-end encryption.[7] TOLA poses a challenge to wider adoption of effective end-to-end encryption, since by design, TOLA is about enabling a capability to access the content of encrypted data.

We were surprised to find that there have been no prior, substantial efforts to empirically estimate the economic costs or benefits of TOLA, or of analogous legislation (with economic implications for digital security) in Australia or elsewhere.

Lacking third-party research on which to ground an estimate of the economic impact of TOLA, we conducted primary research in the form of in-depth video-conference interviews with leading multinational DCPs and via an anonymous survey of DCPs, all of which have operations in Australia. As we explain more fully in the report, the empirical data collected is wholly consistent and supports the analysis in the rest of our report. The research of DCP experiences and expectations with TOLA provides empirical support for concluding that:

1. The expectation is that TOLA will have adverse impacts on businesses and their customers that is broad-based (*i.e.*, not just limited to firms in the ICT sectors);
2. Most of the expected harms will be indirect and associated with the threat that TOLA poses for customer and industry partner perceptions of digital trust;
3. Significant uncertainty about TOLA and its effects continues;
4. Direct empirical evidence of economic costs (or benefits) is quite limited, but we attribute that to (a) opacity with which TOLA activities are shrouded due to the non-disclosure provisions; (b) limited time since TOLA's passage and continuing controversy suppressing LEIA use of TOLA authority; and (c) expectation that impacts are most likely to be indirect and in the future;
5. The limited direct evidence we did observe supports the conclusion that company-specific benefits are likely small, while company-specific costs may be quite large; and,
6. The available empirical data does not provide a reliable basis for quantifying the aggregate dollar economic impact of TOLA.

The evidence was also consistent with our expectation that empirical evidence of direct TOLA effects would be sparse and difficult to observe. This lack of empirical evidence, however, is *not* evidence of a lack of an effect. Nevertheless, the limited evidence collected is telling. One respondent that had experienced a direct adverse economic impact estimated the effect as being on the order of one billion (Australian) dollars,[8]

[7] "End-to-End encryption — where the keys needed to unscramble an encrypted communication reside only on the devices communicating — provides the strongest level of security and trust, because by design, only the intended recipient holds the key to decrypt the message" (see https://www.internetsociety.org/resources/doc/2020/fact-sheet-client-side-scanning/)

[8] The adverse outcome was directly attributed to TOLA's harm to the DCP's brand image resulting in losses in current and future sales. See Chapter 6 for a fuller discussion of interview and survey results.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

while the sole respondent that viewed the impact of TOLA mostly favourably saw its principal effect as rationalising existing legislation.[9] Both observations are consistent with the conclusion that company-specific benefits are likely to be small, while company-specific costs may be quite large. Although the empirical research supports the overall conclusion of the report, the size of the sample precludes using this as the basis for a more precise quantification of those harms.

Summing Up

Taken together, this analysis leads us to conclude that *TOLA poses a significant risk of future net economic harms for Australia's economy, with likely adverse spillovers abroad*. The preliminary evidence demonstrates that some firms have already experienced significant economic harms; although it appears likely that most of the aggregate impact of harms is likely to occur in the future and be widespread, if TOLA's threat to encryption continues. Furthermore, the confusion and uncertainty for DCPs caused by TOLA persist and have yet to be adequately addressed.

While the challenges of estimating the economic impact are difficult, there has not been *any* significant public research that attempts to quantify the economic impact of TOLA or similar legislation in Australia or elsewhere. However, the lack of such empirical evidence does not imply that there is no significant impact. Instead, it suggests that the burden of proof should be shifted to evaluating the case for why TOLA is expected to yield significant benefits since the risk of significant harms posed by TOLA is clear.

2. Introduction and Overview

The focus of this report is on providing an assessment of the available evidence of the economic impact of the Australian *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (better known as "TOLA").[10]

TOLA represents major, complex legislation. As we shall explain further below, it amends seven important Acts of the Australian Parliament related to information security, and follows on and contributes to related legislative efforts in a number of other countries like the UK and US. As such, it is expected to have both national (for Australia) and international implications for efforts to secure digital data.

The focus here is on the creation of new government capabilities to circumvent encryption by expanding government authority to request (or require) the assistance of Digital Communications Providers (DCPs) in gaining access to digital data, including

[9] Prior to TOLA, a subset of the DCPs were subject to existing legislation providing government access to digital data. One respondent viewed TOLA as reducing costs by rationalising the firm's exposure to existing legislation. The respondent did not provide an estimate of the cost-savings, but they were not viewed as very large.

[10] For the text of TOLA, see https://www.legislation.gov.au/Details/C2018A00148/Download. TOLA is also sometimes referred to as the "Encryption Act," the "Australian Assistance and Access Act," or the "AAA."

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

data that is encrypted. Under TOLA, DCPs are defined quite broadly to include an expanded array of businesses and activities associated with providing information and computing technology (ICT) products and services.

Chapter 3 provides a brief overview of TOLA's history and legal impact. After an abbreviated and fast process, TOLA was passed in December 2018. Subsequently, TOLA has been subject to multiple reviews, each of which has recommended modifications to the legislation and its application.

Chapter 4 explains the critical role that encryption plays in securing digital data and highlights some of the technical implications of introducing expanded capabilities to circumvent encryption.

Chapter 5 addresses the potential economic impacts of TOLA. The conclusion that emerges from this analysis is that TOLA risks incurring significant future economic costs that are unlikely to be offset by future compensating economic benefits. This conclusion is warranted even though a precise quantification of the net economic impact is not feasible based on the data and research available to date, in part due to the opacity that TOLA creates.

Chapter 6 presents the results of the primary research undertaken as part of this project. This included detailed interviews with leading multinational DCPs and an anonymous survey of DCPs with operations in Australia to assess their experiences and expectations regarding TOLA since its passage in 2018. The survey was similar to two earlier efforts – the first conducted on the eve TOLA's passage, and the second, one year later. While the results of this research are insufficient to provide a reliable empirical basis to quantify the expected impact of TOLA, the results were consistent with and support the conclusion reached in Chapter 5.

Taken together, this analysis leads us to conclude that *TOLA poses a significant risk of future net economic harms for Australia's economy, with likely adverse spillovers abroad*. The preliminary evidence demonstrates that some firms have already experienced significant economic harms; although it appears likely that most of the aggregate impact of harms is likely to occur in the future and be widespread, if TOLA's threat to encryption continues. Furthermore, the confusion and uncertainty for DCPs caused by TOLA persist and have yet to be adequately addressed.

While the challenges of estimating the economic impact are difficult, there has not been *any* significant public research that attempts to quantify the economic impact of TOLA or similar legislation in Australia or elsewhere. However, the lack of such empirical evidence does not imply that there is no significant impact. Rather, this suggests that the burden of proof should be shifted to evaluating the case for why TOLA is expected to yield significant benefits since the risk of broad and significant economic harms posed by TOLA is clear.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

3. TOLA Structure and Background

In the following two sub-sections, we provide a high-level overview of TOLA's legal structure and its history to date. First, we describe how TOLA expands government authority to acquire industry assistance in accessing encrypted digital information. Second, we review the history of TOLA from its recent origins through multiple reviews that are ongoing.

3.1. TOLA structural review

TOLA involves extensive and significant changes to seven important Acts of the Australian Parliament and was introduced in order to "introduce measures to better deal with the challenges posed by ubiquitous encryption" to Law Enforcement and Intelligence Agencies (LEIA).[11] The impacted legislation includes:[12]

1. *Telecommunications Act 1997* (TA1997),[13]
2. *Telecommunications (Interception and Access) Act 1979* (TIA Act),[14]
3. *Surveillance Devices Act 2004* (SD Act),[15]
4. *Crimes Act 1914* (Crimes Act),[16]
5. *Mutual Assistance in Criminal Matters Act 1987* (MACMA),[17]
6. *Australian Security Intelligence Organisation Act 1979* (ASIO Act),[18] and
7. *Customs Act 1901* (Customs Act),[19]

3.1.1. Expansion of Government Authority to Access Encrypted Data

At 228 pages, TOLA is a substantial piece of legislation comprised of five schedules addressing different aspects of government capabilities to obtain lawful access to digital information. The focus of our analysis is on Schedule 1, which introduced new capabilities to request or require industry assistance in accessing encrypted digital

[11] The quote is from the opening paragraph of the Explanatory Memorandum that accompanied TOLA's introduction to Australian Parliament in September 2018. See "Explanatory Memorandum," circulated to the House of Representatives by the Minister for Home Affairs, the Honourable Peter Dutton MP on the introduction of TOLA, September 20, 2018, available at https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22legislation/billhome/r6195%22 (hereafter, Explanatory Memorandum 2018).

[12] See paragraph 1 in Explanatory Memorandum 2018, Note 11 *supra.*

[13] TA1997 available at https://www.legislation.gov.au/Series/C2004A05145.

[14] TIA Act available at https://www.legislation.gov.au/Series/C2004A02124.

[15] SD Act available at https://www.legislation.gov.au/Series/C2004A01387.

[16] Crimes Act available at https://www.legislation.gov.au/Series/C1914A00012.

[17] MACMA available at https://www.legislation.gov.au/Series/C2004A03494.

[18] ASIO Act available at https://www.legislation.gov.au/Series/C2004A02123.

[19] Customs Act available at https://www.legislation.gov.au/Series/C1901A00006.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

information from a "broader range of providers."[20] Thus, the focus here on TOLA's economic impact and on the demand for and use of encryption is warranted.

In short, TOLA allows a select but large number of different LEIA to request or order a Designated Communications Provider (DCP) to provide technological assistance to remove or circumvent encryption using three legal instruments, which collectively we refer to herein as "TOLA notices":[21]

1. Technical Assistance Request **(TAR)** – a request asking a Designated Communications Provider (DCP) to
    1. *Voluntarily* offer help or assistance to a government agency – and/or
    2. *Voluntarily* build capability to help a government agency.
2. Technical Assistance Notice **(TAN)** – similar to a TAR except that it is compulsory, an order rather than a request issued to a DCP, and must be limited to requiring help only, and not requiring to build capability to help.
3. Technical Capability Notice (**TCN**) – again, a compulsory order that requires or mandates that a DCP establish new capability to enable the circumvention of encryption,[22] and can also require the offering of help or assistance.

Each type of TOLA notice is subject to different legal requirements regarding who may issue the notice, the circumstances and due process rules governing the use of the capability, what may be requested or compelled, and the oversight and options for appeal that recipients of TOLA notices have available.

The TOLA notices create new government capabilities to request and require industry (a) to provide assistance; and/or (b) to provide a capability to circumvent encryption. Both types of powers raise concerns, but the threat that a recipient of a TOLA notice might be called upon to create a capability to circumvent encryption has raised the most significant concerns. Once created, such a capability could provide the basis for circumventing the encryption for any digital information to which it may be applied, not just the digital information for the designated target that justified the TOLA request in the first place.[23]

---

[20] See ¶8 and 10 of Explanatory Memorandum 2018, Note 3 *supra.*

[21] TOLA addresses these in its Schedule 1, comprising over half of the length of TOLA, proposes to add a new "Part 15-Industry Assistance" to the TA1997 (see pages 4-109 of TOLA, Note 2, *supra*).

[22] Whereas the "removing one or more forms of electronic protection" (i.e., removing encryption) is included as one of the listed acts or things that a TAR may request or a TAN may require (see s 317E (1)(a) of TOLA, Note 2 *supra*), TOLA excludes requiring a DCP enable the capability to remove encryption for a TCN (see s 317T(4)(c)(i) of TOLA, Note 2 *supra*). Because TCNs may require DCPs to provide a capability to enable other s 317E listed acts, TCNs may result in DCPs being required to provide capabilities that may assist LEIA to circumvent encryption.

[23] For example, a capability once created may provide the basis for circumventing the digital security by others who were not the original target of the TOLA notice. The breaches by those others may be intentional (e.g., malicious actors that are intentionally seeking to acquire access to confidential information) or unintentional (e.g., actors that comprise digital security

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

Without knowing the precise nature of the capability that might be created, it is impossible to know the magnitude of the threat to digital security that such a capability may pose. TOLA sought to address this obvious concern by limiting TOLA requests to those that would not result in the creation of a "systemic vulnerability." That is, that any request for industry assistance or for a capability would be sufficiently narrowly focused to address the particular target(s) of the government authority's lawful warrant interest, without creating a security vulnerability that would impact others who are not the target.[24] As we discuss further below, the effectiveness of this limitation continues to raise concerns.

The types of assistance or capabilities that government agencies may request under TOLA is extensive and complex. These include "removing one or more forms of electronic protection," which includes encryption, but also includes "providing technical information," "facilitating…access to…a facility, customer equipment, a data processing device, a listed carriage service, …, software," etcetera.[25] Although Australian law provided provisions authorising government agencies to request industry assistance in the execution of lawful warrants and in accessing digital data, TOLA significantly expands that authority.[26] Moreover, as noted, the ability to request and require assistance in circumventing encryption is, apparently, new for Australia.[27]

---

through ignorance or carelessness). The point is that once a capability to circumvent encryption is created, restricting its subsequent abuse poses an additional challenge.

[24] TOLA defines a "systemic vulnerability" or "systemic weakness" as a vulnerability or weakness that affects "a whole class of technology" (see pages 12, 84-81 in Tola, Note 2 *supra*).

[25] TOLA s 317E provides a list of the various types of assistance that may be requested (page 18-20 of TOLA, Note 2 *supra*).

[26] For example, Part 14 of the TA1997 Act imposes obligations on carriers and carriage service providers to provide assistance to LEIA "as is reasonably necessary" for "enforcing the criminal law," "assisting in the investigation and prosecution" of crimes and "safeguarding national security" (see pages 322-328 of TA1997IA Act, Note 5 *supra*). Additionally, Chapter 5 of the TIA Act establishes obligations for carriers and carriage service providers to cooperate with LEIAs and provide assistance in implementing lawful interception activities (e.g., wiretaps) (see pages 360-410 of TIA Act, Note 6 *supra*).

[27] We caveat our claim that TOLA's authority to circumvent encryption is "new" because (a) government authority to require industry assistance to gain access to encrypted information existed in the UK since before TOLA and TOLA borrowed from the UK's Investigatory Powers Act of 2016 (see "Investigatory Powers Act 2016," United Kingdom, available at https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted); and (b) numerous recommendations for further amendments to TOLA are being considered, and given the complexity of TOLA and the laws it overlaps with and amends, it is beyond the scope of this report to provide a full legal analysis of TOLA and the extent to which its capabilities are truly novel. Legal scholars may disagree as to the interpretation of both the amendments in TOLA and the extent to which pre-TOLA legislation that is part of the legal framework related to the government's lawful access to information might be interpreted as granting some level of government powers to circumvent encryption.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

It is clear that TOLA extends the power of LEIAs to circumvent encryption, but the precise limits to that power, if any, is unclear.

In addition to expanding the types of industry assistance that may be requested or mandated by government agencies, TOLA also expanded the range of ICT firms to which such obligations apply. That represents a significant change. Prior to TOLA, communication service providers (CSPs) were already accustomed to cooperating with LEIAs in providing lawful access to digital data in a variety of contexts (e.g., providing assistance in the execution of lawful wiretaps). TOLA expands the range of firms subject to legislative requirements to entities classified as Designated Communications Providers (DCPs). A DCP is defined in TOLA as any "person" falling into one of fifteen business categories identified in section 317C[28] and listed in full in the Appendix.

Although some business entities identified as DCPs were already subject to legal obligations to cooperate with LEIAs in obtaining lawful access to digital information, TOLA significantly expanded the scope of ICT firms that could be subject to requests or mandates to provide assistance, and the activities affected. Since many ICT firms are engaged in multiple activities that span multiple categories and the appropriate categorisation of activities into categories may be ambiguous, it is clear that TOLA's reach is broad. What is not clear is which types of ICT firms, if any, or activities are exempt from being recipients of TOLA notices. This broad but uncertain reach of TOLA means that TOLAs potential impact is also quite broad since it includes essentially the entire ICT sector. Additionally, most businesses in non-ICT sectors heavily utilise ICT and have business functions that may qualify as recipients of TOLA notices. Arguably, any company that interacts with its suppliers or customers through a website or an application is a DCP.

The range of LEIAs that may issue TOLA notices is also extensive. It includes agencies responsible for domestic law enforcement, national security, and extra-national law enforcement and security activities (including intelligence gathering).[29] The authority granted to different LEIAs under TOLA is spelled out in varying degrees of specificity. For example, the number of LEIAs that can issue (voluntary) TARs is broader than the number that can issue (compulsory) TANs or TCNs.[30] Many of the proposed amendments to TOLA and concerns raised about TOLA relate to the need for better oversight to help ensure that the new capabilities to access digital data and circumvent encryption are not abused. A number of those amendments take the form of revising the restrictions on who may issue TOLA notices, the circumstances under which TOLA may be issued, the review process before TOLA notices are approved, and sundry other oversight-related measures. A full legal review or assessment of the efficacy of these

[28] Pages 14-18 of TOLA, Note 2 *supra*.

[29] LEIAs that are specifically identified as being able to issue TOLA notices include the Australian Security Intelligence Organisation (ASIO), multiple Interception Agencies (IA) such as various police authorities, the Australian Security Intelligence Service (ASIS), and the Australian Signals Directorate (ASD).

[30] For example, ASIO and IA may issue all three types of notices (subject to different restrictions for different types of notices), but ASIS and ASD may only issue TARs.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

oversight provisions and efforts to limit the scope of TOLA's impact is beyond the scope of this report, but suffice it to say, that a number of significant recommendations for reforms have been made.[31]

In summary, TOLA creates significant new capabilities for a wide array of LEIAs to request or mandate assistance from a broader array of ICT entities to acquire access to confidential digital data and circumvent encryption. Moreover, the nature and limits of these powers are subject to significant uncertainty.

3.1.2. Details about TOLA notices and other important provisions

A key distinction among the different types of TOLA notices is that a recipient's compliance with a TAR is voluntary, whereas compliance with a TAN or TCN is compulsory. This distinction is important because non-compliance with a TAN (a compulsory request for "assistance") or a TCN (a compulsory request for a "capability") renders the recipient subject to sanctions in the form of civil liability, penalties, injunctions, or criminal proceedings. *Because recipients may view a TAR that is refused as a precursor to a TAN or TCN, the distinction between a voluntary versus a compulsory notice may be less important than it at first appears.* To the extent that recipients interpret TAR compliance as not really "voluntary," the incentive to comply will be greater.

In all cases, recipients of TOLA notices are prohibited from disclosing the contents of TOLA notices and the circumstances related to the issuance of a TOLA notice. Unlawful disclosure of TOLA notices, like failure to comply with compulsory notices, can result in legal sanctions. Moreover, reporting on TOLA notices is quite limited, with no disclosure of who received notices and only high-level statistics reported on the number of TOLA notices issued.[32] The disclosure restrictions and the limitations on

[31] For example, as we explain further below in the discussion of the history of TOLA, the INSLM report calls for a major change in the allocation of authority to issue TOLA notices (see Note 40 *infra*).

[32] The record on precisely how many TOLA notices have been issued to date is unclear. The lack of transparency regarding even the number of TOLA notices issued renders any attempt to estimate empirically the economic impact of TOLA extremely difficult, if not wholly infeasible. In addition, the lack of transparency regarding the enterprises (or even their type) that received TOLA notices, what assistance was requested, and how the recipients responded, further complicates the challenge.

Nevertheless, what we believe is the case is that to date, *only voluntary TAR notices have been issued and that the total number of such notices is likely less than 50*. We have seen no reports of TAN or TCN notices being issued. Our estimate of the number of TAR notices is based on what has been reported in two official reports and in speeches. Two reports document that 18 TARs were issued from December 2018 through June 2020, as follows: Australian Criminal Intelligence Commission (ACIC), 1; Australian Federal Police (AFP), 8; New South Wales (NSW) Police, 9 (see Table 45 in DHA (2019), "Telecommunications (Interception and Access) Act 1979 Annual Report 2018-19," Australian Department of Home Affairs (DHA), available at https://www.homeaffairs.gov.au/nat-security/files/telecommunications-interception-access-act-1979-annual-report-18-19.pdf; and

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

reporting on how TOLA is being used make effective oversight challenging and complicate efforts to evaluate the economic impact of TOLA.[33]

Another important provision in TOLA is the guarantee of "safe harbours," protecting DCP recipients of TOLA notices from liability associated with their compliance. Under the prior regime, it was not always clear when industry cooperation in providing access to digital data might render the cooperating party liable for violating other legal security or privacy protections. In addition, TOLA provides for the reimbursement of costs incurred in complying with TOLA notices. Together, the safe harbours and the cost reimbursement provisions have the effect of increasing recipients 'incentives to comply with TOLA notices.

As we explain in subsequent chapters, increasing the likelihood that (unknown) recipients of (unknown) TOLA notices may undertake (unknown) activities that may result in the circumvention of encryption increases the potential breadth of TOLA economic impacts and the (perceived) risk that TOLA weakens digital security.

3.2. TOLA History

The motivation for passage of TOLA derives from the growing concern in Australia and around the world that increased use of encryption poses a threat to the ability of LEIAs to access digital data in the course of their law enforcement and security efforts. From late 2017 the Australian Government moved relatively swiftly to introduce TOLA and provide LEIAs with expanded capabilities to remove or circumvent encryption.[34]

Table 44 in DHA (2020), "Telecommunications (Interception and Access) Act 1979 Annual Report 2019-20," Australian Department of Home Affairs (DHA), available at https://www.homeaffairs.gov.au/nat-security/files/telecommunications-interception-access-act-1979-annual-report-19-20.pdf).

In addition, the Director General of the Australian Security Intelligence Organisation (ASIO) reported to the PJCIS in August 2020 that "we have used the industry assistance powers fewer than twenty times" (see https://www.asio.gov.au/publications/speeches-and-statements/director-general-opening-statement-pjcis-august-2020.html). It is unclear from the speech whether this is an approximate reference to the TARs issued by the specific agencies noted above or whether these "twenty" notices are in addition to those noted in other reports. In any case, whether the number is 18 or 50 (and no data suggests it is higher), government use of TOLA has been quite limited thus far.

[33] Some limitations on disclosure of TOLA notice activity may be justified as needed to protect the efficacy of LEIA actions.

[34] Walker-Munro, Brendan (2019), "A shot in the dark- Australia's proposed encryption laws," Adelaide Law Review 40(3).

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

In July 2017, the government signalled its intention to address the issue.[35] In August 2018, Australia met with the other Five Eyes nations[36] where a joint position was reached.[37] The exposure draft of TOLA was released on 14 August 2018.[38] The Department of Home Affairs (DHA, which was the principal government agency responsible for TOLA) received over 340 submissions. The draft Bill with proposed amendments was introduced into the House of Representatives on 20 September 2018 and referred to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) for inquiry, with a report published in early December 2018. The PJCIS held public hearings from 19 October to 30 November 2018, and also invited further submissions. In total (including confidential and withheld submissions) 105 submissions were received by the PJCIS during its inquiry. Eleven submissions were from government agencies, police or crime commissions in support. There were many more submissions in opposition from representatives of Australia's information technology industry.

In light of the number of submitters that expressed concern about the impact on businesses, particularly small businesses, when complying with industry assistance measures, the PJCIS asked the Department of Home Affairs, whether the Government had prepared a regulatory impact statement on the Bill, and in reply DHA responded that the Government prepared a short form regulatory impact statement which concluded "the regulatory impact of the industry assistance measures will be minimal."[39]

On 22 November 2018, PJCIS received advice from the Minister for Home Affairs that there was an immediate threat and a need to provide agencies with additional powers and to pass the Bill in the last sitting week of 2018. Although the PJCIS did not reach full agreement on all aspects of the TOLA Bill, the Committee tabled an Advisory Report on 5 December 2018[40] which concluded that:

---

[35] Malcom Turnbull, 'Press Conference with Attorney-General and Acting Commissioner of the AFP — Sydney — 14 July 2017' (Press Conference, 14 July 2017, https://www.malcolmturnbull.com.au/media/press-conference-with-attorney-general-and-acting-commissioner-of-the-afp-s).

[36] The Five Eyes Alliance is an intelligence-sharing alliance established under the UKUSA Agreement between Canada, New Zealand, the United Kingdom, the United States of America and Australia. The alliance is designed to facilitate the timely and free sharing of intelligence and national security information.

[37] "Statement of Principles on Access to Evidence and Encryption," Attorney-General's Department, August 2018, available at https://www.ag.gov.au/sites/default/files/2020-03/joint-statement-principles-access-evidence.pdf.

[38] The framing of TOLA borrowed substantially from the UK's Investigatory Powers Act that was passed in 2016 (see "Investigatory Powers Act 2016," United Kingdom, available at https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted).

[39] See page 13, DHS Review of TOLA, Note 3 *supra*.

[40] PJCIS (2018), "Advisory Report on the Telecommunications and Other Legislation (Assistance and Access) Bill 2018," Parliamentary Joint Committee on Intelligence and Security (PJCIS), December 2018, available at

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

> "... there is a genuine and immediate need for agencies to have tools to respond to the challenge of encrypted communications. The absence of these tools results in an escalation of risk and has been hampering agency investigations over several years.... Responding to these escalating risks, the Committee recommends that the Parliament give urgent consideration to the Bill and its immediate passage."[41]

Despite the many submissions and committee reports relating to the proposed amendments, the PJCIS made only modest recommendations. The Bill was amended to clarify certain definitions and inserted provisions for a service provider to be consulted and obtain advice about compliance with a compulsory order to build capability to help LEIAs.[42] Provisions relating to requests and orders for help were also amended to ensure they could not be used to circumvent existing processes for which a warrant was already required. Nevertheless, a number of concerns remained.[43] The Parliamentary Standing Committee for the Scrutiny of Bills also reviewed the Bill.[44] Whilst a full analysis of the Standing Committee's findings is beyond the scope of this report, the Committee raised additional concerns regarding the potential unconstitutional nature of excluding judicial review of TOLA notices under the *Administrative Decisions (Judicial Review) Act 1977*,[45] the blurring of the separation of powers doctrine,[46] as well as incompatibility with the Attorney-General's own policy guidance.[47]

---

https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/TelcoAmendmentBill2018/Report_1.

[41] Biddington, M. (2019), "Telecommunications and Other Legislation Amendment (Miscellaneous Amendments) Bill 2019 – Law and Bills Digest Section," March 27, 2019, available at https://parlinfo.aph.gov.au/parlInfo/download/legislation/billsdgs/6581692/upload_binary/6581692.pdf.

[42] See pages 5-7, PJCIS (2018) Report, Note 12 *supra*.

[43] Such as in the definitions for systemic vulnerability and weakness, target technology, imposition of relevant objectives for the issuance of Part 15 notices as well as a process for State and Territory interception agencies to apply to the AFP Commissioner for such notices.

[44] Parliamentary Standing Committee for the Scrutiny of Bills, Parliament of Australia, *Scrutiny Digest* (Digest No 14 of 2018, 28 November 2018) 23–82, available at https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Scrutiny_of_Bills/Scrutiny_Digest/2018, hereafter Scrutiny Digest 2018.

[45] See Scrutiny Digest 2018, Note 25 *supra*, page 42. The Administrative Decisions (Judicial Review) Act 1977 (Cth) ('ADJR') is available at https://www.legislation.gov.au/Details/C2021C00035/Download.

[46] Where officers of the administrative branch of government could offer civil immunity to designated communications providers to comply with TOLA notices (see Scrutiny Digest 2018, Note 25 *supra*, pages 47, 81).

[47] See Scrutiny Digest 2018, Note 25 *supra*, page 47. For the "A Guide to Framing Commonwealth Offences Infringement Notices and Enforcement Powers," The Attorney-

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

The Bill passed both Houses on 6 December 2018 and received Royal Assent on 8 December 2018 to become part of Australian law. The passage of the legislation from exposure draft to enactment took less than four months and has been described by some as hasty, and the associated consultation process as limited.[48]

The PJCIS requested that the Independent National Security Legislation Monitor (INSLM) commence a review of TOLA on 26 March 2019. This INLSM review was commissioned just before PJCIS completed its own second report on TOLA on 3 April 2019 that recommended (i) that sufficient resources be made available to the INLSM to enable its review; (ii) that the PJCIS be required to produce a third report by June 2020; and (iii) that the Inspector General of Intelligence and Security and the Commonwealth Ombudsman have sufficient resources to ensure that they can properly execute their additional responsibilities under TOLA.[49]

The INSLM provided its report to the PJCIS on 30 June 2020 which made a series of recommendations for amendments to TOLA.[50] The INSLM recommended that the power to issue and authorise TOLA notices be taken away from agency heads and the government and handed to a new judicial oversight body. The INSLM report also called for a new definition of "systemic weakness" and for "systemic vulnerability" to be removed from the bill entirely.[51] Originally, the INSLM report was meant to inform a third PJCIS report which had been scheduled to be delivered to government in June 2020. The PJCIS third report was pushed off to September 2020, but as of March 2021, the PJCIS had not delivered its report.

General's Department, September 2011, available at https://www.ag.gov.au/sites/default/files/2020-03/A%20Guide%20to%20Framing%20Cth%20Offences.pdf.

[48] See Hardy, K. (2020), "Australia's encryption laws: practical need or political strategy?," Internet Policy Review, 9(3), available at: https://policyreview.info/articles/analysis/australias-encryption-laws-practical-need-or-political-strategy; or Miley, V. (2019), "Hastily written tech laws threaten online privacy and security," GreenLeft, available at https://www.greenleft.org.au/content/hastily-written-tech-laws-threaten-online-privacy-and-security.

[49] PJCIS (2019), "Review of the Telecommunications and Other Legislative Amendment (Assistance and Access) Act of 2018," Parliamentary Joint Committee on Intelligence and Security (PJCIS), April 2019, available at https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/ReviewofTOLAAct/Report.

[50] INSLM (2020a), "Trust but Verify: A report concerning the Telecommunications and Other Legislation (Assistance and Access) Act 2018 and related matters," Australian Independent National Security Legislation Monitor (INSLM), July 9, 2020, available at https://www.inslm.gov.au/reviews-reports/telecommunications-and-other-legislation-amendment-act-2018-related-matters; and see INSLM (2020b), "Trust but Verify: Summary of Recommendations," available at https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/AmendmentsTOLAAct2018/Additional_Documents.

[51] See Recommendations 3, 9, and 10 of INSLM (2020a), Note 42 *supra*.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

Thus, two years after passage of TOLA, the Act remains controversial. Part of the controversy may be due to the fact that the Act was drafted and passed in haste, without adequate assessment of the potential or expected impact of the Act. During the first PJCIS inquiry into TOLA prior to its enactment in December 2018, the DHA was asked whether the Government had prepared a regulatory impact statement (RIS)[52] to assess its likely economic impact on business and global competitiveness. The DHA responded by written reply that the Government had prepared only a *short form*[53] regulatory impact statement, which concluded, "the regulatory impact of the industry assistance measures *will be minimal*."[54]

We have been unable to find any substantive evidence that the potential economic impact of TOLA has been considered in any detail. We are unaware of any serious attempt to quantify or even characterise in any detail how TOLA may actually deliver benefits (e.g., in improved national security or law enforcement)[55] or the potential economic harms that TOLA may give rise to if it damages the economic prospects of Australian firms or threatens digital trust.[56]

In subsequent chapters we explain why encryption is critical for promoting digital security, and given the importance of digital information for the Australian and global

---

[52] According to the 2014 Australian Government Guide to Regulation (the Guide) that applied at the time of TOLA's introduction and passage: "*every policy proposal designed to introduce or abolish regulation must now be accompanied by an Australian Government Regulation Impact Statement, or RIS…RIS must have been developed early in the policy making process"* (see page 4, 2014 The Australian Government Guide to Regulation, available at https://apo.org.au/sites/default/files/resource-files/2014-03/apo-nid270966.pdf.

[53] The first step in the preparation of a RIS in 2018 was for the responsible agency to give a written summary known as the Preliminary Assessment to the Office of Best Practice Regulation (OBPR) department of the Prime Minister. So long as the RIS provides enough information to help OBPR understand the nature of the policy issues dealt with, OBPR was required to give a response within 5 working days confirming whether or not a RIS is required and if so what type. There were three types of RIS: Long Form, Standard Form and Short Form. In all cases the agency must undertake a regulatory costing (including offsets) regardless of which type of RIS they opt for (see the Guide, Note 33 *supra*, page 11).

[54] Page 13, "Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 Submission 18 – Supplementary Submission 6: Department of Home Affairs responses to Questions on Notice," Australian Department of Home Affairs, November 2018, available at https://www.aph.gov.au/DocumentStore.ashx?id=13d6d87f-a64e-4e7c-8cc1-83d939e9fe1d&subId=660956 (hereafter, DHS Review of TOLA).

[55] Simply saying that there are crimes (terrorism, human trafficking, etc.) that are heinous and pose a serious threat to national security and safety, while certainly true, is not sufficient to demonstrate an impact assessment for how the actual TOLA law will, in fact, address these and other types of crimes that TOLA may be used to address.

[56] A Freedom of Information Request for a copy of the short form RIS was lodged with the Department of Home Affairs on 1 October 2020. DHA advised on 1 March 2021 that the RIS was an exempt document and would not be released.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

economy, how a threat to encryption poses a risk of significant economic harms. We explore the various mechanisms by which TOLA may threaten digital trust and harm the Australian economy.

4. Technology Considerations

LECA has been engaged to test the hypothesis that legislative and other legal attempts to undermine encryption will have a negative impact on economic considerations such as business, innovation, trade, and inward investment. While this report is an economic analysis, undermining encryption (or as TOLA describes, "removing encryption") involves technology. To that end, this section of the paper considers the technical implications of removing or circumventing encryption and provides a framework for how technological considerations impact economic issues. The goal here is not to provide an in-depth technical analysis, but simply to provide context for the economic analysis.

It is widely recognised that strong encryption is essential for such critical elements of our society such as commerce, liberty, freedom of speech, and national security.[57] Strong encryption could allow criminals to communicate without being observed or understood and LEIAs assert that such encryption hinders their ability to conduct their missions. LEIAs have sought laws that would oblige DCPs that offer encrypted products and services to help to provide unencrypted access to targeted communications based on a warrant or statutory notice. This type of legal third-party access is often referred to as *exceptional access*[58] to encrypted content.

There is strong consensus among technical experts that such interventions, even in the most targeted manner, increase risk and have the adverse impact of eroding trust in the encrypted services.[59] In an analysis of exceptional access methods being discussed in the European Union, leading cybersecurity experts noted that every exceptional access method would introduce vulnerabilities that a third party (e.g., bad actor) could exploit to impact all users.[60] The very possibility of exceptional access could weaken trust and use of encryption and services that rely upon it, such as e-commerce or e-finance.

[57] Internet Society-Chatham House Roundtable on Encryption and Lawful Access, October 2017 https://www.internetsociety.org/resources/doc/2018/internet-society-chatham-house-roundtable-on-encryption-and-lawful-access/

[58] Exceptional access requirements refer to some means of allowing law enforcement the ability to lawfully access the content of encrypted communications and data in an unencrypted form.
See https://www.internetsociety.org/resources/doc/2018/encryption-brief/

[59] Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications https://www.csail.mit.edu/research/keys-under-doormats; and National Academy of Sciences. 'Decrypting the Encryption Debate: A Framework for Decision Makers' (2018) https://www.nap.edu/read/25010

[60] https://www.globalencryption.org/2020/11/breaking-encryption-myths/

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

In the following, we explore specific concerns of allowing access to encrypted data as proposed in TOLA.[61] We first address at a high-level the following questions:

- What is encryption, how is it used, and what is its value?
- How might access to encrypted data be provided and how is this defined in the Act?
- What are the potential technical consequences of TOLA?

To summarise this section, we describe the challenges of creating a targeted intervention on an encryption service and indicate how such interventions could be maliciously applied beyond the target despite best intentions of either the LEIAs or the DCPs. We find that the vague language and broadly applied requirements and obligations in the Act compound concerns over the ability to create a targeted intervention. While it is difficult to quantify the impact associated with any effort that would remove or undermine encryption, we do see increased risk, and potential for decreased trust in these encrypted systems. TOLA could undermine and erode public trust in the many encrypted services we all now use on a daily basis. The mere perceptions of weaker encryption or the threat of government agencies having the ability to gather information undermines trust.

4.1. What is encryption?

There are many definitions of encryption, but a simple and fairly complete one is, "any procedure used in cryptography to convert plaintext into ciphertext to prevent anyone but the intended recipient from reading that data."[62] Of course, in the context of the issue at hand, "text" can mean any type of communication, such as voice, images, characters, video, chat, websites, and more.[63] The intent of encryption is to provide a means to prevent others who might intercept an encrypted communication from understanding its content. An encryption algorithm is used to take plaintext in combination with a "key" to generate a ciphertext. Decryption algorithms employed upon receipt reverse this process to reproduce plaintext, meaning that the intended recipient of an encrypted message must have the key to read that message. We can think of encryption as a system, including many elements working together across the Internet. Encryption is not just the mathematical elements instantiated in software but also a broad set of algorithms and critical functions such as secure key exchange. The

[61] These findings were drawn from analysis of the proposed Act, a review of trade press and academic publications, the comments submitted as part of the public record, as well as interviews with a number of communications providers that offer encrypted services.

[62] NIST SP 800-101 Rev. 1, https://doi.org/10.6028/NIST.SP.800-101r1, under Encryption, visited 11/2020

[63] Security and privacy concerns may also arise associated with the metadata of secure communications, although this content might not be protected through encryption. This includes information about the source and destination of the communications, the applications used, the time that the communications occurred, and more. Many of the same concerns arise for protecting metadata as securing the content of the communications, and as such this information is legally protected and requires a warrant for government agencies to obtain its content.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

assumption is that no one but the sender and the intended recipient should have the keys.[64]

The secrecy afforded by encryption is only as strong as its implementation. Strong encryption could be thought of like a strong bank vault, both of which make gaining access to what is inside impractical, in that it would take too much time, money, resources, and/or expertise to break the encryption just as it would to break into the vault. If an encryption algorithm is weak, then the plaintext could be recovered fairly readily by an interceptor. A weak algorithm is like an unsophisticated lock on the vault, but a strong lock on the vault is useless if you can just cut through the hinges and lift the door off. All the parts of the encryption system must contribute to its strength. With increasingly strong encryption, it becomes very difficult, approaching impossible, to break the encryption. It is also crucial to ensure that private keys are only distributed to their intended recipients, not any other third parties who could use them to access the encrypted data. To take the analogy further, even the strongest of vaults will open if you gain access to the keys.

It is also worth mentioning that encryption can be implemented at a variety of points in the network and by a variety of entities. In fact, it is now trivial for users to implement their own strong end-to-end encrypted services without making use of a commercial service. As we will discuss, this has implications for LEIAs.

4.2. How is encryption used, and what is its value?

Encryption has a great variety of applications. Primarily it is used to protect (i.e., keep confidential and free from tampering) data that is being stored ("data at rest") or being transmitted ("data in motion"); of course, users want their data protected both while in transit and at rest. Encryption has a broad range of uses, with examples including: protection of financial transactions and healthcare records, secure storage of files, disk encryption, device locking, credential verification to access virtual private networks, secure web browsing, private or anonymous messaging, cloud security, and more.[65] By providing these protections, encryption plays an important role in enabling critical parts of our economy, by ensuring trust in e-commerce, e-finance, e-health, e-learning, secure information storage, and secure private communications, and by assuring our civil liberties, such as privacy, freedom of speech, and freedom of association.

While some research (as described in the economics section of this paper) has tried to assign a monetary value to encryption, it is a difficult task given the manner in which encryption is woven into our modern existence, the countless ways upon which we rely on it in our daily lives, and the innumerable second and third order effects that

[64] The details on key exchange, symmetric and asymmetric cryptography, and related issues, while important, are beyond the scope of this report. For a more detailed treatment of the subject of encryption, see < https://www.internetsociety.org/issues/encryption/>

[65] National Academy of Sciences. 'Decrypting the Encryption Debate: A Framework for Decision Makers' (2018) https://www.nap.edu/read/25010

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

encryption now plays in our lives.[66] As described earlier, encryption provides the very foundation for trust on the Internet, and it is this trust that has enabled the tremendous growth of communications, commerce, financial, and health services across the network and the globe. During the COVID-19 pandemic, encryption has enabled the flexibility for working from home for many businesses – allowing commerce to continue despite COVID restrictions and the practical realities of a pandemic.

The value of encryption is in securing these services and providing a basis for trust. Without strong encryption, this trust does not exist, and that lack of trust harms the aforementioned services. Trust via encryption is the underpinning for all of these activities on the Internet, and without it, individuals and entities may not be willing to engage in these activities online. Indeed, as our society continues to shift to more of an information and data economy, more encryption is needed, not less, and undermining its strength takes us in the wrong direction.

As Apple has pointed out, "Every day, over a trillion transactions occur safely over the internet as a result of encrypted communications."[67] It is well accepted that the best way to promote cybersecurity is to promote wider adoption of strong end-to-end digital encryption.[68]

---

[66] See the discussion in the economic section of this paper. Estimates on investment in cyber security are in the hundreds of billion USD. See, Leech, D. and John Scott (2018), "The Economic Impacts of the Advanced Encryption Standard, 1996-2017," prepared for the National Institute of Standards and Technology, NIST GCR 18-017, available at https://doi.org/10.6028/NIST.GCR.18-017; published as journal article: Leech, D. P., Ferris, S., & Scott, J. T. (2019). The Economic Impacts of the Advanced Encryption Standard, 1996–2017. Annals of Science and Technology Policy, 3(2), 142-257. doi:10.1561/110.00000.

[67] Page 1, "Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 Submission 53," Apple, Inc., available ast https://www.aph.gov.au/DocumentStore.ashx?id=ecd6be12-ab84-43de-be61-1599e1db2a74&subId=661073.

[68] There are numerous authoritative statements on the value of cybersecurity from policymakers in nations across the globe. For example:

- Attorney General William Barr implicitly acknowledged that there was no way to provide government access to encrypted data without creating vulnerabilities that malicious actors can exploit, arguing that the risk was "acceptable because 'we are talking about consumer products and services such as messaging, smart phones, e-mail, and voice and data applications, not talking about protecting the nation's nuclear launch codes" (see "US Attorney general William Barr says Americans should accept security risks of encryption backdoors," TechCrunch, July 23, 2019, available at https://techcrunch.com/2019/07/23/william-barr-consumers-security-risks-backdoors/?guccounter=1);
- Ash Carter, the former US Secretary of Defense, argued that "there's no point in my buying all these planes and ships and tanks and having soldiers, sailors, airmen and Marines if I can't connect them… so data security is an absolute necessity for us… so we're foursquare behind strong data security, including strong encryption… no question about it" (see Remarks of Secretary Carter in a 'Fireside' Chat with Ted Schlein in San Francisco," transcript, US Department of Defense, March 2, 2016,

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

4.3. How might exceptional access be provided?

The same features of encryption that make it a critical part of the Internet can be used by criminals to hide illegal activities across a broad set of technologies and applications. This impedes the ability of LEIAs to easily intercept and view the content of communications of a target of an investigation. Exceptional access seeks to provide a way for LEIAs to gain plaintext access to the content of encrypted communications.

At a high level, we can think of exceptional access as:

- removing encryption or authentication
- introducing weaknesses or vulnerabilities
- or introducing hardware or software to provide access to decrypted content

This could be enabled through such approaches as key escrow; altering key management; adding a weakness or vulnerability to the cryptography, methods,

available at https://www.defense.gov/Newsroom/Transcripts/Transcript/Article/684858/remarks-by-secretary-carter-in-a-fireside-chat-with-ted-schlein-in-san-francisc/;

- Robert Hannigan, former Director of the **United Kingdom's** GCHQ: "Encryption is an overwhelmingly good thing—it keeps us all safe and secure … Building in back doors is a threat to everybody and it's not a good idea to weaken security for everybody to tackle a minority" (see "UK's ex-spy chief warns Amber Rudd's plan to pass new smartphone encryption law is dangerous," The Independent, July 10, 2017, available at https://www.independent.co.uk/news/uk/politics/uk-ex-spy-chief-amber-rudd-home-secretary-smartphone-encryption-law-dangerous-terrorism-isis-whatsapp-a7833211.html;
- The Canadian House of Commons' Standing Committee on Public Safety and National Security concluded its 2019 report on "Cybersecurity in the financial sector as a national security issue" by agreeing that "it is important, for reasons of security and privacy, that every Canadian have access to strong encryption" and recommending that the Government of Canada "reject approaches to lawful access that would weaken cybersecurity" (see "Cybersecurity in the Financial Sector as a National Security Issue," Canadian House of Commons, June 2019, available at https://www.ourcommons.ca/Content/Committee/421/SECU/Reports/RP10589448/securp38/securp38-e.pdf); and,
- According to the European Commission, "strong encryption is the basis for secure digital identification systems that play a key role in effective cybersecurity; it also keeps people's intellectual property secure and enables protecting fundamental rights such as freedom of expression and the protection of personal data, and ensures safe online commerce" (see pages 9-10 in "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU," European Commission, Brussels, September 13, 2017, available at https://ec.europa.eu/transparency/regdoc/rep/10101/2017/EN/JOIN-2017-450-F1-EN-MAIN-PART-1.PDF).

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

protocols, or implementations of an encryption service; or simply turning off encryption.[69]

In Australia, TOLA allows LEIAs to impose legal obligations on DCPs requiring them to assist in providing LEIAs access to encrypted services and their data. What TOLA does not say is how this access might be provided. We will not attempt to exhaustively discuss technical approaches to providing access to encrypted data (this is beyond the scope of this report); rather, we simply consider and discuss high-level technical implications of TOLA.[70]

Key escrow, where an additional set of decryption keys are held by a "trusted" third party, in "escrow," who would provide them to LEIAs when legally appropriate, provides one type of access for authorised third parties (i.e., law enforcement and intelligence agencies); however, because of concerns about who could get access to these keys (e.g., they can be stolen, mishandled, lost, or shared) and because key-escrow approaches do not require TOLA, we do not discuss this approach further here other than to note that the technical community has been and remains opposed to this approach.[71]

[69] The technical means to provide access to encrypted content could include a broad range of approaches (some beyond the scope of TOLA), such as: taking advantage of discovered vulnerabilities; introducing vulnerabilities; broader attacks with tools such as keyloggers or snooping tools; removing security controls from a specific system, software, or device; disabling or downgrading encryption services; interrupting encryption sessions between the browser and the server; key exchange; key escrow; or other possible approaches. Again, a more extensive discussion is beyond the scope of this paper.

[70] Australia already has existing laws providing lawful access to data that would provide law enforcement and intelligence agencies a legal path to obtain encrypted data from a broad number of service providers. As noted in the legal chapter, TOLA appears to extend existing law to the extent it explicitly mentions the removal of encryption and extends this power to DCPs that are not carriers, carriage service providers, and facility and telecommunications network operators; and services that are not strictly telecommunications services, many of which were already (prior to TOLA) subject to extensive National Intelligence Community legislation. Prior legislation includes the *Telecommunications (Interception and Access) Act 1979* (TIA) and later relevant legislation that followed the 9/11 terrorist attacks in 2001, since which time the Australian Parliament has passed more than 124 Acts amending the National Intelligence Community's legislative framework.

[71] See Abelson, H., R. Anderson, S. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, M. Green, S. Landau, P. Neumann, R. Rivest, J. Schiller, B. Schneier, M. Specter, and D. Weitzner (2015), "Keys under doormats: mandating insecurity by requiring government access to all data and communications," Journal of Cybersecurity, 1(1), pp.69-79; and for extended working paper version, see Technical Report (MIT-CSAIL-TR-2015-026), July 6. 2015, available at https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

Another way to implement such access is to incorporate a "backdoor"[72] weakness or vulnerability in an underlying encryption mechanism or related software. The problem here is that, by design, this process adds weakness or vulnerability, and the consequence of such manipulation undermines encryption. Adding weaknesses also simply runs contrary to the rigorously applied norm of building and assessing the strong encryption, as well as the process of discovering, notifying and patching such weaknesses. Not only does it weaken the actual implementation of the encryption, it also erodes trust in the concept of encryption as a tool that underpins so much of what we do as a society online.[73]

4.4. How such access is defined?

As we will discuss, the current language in TOLA leaves a number of questions and concerns about implementation. While it is not uncommon for aspects of legislative language to be intentionally broad in scope and application, the one clear message that we heard from all of the companies that we interviewed is that they simply don't know what to expect. We outline the lack of clarity and consider its consequences.

One of the first things one notices when reading TOLA is that it says more about what a notice cannot require than it does about what it can require. Not surprisingly, this approach is one way of narrowing the scope in a manner that makes it more acceptable and more difficult to disagree with. However, in reading this language it becomes difficult to grasp the meaning and leaves the ordinary reader uncertain of definitions and obligations.

For example, TOLA provides that a "designated communications provider must not be requested or required to implement or build a systemic weakness or systemic vulnerability etc." It further states that notices must not have the effect of "(a) requesting or requiring a designated communications provider to implement or build a systemic weakness, or a systemic vulnerability, into a form of electronic protection; or (b) preventing a designated communications provider from rectifying a systemic weakness, or a systemic vulnerability, in a form of electronic protection." It goes on to state that notices cannot require a provider to "implement or build a new decryption capability," or "render systemic methods of authentication or encryption less effective," or introduce a "selective" vulnerability or weakness that would "jeopardise the security of any information held by any other person," or create "a material risk that otherwise secure information can be accessed by an unauthorised third party."[74]

[72] As mentioned earlier, one method of gaining alternative access to the content of encrypted communications is referred to as a "backdoor," just as a backdoor allows one alternative access to a building. Of course, most of us would not want a backdoor with a known weakness on our home (i.e., weakened security), and most of us would not want to provide door keys to the government (i.e., key escrow).

[73] As an example, see the Juniper backdoor of the DUAL-EC-DRBG random number generator: https://dl.acm.org/doi/pdf/10.1145/2976749.2978395.

[74] For these and prior quotes in this paragraph, see pages 84-85 of TOLA, Note 2 *supra*.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

The following definitions were added to the legislation:[75]

> *systemic vulnerability* 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* 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.

While these definitions attempt to reduce the risk to non-targeted users, there is still a lack of clarity, and there are implications for possible consequences. Clarifying what is meant by a targeted technology is a first step. It would also be useful to understand how vulnerabilities selectively introduced to targeted technologies could not be used more generally at the systemic level, a point which has been noted by technical experts as an inherent problem with this approach.[76] The approach taken to implement a targeted vulnerability (or possibly the actual implementation) has a high likelihood to leak or be discovered and exploited by others. At that point, it might be applied to one or many other targets.

While some basic methods exist to provide access to such things as mobile voice communications and certain locked devices, many current Internet services make use of strong end-to-end encryption, which could limit the ability of the service provider to assist in providing exceptional access (this is recognised by TOLA).[77] Furthermore, it is now trivial to implement or obtain a strong end-to-end communications service without the help of a service provider, so the service provider would not have the ability to reveal the content if requested to do so by LEIAs.

Indeed, open-source software can be downloaded and implemented for just this type of function, making it increasingly difficult to introduce a vulnerability without detection. It is possible that no provider (including the creator of the open-source software – assuming that TOLA can even legally reach that provider) is able to provide government agencies with the information they seek from such access.[78] The point is that it is not practically possible to stop people from using strong end-to-end encryption if they are motivated to do so. It is unrealistic to expect encryption algorithms to be un-

[75] Page 12 of TOLA, Note 2 *supra*.

[76] See https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/ on EternalBlue.

[77] Companies that offer services that terminate one end of the encrypted channel present a lower bar for intercepting communications. They have access to the unencrypted content. In such cases, responding to the back-door request should impose minimal direct costs.

[78] For example, bad actors who know that they are the potential targets of law enforcement or intelligence agencies may be more likely to employ additional layers of widely available security protection, which would render the access supported by TOLA ineffective.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

invented or un-published, just as it is unreasonable to expect open-source encryption software to be abolished.

4.5. What are the consequences of TOLA?

Numerous technical, economic, and business studies have discussed the concerns of providing exceptional access to encryption.[79] These range from indicating the ways that encryption would be weakened, to the issues presented by eroding trust, to the wider concerns of a fractured Internet. Exceptional access has repeatedly been met with strong resistance by technical experts over the last three decades, and recent efforts supporting exceptional access have not shown a path that overcomes the technical concerns; this includes the approach proposed in TOLA. In this section, we try to provide perspective on the challenges and consequences of exceptional access, and more specifically the difficulties the implementation of TOLA presents. In the remainder of this section, we consider issues around: weakening encryption; unclear targeting; developing and retaining methods; reuse; escalation; leaking and sharing; and uncertain process and obligations.

Weakening encryption

TOLA states that a "communications provider cannot be requested to: build or implement a systemic weakness or systemic vulnerability into a form of electronic protection; or prevent a designated communications provider from rectifying a systemic weakness or a systemic vulnerability in a form of electronic protection."[80] Here, legislators were taking steps to prevent creation of systemic vulnerabilities. However, not requesting a provider to build or implement a systemic weakness or systemic vulnerability does not prevent them from doing so.

Rather than saying that the designated communications provider will not be prevented from rectifying a weakness or vulnerability, the language should state that the

[79] National Academy of Sciences (2018), "Decrypting the Encryption Debate: A Framework for Decision Makers," available at https://www.nap.edu/read/25010; Bellovin, S., M. Blaze, D. Boneh, S. Landau, and R. Rivest (2018), "Analysis of the CLEAR Protocol per the National Academies Framework," CUCS-003-18, May 10, 2018, available at https://mice.cs.columbia.edu/getTechreport.php?techreportID=1637; Bellovin, S., M. Blaze, S. Clark, and S. Landau (2014), "Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet," Northwestern Journal of Technology and Intellectual Property, Vol. 12, Issue 1; Abelson, H., R. Anderson, S. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, M. Green, S. Landau, P. Neumann, and R. Rivest (2015), "Keys under doormats: mandating insecurity by requiring government access to all data and communications," Journal of Cybersecurity, 1(1), pp. 69-79, available at https://academic.oup.com/cybersecurity/article-pdf/1/1/69/7002861/tyv009.pdf and technical report MIT-CSAIL-TR-2015-026 (July 6. 2015) at https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf; Ali, M. (2016), "Backdoor Government Decryption Hurts My Business and Yours," Harvard Business Review, September 15, 2016, available at https://hbr.org/2016/09/backdoor-government-decryption-hurts-my-business-and-yours.

[80] Pages XX TOLA, Note 2 *supra*.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

designated communications provider is obligated[81] to follow industry best practice with regard to the prompt rectification of known vulnerabilities and weaknesses.

The risk is that TOLA may create incentives for companies to keep (i.e., fail to disclose) known vulnerabilities. To do so leaves the wider public at greater risk; there is an over-riding public interest in vulnerabilities being reported, fixed and patched as promptly as possible, especially to reduce the risk and impact of "zero day" attacks.

Similarly, some techniques such as client-side scanning and the UK's "ghost proposal" are often presented by their proponents as using existing capabilities, rather than introducing new weaknesses or vulnerabilities.[82] These techniques do, in fact, introduce new vulnerabilities. For example, the ghost proposal provides a mechanism to effectively circumvent the encryption process by allowing a third party to join a session without the intended participants being aware. Since this mechanism is something a DCP can replicate across the entire user base, it effectively becomes a broadly applicable process.

Unclear targeting
While limiting the request/notice to a specific target in order to limit the exposure is the right approach, it remains unclear how targeting could be accomplished without potentially exposing non-targeted users. It would appear to be the responsibility of the DCP to make that decision, and it is not guaranteed that they will do this correctly. It is also unclear how a DCP will implement the targeted removal or circumvention of encryption (whether updates may be required and how those are targeted and not leaked). This raises the question, where in a system is the exceptional access method implemented and how is it delivered?

Developing and retaining methods
While TOLA tries to safeguard strong encryption by stating that providers must not be requested or required to implement systemic vulnerabilities and weaknesses, it does not preclude them from doing so. While one might argue that a company is not disposed or inclined to implement such systemic vulnerabilities, a prohibition on it would allow for higher consumer trust in encryption. Given that TOLA does allow for certain LEIAs to request or require the implementation of selective vulnerabilities or weaknesses, how is such a vulnerability controlled, and what is the process to prevent future instantiations of this vulnerability?

Reuse

[81] There is always a chance of a vulnerability but liability with respect to vulnerabilities unknown to the provider depends on how the standard for fiduciary duty or due diligence responsibility is assigned, but presumably, typically it would not constitute unlimited liability.

[82] See Callas, J. (2019), "The 'Ghost User,' Ploy to Break Encryption Won't Work," ACLU Blog Post, July 23, 2019, available at https://www.aclu.org/blog/privacy-technology/ghost-user-ploy-break-encryption-wont-work. For background on the Ghost proposal that was first advanced in the UK, see Levy, I. and C. Robinson (2018), "Principles for a more informed exceptional access debate," LawFare Blog, November 29, 2018, available at https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

While limiting obligations to creating only targeted vulnerabilities or weaknesses may seem to be the right direction in principle, in reality the mere act of creating the exceptional access mechanism, no matter how targeted, opens up the system to misuse and bad actors much more broadly. A specific intervention could lead to unintended uses, which are not part of the TOLA Request or Notice, creating a broadly applicable backdoor.

In addition, creating an intervention means that a route in is now known. Knowledge of the method (or worse, software tools or an implementation) could cause unintentional or knowing release to unauthorized others. Uncertainty about who may have been asked to create an exceptional access intervention decreases trust across the value-chain.

Escalation

A fundamental challenge in obligating providers to create targeted access is that there is no guarantee that these won't be applied more broadly to become partially or fully systemic. In developing a systemic attack on a system, the first step is often to define a narrow attack and then determine how to apply it more broadly. Thus, requiring providers to attempt to create targeted interventions is a first step towards creating systemic vulnerabilities. Furthermore, a targeted intervention, if needed more frequently, would likely be made easier to use and more automated, and therefore begin to approach a systemic intervention.

A targeted intervention is more likely to become systemic once knowledge of the weakness is discovered, created, or shared. Even the possibility that it might exist, might also encourage bad actors to hunt for it. A targeted vulnerability or weakness can be escalated into a systemic vulnerability simply by replicating or amplifying the vulnerability across a user base (through updates, viruses, or other methods).

Leaking and sharing

Targeted interventions might be leaked and become available to a broader community, including bad actors who could use these to compromise the public.[83] Additionally, "discovered" vulnerabilities might not be patched, but retained. Once interventions are known, it is imperative that the provider works through the well-established notification and patching processes in security communities, yet TOLA does not require providers to do so. It is reasonable to say that once a vulnerability or weakness is introduced, it is only a matter of time until it is discovered, shared, leaked, stolen, or reverse engineered.

Uncertain process and obligations

Under TOLA, DCPs may be asked to retain inadvertent vulnerabilities in their systems for future use, which may create uncertainty for those providers as to when and how they should participate in vulnerability disclosure. Clear vulnerability disclosure sends a strong signal that robust encryption will be maintained, increasing trust by users –

[83] In their CALEA II paper, ISOC pointed out how such leaks might occur. https://cdt.org/wp-content/uploads/pdfs/CALEAII-techreport.pdf. And see https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/ on EternalBlue.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

both commercial entities and individual end users. There is also uncertainty around what a TOLA Request or Notice might require a company to do; more specifically, to what lengths providers are obliged to aid in the process of intercepting or decrypting communications. The uncertainty around TOLA means that companies are not sure what methods would be required to fulfil a TOLA Request or Notice, and this means security officers within the company must struggle when facing decisions about the adoption of technology, the hiring of security employees, and even the consequence of partnering with other companies or sharing data. This is an area that would benefit from a thoughtful, tailored, and transparent approach.

By design, it is hard (or at least should be hard)[84] to break strong encryption, and it is not clear how each DCP will deal with an access request. This assertion of a lack of clarity is based on discussions that LECA has had with a variety of major DCPs. Based on our interviews, companies are not sure of their obligations and unclear what methods would be required to fulfil a TOLA Request or Notice.

Furthermore, different parts of the ecosystem (i.e., different DCPs) will need to take different approaches to remove or circumvent encryption. We found in our interviews that different classes of providers have different perspectives on how challenging or detrimental it might be to remove or circumvent encryption. We found that traditional carriers (i.e., former telephone service providers) have a less critical view of implementing TOLA requests than we found when talking to web service, application, and other Internet service providers.

To summarise, TOLA could undermine and erode public trust in the many encrypted services we all now use on a daily basis. The mere perceptions of weaker encryption or the threat of government agencies having the ability to gather information undermines trust across entire systems.

Consumers, be they commercial entities or private individuals, may shy away from conducting business in a weakened trust environment. Companies will also face decisions about whether they want to face the legal, operational and logistical difficulties that might come with doing business in Australia (this point was raised by several major companies during our interviews). Numerous technology companies based in Australia have voiced their concerns over TOLA.

For example, in 2020, Patrick Zhang, Atlassian Head of Policy and Government Affairs, stated that, "The continued viability and growth of technology innovation and manufacturing in Australia will in large part be based on the actual and perceived security of the technologies that underpin the digital economy and its ecosystem."[85] These claims of harm are not just speculative. Vault Systems, an Australian cloud

[84] The use of methods such as Ghosting allows for a third party to silently be added to a secure session, and one could argue that this is not hard to do, and so we add this qualification.

[85] "Encryption laws damage potential: Atlassian," InnovationAus, 24 June 2020, available at https://www.innovationaus.com/encryption-laws-damage-potential-atlassian/.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

services provider stated that it is being, "materially and detrimentally impacted" by TOLA.[86]

Accordingly, it might be easier to simply locate services in another country to avoid the myriad of challenges and economic uncertainty: The Internet Architecture Board stated, "This risk might cause some infrastructure providers to relocate, reduce service, or even block service to Australian users. Such fragmentation of the Internet is one of the primary concerns we have today as it reduces the value of a global, highly-connected Internet."[87]

[86] "Huge scope of Australia's new national security law reveals itself," ZDNet, 6 June 2019, available at https://www.zdnet.com/article/huge-scope-of-australias-new-national-security-laws-reveals-itself/) and "Encryption laws are creating an exodus of data from Australia: Vault," ZDNet, 5 July 2019, available at https://www.zdnet.com/article/encryption-laws-are-creating-an-exodus-of-data-from-australia-vault/.

[87] Internet Architecture Board (IAB) Comments on the Australian Assistance and Access Bill, 9 September, 2018, available at https://www.iab.org/wp-content/IAB-uploads/2018/09/IAB-Comments-on-Australian-Assistance-and-Access-Bill-2018.pdf.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

5. Economic Framework

The principal goal of this research effort is to evaluate all evidence available on the economic impact of TOLA. One might have expected that such an effort would have been undertaken prior to the passage of TOLA, but as we have explained that did not happen. Somewhat more surprising for us is the observation that there are *no* studies estimating the economic impact of TOLA-like legislation that we could find anywhere, either through our review of the published literature or in the course of our primary research involving in-depth interviews with large multinational DCPs (discussed further in Chapter 6). While supporters and critics of TOLA-like regulations have contributed to a large body of academic literature and submitted comments in the TOLA proceedings (as already noted) and in similar proceedings associated with other legislation, such as the UK's Investigatory Powers Bill (2016),[88] in all of this material, there is a noted dearth of attempts to quantify either the economic costs or benefits that might be expected.

In an ideal world, one look to a study that identified all of the potential costs and benefits, translated those into monetary terms, and then aggregated them to arrive at an estimate of the net economic benefits that TOLA is expected to produce. If one had such an estimate, it could help inform an assessment of whether TOLA's net benefits are likely to exceed its net costs. Of course, a monetary estimate of aggregate net economic impact alone would not be all that policymakers would consider in order to evaluate the impact of TOLA. Some impacts are inherently difficult to translate into monetary terms (e.g., national security and the prevention or prosecution of crime); and the distribution of economic effects is also an important consideration (both with respect to the allocation of costs and benefits, and how those are realised over time).

We do not live in an ideal world, and this report cannot produce a quantitative monetary estimate of the impact of TOLA. Instead, we examine qualitatively the different mechanisms by which TOLA may result in economic effects. This analysis readily identifies many mechanisms by which TOLA can produce both direct and indirect costs for DCPs, other enterprises, and consumers across the economy. Relevant costs are not limited to the direct costs to DCPs that may receive TOLA notices, or even just to the indirect costs to firms in the ICT sector, but rather include indirect costs to other firms and consumers more widely. Moreover, the costs are expected to accumulate over time as the new government authority created by TOLA is utilised.

Our analysis leads us to conclude that TOLA has the potential to result in significant economic harm for the Australian economy, and produce negative spillovers that will amplify that harm globally.

We explain why quantifying the cost and benefit components would be challenging even if better data were available, while noting the almost complete lack of relevant data. Moreover, we explain why quantifying, at least partially, the costs that TOLA is likely to cause is inherently a more tractable challenge than quantifying the benefits that TOLA might deliver.

[88] See Note 27 *supra*.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

Our analysis leads us to conclude that the most significant potential source of TOLA-related costs is associated with the threat that TOLA poses to online trust. As we explain, even a small impact on trust can lead to broadly distributed economic harms resulting in adverse economic impacts in the billions of dollars. Compared with those indirect costs which will accumulate over time, the direct costs incurred by firms whose individual business prospects may be harmed by TOLA are likely to be far smaller in aggregate, but still significant for the impacted firms and in aggregate monetary terms. For example, one of the multinationals we interviewed recounted how TOLA had already resulted in the firm losing upwards of one billion AUS$ in revenue as a consequence of TOLA, and several of the respondents to our survey reported having incurred double-digit percentage revenue losses already. Unfortunately, these individual data points do not provide a reliable basis for deriving an economy-wide estimate of aggregate costs.

5.1. Framework for understanding TOLA economic impacts

The appropriate framework to make such an assessment is to compare what happened (or is likely to happen) in the world in which TOLA is adopted to a hypothetical "but-for" world in which TOLA is not adopted.[89] This raises many complex theoretical and empirical challenges for multiple reasons, including the need to scope the effort by addressing the following questions:

1. What economic impacts are to be considered?
2. Should the focus be on Australian or global impacts?
3. How to balance the focus on TOLA costs versus benefits?
4. Is the analysis of impacts long-term or short-term?
5. How is the "but-for" world characterised?
6. How to collect data on TOLA impacts?

Each of these challenges are addressed in the following sub-sections.

5.1.1. What economic impacts are to be considered?

Assessing the economic impact of legislation depends on being able to assess how firms and consumers impacted by TOLA either directly or indirectly will change their behaviour as a result of TOLA, which is challenging because behaviour depends on expectations. Ideally, we would like to quantify the measurable impacts on total surplus, which is the sum of producer and consumer surplus in monetary ($AUS) terms. The monetary effects of TOLA on producer and consumer surplus are not directly observable and must be estimated from collections of monetary and other outcome-

[89] Note, the prospect of TOLA's adoption is likely to have impacted behaviour and outcomes even prior to its adoption in December 2018. Moreover, continuing uncertainty about future regulatory or legislative reforms and disagreements regarding the legal interpretation of TOLA and how it is or will be used contribute to distorting the challenge of identifying a clear before/after, with-TOLA/without-TOLA comparison set for assessing economic impacts. As we will discuss further below, one reason we may fail to observe measurable impacts on behaviour due to TOLA is because it is not yet fully "effective" due to concerns over on-going challenges to TOLA.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

related data. The types of behavioural and outcome-related impacts may be construed broadly to include the potential effect of TOLA on business revenues, investment, and strategic plans. For example, producer surplus may be estimated from sundry outcome-related data such as data on business revenues, operating costs, and investments, which may be estimated from data on unit-sales and per-unit price and cost data. Attributing changes in such variables to a single effect like TOLA requires additional data to control for other effects.

Estimating consumer surplus is even more difficult but includes estimating the extent to which inframarginal consumer demand exceeds the prices paid (i.e., extent to which willingness-to-pay exceeds price).[90] Moreover, consumer surplus also depends on product choice (selection) and quality.[91]

Behavioural responses include changes in firms 'employment practices, investment behaviour, and innovation activity, which are related. For example, investments in business capacity depend on expectations regarding the future prospects for the firm, which depend on the firm's competitive advantage and on the firm's investments in R&D and sundry strategic investments (e.g., in its brand image, in cybersecurity, in intellectual property, etc.). As we explain further below, one of the potential behavioural responses that might be anticipated is for firms to reduce their investments in R&D and new product introductions in Australia that are expected to be adversely impacted by TOLA, whether directly or indirectly. To the extent that occurs, estimating the economic impact will depend on computing the future net benefits expected from the deterred investments or improvements in product choice and pricing that otherwise would have occurred. That is inherently more challenging than measuring what actually happened.

Thus, the behavioural and outcome-related impacts depend on the business attitudes and expectations. The impacts are potentially economy-wide and even global, and hence extend beyond those attributable directly to enterprises that receive TOLA Requests or Notices, and indeed, those indirect impacts are expected to be much larger

[90] Willingness-to-pay is not observed directly but may be inferred from consumer surveys and by revealed preference behaviour in the marketplace (i.e., the estimated industry demand function).

[91] Consumers typically make their purchase choices from among multiple firms, each of which offers multiple tiers of products (e.g., premium, discount) and choose the product that offers the best price-quality trade-off. For the same quality good, consumers always prefer lower prices. However, since consumers' demand for quality and other product features varies, having multiple choices increases the likelihood that consumers can find goods that more closely match their idiosyncratic tastes. Additionally, the more firms to choose among, the more competition, which may (or may not) result in wider selection of quality-tiers depending on the nature of the product and the competitive dynamics, but generally will result in lower prices. However, even with a single firm, the selection of products offered is designed to maximise producer surplus which confronts firms with the challenge of setting product tier pricing to optimally price discriminate: that is, to price so that some consumers find the added-quality-for-a-higher-price trade-off rational; otherwise, consumers opt for the lower-priced, lower-quality good and the higher quality tier is not viable in the marketplace.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

in aggregate than the direct effects. However, even though it is difficult to assess the direct economic impacts, estimating the indirect impacts is even more challenging.

5.1.2. Focus on Australian or Global Impacts?

While our focus is on the Australian economy, we are also interested in identifying likely spillover effects more broadly. The market for ICT technology, products, and services is global and the legislation in Australia may influence the likelihood of similar legislation in other nations that strengthen or weaken the economic impact of TOLA within Australia over time.

The concern over the ability of LEIAs to access information that is increasingly in digital form, either "in motion" (telephone calls, messages, file transfers, identity or credential exchanges) or "at rest" (stored as digital files or programs on devices or file-servers in the cloud), that is also increasingly protected by cybersecurity tools, such as end-to-end encryption technologies, is considered by some as posing a serious threat to the effectiveness of law enforcement and security services internationally.

Policymakers in multiple countries have proposed and debated legislative initiatives that would grant law enforcement and intelligence agencies additional powers to gain exceptional access to digital data.[92] As explained earlier, although TOLA follows on the UK's earlier adoption of expanded government powers to acquire industry assistance in circumventing encryption, the lessons learned in Australia are likely to impact whether other nations follow Australia's example. This causes concern since the lack of empirical evidence of significant economic harms may be mistaken for evidence of a lack of such harms, which might encourage other countries to adopt similar TOLA-like legislation, thereby amplifying the costs of TOLA.

5.1.3. How to balance the focus on TOLA costs versus benefits?

Assessing the net aggregate monetary impact of TOLA requires considering both the costs that TOLA is likely to impose as well as the benefits that TOLA may deliver. While it is relatively easy to identify multiple mechanisms by which TOLA may directly impact the behaviour of firms, and hence consumers, in ways that will result in increased costs, tracing the mechanism by which TOLA will lead to increased benefits turns out to be more difficult.

[92] For example, the UK has had legislation in place enabling law enforcement and national security intelligence services to gain lawful access to encrypted information since the early 2000s, which was expanded via the UK's Investigatory Powers Bill (2016) (see Note 27 *supra*). More recently, in the U.S., Republican Senator Lindsay Graham introduced Senate Bill 4051 – the Lawful Access to Encrypted Data Act (LAEDA) in June 2020 (see https://www.congress.gov/bill/116th-congress/senate-bill/4051); and in October 2020, the "Five Eyes" intelligence alliance among Australia, Canada, New Zealand, the UK, the US (the original "Five Eyes"), India and Japan issued a joint statement calling stronger capabilities to enable lawful access to encrypted data (see https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/925601/2020.10.11_International_statement_end-to-end_encryption_and_public_safety_for_publication_final.pdf)

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

In subsequent sections, we identify the various mechanisms by which TOLA may result in increased costs. In the remainder of this section, we explain why estimating benefits is more challenging.

On both the cost and benefit side, the restrictions on disclosure that are part of TOLA interfere with detailed data collection on how the use of TOLA changes behaviour. The data gaps are even more severe and the trail of causality even more difficult to trace on the benefit-side than the cost-side, however. The principal perceived benefit for passing TOLA was to address the perceived challenge that increased use of encryption poses for LEIAs in pursuing their law enforcement and national security missions. Presumptively, the expanded capabilities enabled by TOLA are supposed to improve the effectiveness and efficiency of LEIAs. This lack of transparency makes it more difficult to ascertain how TOLA has or may change the behaviour of LEIAs (relative to the relevant but-for world).

However, even before one digs deeper into resolving those data deficiencies, it is possible to qualitatively consider how TOLA may impact the effectiveness of LEIAs. There are several plausible reasons that suggest that the benefits to LEIAs are likely to be small. Those include the fact that (a) technologies are widely available to anyone (including criminals) to overlay additional layers of data security, including encryption; and (b) extensive legislation already exists in many countries that provides for lawful access to data.

The first point suggests that suitably motivated targets who want to secure their data can do so even if TOLA is adopted, by employing strong encryption for both in transit (*e.g.*, end-to-end messaging) and at rest (*e.g.*, storage on a device), and making use of other techniques (e.g., various forms of indirection such as onion-routing) to render any efforts at providing assistance by DCPs ineffective. Criminals know they are always playing a cat-and-mouse game with law enforcement. Thus, they have an added incentive to take advantage of techniques that utilise additional layers of security.

Even if one rejects the first point, however, the second point highlights that the incremental benefits of TOLA depend on the extent to which TOLA creates new capabilities that expand law enforcement's capabilities to access the data of lawful targets. However, since there is uncertainty as to how TOLA may be used, it is uncertain how large those incremental benefits may be.

In any case, the evidence-based policy analysis needed to estimate costs and benefits of TOLA more precisely only becomes necessary if one expects that the costs and benefit estimates are likely to be relatively close in magnitude. If there is convincing support (or evidence) that the total costs are minimal, but the total benefits are substantial (or vice versa), then having precise estimates of the economic impact is less important.[93]

[93] There are four possible cases (Costs/Benefits) as follows (large, large), (large, small), (small, large), (small, small).

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

Since no actual detailed economic impact analysis has been conducted (or made publicly available) thus far, one might reasonably conclude that the benefits would outweigh the costs most readily if one concluded either that (1) the potential costs are minimal while the benefits are large, or (2) that the potential costs and benefits are both minimal but the potential benefits are larger.[94] The above-cited qualitative arguments suggest that the first case is unlikely, but that second case still needs to be addressed. Thus, focusing on the magnitude of the potential costs is a reasonable starting point.

5.1.4. Is analysis of impacts long-term or short-term?

It is obviously of interest to see if it is feasible to measure any short-term impacts due to TOLA since its passage just two years ago. However, the full effect of TOLA is likely to be experienced over time, and the future has a lot more time over which to realise whatever costs TOLA may bring. Thus, it is expected that the most significant economic impacts of TOLA are likely to be in the future. For example, the expected impacts would be larger if the full breadth of TOLA remains in force, the number of Requests and Notices under TOLA increases beyond the low level seen during its first two years, and further expands to include the use of Technical Capability Notices that require service providers to modify their systems or technology.[95]

5.1.5. How is the "but-for" world characterised?

We take the pre-TOLA situation as our "but-for" standard, while recognising that in a world without TOLA, other things would have happened that might be amenable to forecasting (e.g., a different version of TOLA or a different rate of adoption of encryption technology). Identifying an appropriate but-for scenario poses a special problem in the case of assessing the economic impact of investments in information security (i.e., "InfoSec," such as in firewalls, enhanced security monitoring, and encryption technologies). That is, because the return on investment is based on the cost of harms avoided, and any such estimate depends on the probability of those harms being realised in the absence of the InfoSec investment – which is inherently probabilistic and uncertain.[96] Further elaboration of the but-for scenario would be part of a more general equilibrium evaluation of TOLA's economic impacts.

[94] Here we ignore the cases where costs are thought to be large since that would make it less likely that passage of the TOLA would have been supported by an economic impact assessment.

[95] To date, TOLA has been utilised minimally: to date, less than 50 TARs (and no TAN or TCN) notices have been issued (see Note 32 *supra*).

[96] For most investments, a user will observe benefits flowing from use of the capabilities enabled by the investment (e.g., a car and the travel that is enabled by the car can allow the investment to be amortised over the miles driven). With cybersecurity investments, the benefit derives from the harms not realised (e.g., the reduced incidence of fraud or costs incurred in the event of a data breach). Like fire insurance, as a consumer, I wish I could recoup all the past insurance payments I made for the years when I did not experience a fire.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

5.1.6. How to collect data on TOLA impacts?

The challenges to estimating the economic impact of TOLA are made significantly more difficult due to the non-disclosure requirements in TOLA. Those prevent recipients of TOLA notices from reporting on the details of any notices they received or what transpired as a consequence. They also prevent LEIAs from disclosing how they may be using TOLA. This makes it very difficult to isolate TOLA related impacts from the many other impacts that may affect economics-relevant firm behaviour or firm outcomes (e.g., revenues, investment in cybersecurity, etc.). For example, if firms modify their brand marketing, product advertising, or customer support practices, it is unclear whether firms are doing so as the result of having received a TOLA notice, in anticipation of how TOLA may be impacting their markets, or due to some entirely unrelated cause.

Reporting on TOLA notices is delayed and provided only at an aggregated level. The number of notices issued in total are reported, but not what types of firms received TOLA notices. DCPs are authorised to make statistical disclosures regarding the total number of notices received over the prior six-month periods and whether the notices were voluntary (TARs) or mandatory (TANs or TCNs), but companies cannot detail which LEIA issued those notices or further details.

DCPs *may* seek authorisation to allow them to disclose information about the assistance.[97] Whether DCPs will seek such authorisation and whether it will be granted is uncertain. For example, any DCP that is induced to provide assistance that actually threatens or may be perceived to threaten the digital security of that DCP's products or services may be disinclined to disclose any such action for fear of the adverse brand impact that may result.

While full transparency regarding how TOLA is being used by LEIAs would likely harm the effectiveness of TOLA-aided LEIA activities and may pose additional cybersecurity risks,[98] the near total blockage of any data on how TOLA is being used renders any accurate assessment of its economic impacts nearly impossible.[99]

---

[97] See s 186(2) of the TIA Act, Note 6 *supra* and s 317ZF(13)-(17) of TOLA, Note 2 *supra*. Also, see "Assistance & Access: Common myths and misconception," Note 130 *infra*.

[98] For example, full transparency would include information about which DCPs received TOLAs, what those TOLAs requested or required the DCPs to do, what the DCPs did in response to the TOLAs, which LEIA issued the TOLAs, and what did the LEIA do as a consequence of the assistance provided by DCPs. Obviously, that level of public disclosure would serve notice to LEIA targets of interest (e.g., potential criminals) that would enable them to take evasive actions to counter the LEIA investigatory efforts. Full disclosure might also reveal details about LEIA or DCP security capabilities that might be exploited by others, resulting in additional cybersecurity risks.

[99] To estimate the economic impact of TOLA, disclosure need be neither complete nor public. More granular, detailed data may facilitate better estimates, but even relatively coarse data on the types of assistance that have been requested, required, and/or provided would greatly overcome the data gaps. Additionally, this data might be disclosed under protective orders that restrict reporting of detailed data used to estimate aggregate economic impacts by the

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

Furthermore, the gaps in TOLA-related data, coupled with the safe-harbour rules, reimbursement provisions allowing DCPs to petition for recovery of assistance-related costs, and the ambiguity in what LEIAs may request or require, have the perverse result that they may increase the expected economic harms from TOLA. Those harms are most likely to be associated with indirect effects. The reason for this is that together, these features of TOLA lower the incentives for DCPs to resist complying with LEIA requests, even if such requests may pose a threat to digital security.

A DCP that cooperates is less likely to be penalised for its cooperation by either its customers or other entities it does business with since those other entities or customers can only guess at whether the DCP had received a notice and how it responded. The secrecy surrounding TOLA's use adds to the business uncertainty confronting all entities that may be impacted by TOLA, spreading those impacts more broadly as interested parties are left to assume that any of the DCPs, or all of the DCPs may have had to comply with TOLA requests or requirements.

Finally, the same lack of access to TOLA-related data that inhibits estimating TOLA's economic impacts also renders oversight of TOLA more difficult.[100] An increased perception that TOLA oversight may be inadequate may contribute to the perceived risk of LEIA abuses that threaten digital security, and hence digital trust, thereby compounding any adverse economic impact that TOLA may have.

5.2. Qualitative Discussion of Economic Impacts

As noted above, the economic impacts of TOLA are likely to be both direct and indirect, to accrue and change over time, and to have spillover effects beyond Australia. Some of these impacts may be more readily observable and quantifiable than others. For example, assessing the direct effects of TOLA by focusing first on the business enterprises that are obligated by the scope of the legislation to respond to TOLA Requests and Notices and the products and services offered by such enterprises which make use of encrypted data, either in motion or at rest, is likely to offer the greatest opportunity for detecting measurable behavioural or outcome-related economic impacts of TOLA.

Moreover, a better understanding of the direct effects is likely to assist in understanding the nature of potential indirect effects. Furthermore, it is reasonable to focus first on trying to detect from past experience with TOLA whether there have been measurable impacts before trying to assess forecasts of future impacts, even if one suspects – as we do – that most of the economic impact is likely to occur in the future. This logic

analysts or researchers tasked with deriving the estimates. Specifying what minimal disclosure might facilitate reasonable estimates of economic impacts is beyond the scope of this report, however, we believe more protected access to relevant data could be enabled that would facilitate estimating economic impacts while preserving the efficacy of TOLA assistance to LEIAs.

[100] Indeed, estimating the economic impact of TOLA is part of the oversight that is needed to protect Australia and other countries from the effects of misguided legislation.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

provides a natural way to discuss qualitatively our expectations regarding the sorts of impacts that may be observed.

First, TOLA Requests and Notices can only be directed to DCPs, which is construed broadly to include any enterprise that provides Information and Communications Technology (ICT) services or products that make use of encrypted data in Australia (whether those companies are headquartered in Australia or abroad).[101] Even this scoping presents a complex "supply chain"[102] of upstream and downstream firms that collectively are responsible for delivering encrypted data services and products for use (consumption) by end-users, which comprise other businesses that make use of encrypted data in their daily operations (e.g., banks, hospitals, and indeed, most businesses today, but with varying degrees of importance to their operations) and mass market consumers (e.g., home users of mobile and fixed broadband services).

The supply chain includes the upstream producers of encryption technologies, equipment and services such as the firms that make the network equipment, contribute to the development of international standards, possess patents or trademarks for security technologies, etc. Those firms, loosely characterised as the "InfoSec" industry sell software and hardware products that are used to authenticate digital credentials, filter and selectively block digital traffic (e.g., firewalls), and sundry other services (e.g., cybersecurity traffic monitoring feeds) that are purchased and used by downstream DCPs such as Internet Service Providers (ISPs) such as Telstra and TPG or providers of cloud or edge services that provide applications and content services such as Facebook, Google, or Netflix. It includes end-user device makers and the developers and vendors of software applications and services that make use of those devices, ranging from smartphones to tablets to Internet-of-Things (IoT) devices.

Tracing the business relationships among ICT enterprises is complicated by the fact that ICT enterprises both sell to other ICT firms, as well as directly to end-users (e.g.,

[101] This scoping excludes consideration of enterprises or end-users that may be the purchasers of ICT services that make use of encrypted data (e.g., hospitals, banks, or other end-users). However, since end-users constitute the final demand for the use of encrypted data services, the impact of TOLA on their behaviour and the outcomes they experience (e.g., in the prices they pay and the selection of products they are able to choose from, or equivalently, the quality of those products) is also relevant to the assessment of the total economic impact of TOLA.

[102] The terms supply chain, value chain, or production chain may be used interchangeably here. These reflect the concept that the production of most goods and services may be organised into a chain of tasks or stages flowing from raw resources through intermediate stages of production to final sales to end-users. In its simplest form, this is viewed as a linear flow of stages that may be organised into a series of upstream and downstream firms, with some firms being vertically-integrated into multiple sequential stages. Firms that operate at the same stage are horizontal competitors, whereas firms that operate at different stages are vertical competitors. In this sense, the competition is ultimately for the final-demand that provides the revenue flows that support the supply-chain activity. However, most production processes, especially when it comes to ICT products and services, do not fit this model cleanly. There are multiple parallel processes and complex feedback loops. Firms may simultaneously be vertical and horizontal competitors.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

businesses and mass-market consumers operating internal, private data networks). Moreover, many ICT enterprises operate at different levels within the supply-chain and may simultaneously sell components and technology to firms as upstream suppliers to the same enterprises that they simultaneously compete with in downstream markets (e.g., Apple buys components from Samsung, they cross-license technology, and both sell smartphones).

To analyse the economic impact of TOLA, one could focus on the entire ICT value chain that provides products and services that make use of encryption or encrypted data, viewing this entire value chain as a "black box" that supplies a range of products and services that make use of encrypted data and focus on how TOLA might impact aggregate supply and demand for those products and services. At an abstract level and in an increasingly digital economy, that may be seen to include the entire economy of goods and services, since virtually everything in a modern economy makes use directly or indirectly of ICT and, increasingly, encrypting data is viewed as a key "best practice" for ensuring that ICT products and services are "trustworthy" or equivalently protected against cyber-risk, which includes against data breaches that may threaten privacy or other forms of economic loss (e.g., fraud, ransomware attacks, destruction of value, loss of personal safety, etc.).

From this perspective, TOLA may be viewed as imposing costs on securing data, and hence, as posing a threat to "trust" of digital products and services that includes trust in using the Internet and other data networks for eCommerce, which as already noted, will increasingly include the entire economy. In the simplest economic analysis, the increased cost of providing "trusted" ICT services will raise the costs of supply and decrease end-users 'willingness to pay. This would suggest an upward shift in aggregate supply and a downward shift in aggregate demand, resulting in a new, post-TOLA higher equilibrium price at a lower level of aggregate demand. Prices would be higher and aggregate demand would be lower, producing what economists refer to as a "deadweight loss" associated with the imposition of TOLA.

If this simple analysis of effects were the entire story, then of course, it would be irrational to have adopted such a policy. Complicating factors include the already noted fact that we are ignoring the potential ways in which TOLA might increase trust by enabling law enforcement to be better at preventing crime, resulting in a net upward shift in aggregate demand that might more than offset for any threat TOLA might be estimated to cause due to an increased risk of a perceived loss of privacy or from higher costs that enterprises may incur as a result of the constraints TOLA imposes on the use of encryption technologies.

A further complication with the analysis of TOLA is that the effects are unlikely to be uniform across all sectors of the economy, ICT supply chain stages, or encryption-using products and services, and hence, final demand for those products and services. One way to address this challenge is to conceptually apply the above framework separately to different sectors, ICT production stages, or "markets" for products and services, and then model the interactions among these different partial-economy, partial-equilibrium analyses to compute overall effects. Such analyses may be undertaken by constructing

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

a suitably detailed Input-Output model of the economy or of the ICT supply-chain that tracks the purchases and sales that firms or aggregates of firms (or "industries" or "industry segments") make from each other and the impact of TOLA on the prices and quantities of those transactions. In principle, the more detailed the model and the better the data, modelling and forecasting tools are for implementing the model, the better the picture one might get of both the aggregate and distributional effects of TOLA.

Such an ideal economic model would allow one to consider how ICT businesses, end-user businesses, and individual consumers would change their behaviour in response to TOLA and its impact first on the firms directly impacted, and then as a consequence of the reactions of other firms, and so on. The direct and indirect behavioural responses by firms would ripple through the model to produce a new equilibrium outcome that could be compared with the pre-TOLA equilibrium (i.e., the "but-for" world) to see whether the total aggregate net benefits to the Australian, or indeed, global economy were higher or lower with TOLA and to show how total aggregate benefits are distributed.

Unfortunately, such an ideal model is not feasible because none of the elements needed exist. Before considering the available economic tools and methods for constructing such an idealised model, it is sufficient to note that the near complete lack of relevant data, by itself, is a sufficient impediment to estimating the economic impact of TOLA, regardless of the scoping perspective taken. Data does not exist even to identify unambiguously, let alone measure the behavioural and outcome impacts, on the subset of enterprises in the ICT supply chain that will be impacted by TOLA.

Proponents of TOLA have taken the perspective that any adverse economic impacts from TOLA are likely to be minimal because:

- only DCPs that receive TOLA notices are impacted,
- TOLA provides for the recovery of reasonable costs incurred in responding to notices, and
- TOLA precludes LEIAs from requesting DCPs to do anything that would result in systemic harm to the security of their products and services.[103]

That is, their argument is that few firms will be impacted and the implications on the trustworthiness ("quality") and price ("cost") of those firms 'products and services will be negligible, and so there will not be either significant adverse distributional or aggregate adverse economic impacts from TOLA.

Opponents of exceptional access legislation like TOLA, which includes most of the global technical community and ICT industry, dispute both of these claims. We take as evidence of this consensus view the Carnegie Report (2019) that echoed conclusions reached earlier by an earlier paper authored by some of the same experts, which concluded that there is no known way to enable the sort of targeted access to encrypted

[103] Systemic harm to digital security is differentiated from the selective reduction in digital security for the narrowly targeted individual or individuals that is/are the focus of a TOLA request.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

data that TOLA anticipates which does not result in the creation of systemic vulnerability.[104]

In framing the analysis of the potential adverse impacts of TOLA, the creation of a systemic vulnerability – and thus, enabling the targeted access to encrypted data that TOLA facilitates -- will adversely impact "trust" in cybersecurity.[105] This adverse impact on trust may arise from multiple effects.

First, the potential that TOLA will result in a LEIA accessing data that the target had previously viewed as secure means that the target experiences a reduction in cybersecurity. Second, since TOLA leaves it inherently uncertain as to whose data will be targeted, this means that there is an increase in cyber-risk for all.[106] Third, if one accepts the Carnegie Report view that there is no known way to enable targeted access without introducing a systemic vulnerability, the application of TOLA would reduce cybersecurity directly for any systems/services that suffer the introduction of the systemic vulnerability. Taken together, these effects suggest that TOLA results in increased cybersecurity risk.

Moreover, even if it were feasible to limit systemic vulnerability, the comments submitted during the public consultation over TOLA before its passage in December 2018 highlighted the multiple ways in which the passage of TOLA increased uncertainty regarding the government's powers to potentially adversely impact cybersecurity.[107] Therefore, even if one were to determine that the real threat to cybersecurity, or equivalently, the increase in cyber-risk were trivial, the perception of the adverse impact potential could harm trust and that could result in potentially

[104] See "Moving the Encryption Policy Conversation Forward," Encryption Working Group, Carnegie Endowment for International Peace, September 2019, available at https://carnegieendowment.org/files/EWG__Encryption_Policy.pdf. This report summarised the conclusion of an Encryption Working Group convened by the Carnegie Foundation to provide guidance from senior researchers within the cybersecurity community on how to approach lawful access legislation. The overall conclusion was that they did not (as yet) see any way to broadly enable such lawful access without introducing systemic vulnerabilities.

[105] We use "trust" here abstractly to refer to the perceptions that stakeholders (customers, firms, policymakers, etc.) have in cybersecurity, which only imperfectly maps to whatever the actual state of cybersecurity is.

[106] One may argue that since only criminals should be the target of lawful access requests, the likelihood that lawful citizens would ever be a target is sufficiently small to be ignored but that depends on accepting the assumption that TOLA powers would not be abused by accident, or by knowing abuse, and both of those are legitimate concerns.

[107] The Australian Department of Home Affairs published 343 of the comments received during the public consultation (see https://www.homeaffairs.gov.au/help-and-support/how-to-engage-us/consultations/the-assistance-and-access-bill-2018). Common concerns expressed by many commenters included the lack of clarity regarding the scope of TOLA powers, the effectiveness of protections and oversight, the lack of transparency, and the lack of any empirical analysis of the economic impact of TOLA. All of this, and the subsequent challenges, contributed to increasing uncertainty as to the likely impact of TOLA on cybersecurity.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

significant adverse economic effects that would not be limited only to ICT firms or DCPs who might be recipients of TOLA notices.

Thus, one way to think about TOLA is to consider what the economic impact of reduced trust in cybersecurity might be for the aggregate economy. Reduced trust would lead to reduced demand for and activity in the digital economy, which would reduce or delay (which reduces the economic value in present value terms) ICT-driven productivity growth and innovation.[108]

One way to size the economic value of an economy-wide increase in perceived cyber-risk or reduced trust is to develop scenario-based forecasts of what happens under different levels of trust. A good example of such an analysis was prepared by the Zurich Insurance Group in 2015.[109] The Zurich study used a macroeconomic model to forecast the potential benefits for global economic growth under a variety of scenarios that differed with respect to the level of trust in a secure Internet.

Under a high-trust scenario, eCommerce is not threatened by cybercrime and the economic growth is faster, whereas under a worst-case scenario, cybercrime so damages trust in on-line economic activity that eCommerce grows much more slowly. The base-case is somewhere in between. This study pointed to a potential gap between the best and worst cases forecasts through 2030 of 120 Trillion USD, accounting for a 6% swing in cumulative global GDP, demonstrating the serious threat that cybercrime poses for the global economy. The slower growth is due to the joint effects of reduced demand to engage in online commerce and the resulting reduction in incentives by supply-side firms to invest in providing the capacity to support slower demand growth.

To bring the context closer to Australia, an AustCyber (July 2020) report estimated that digital activity "contributes AU$426 billion to the Australian economy and generates AU$1 trillion in gross economic output, generating 1 in 6 jobs."[110] That report

[108] There is significant economics literature demonstrating that investment in ICTs has the potential to deliver significant excess returns and contribute to economic productivity growth. For a summary of this, see Lehr, W. & Sharafat, A. (2017), "ICT Engines for Sustainable Development," in A. Sharafat & W. Lehr (eds.); ICT-centric economic growth, innovation and job creation, Geneva, Switzerland: International Telecommunications Union (ITU), available at https://www.itu.int/dms_pub/itu-d/opb/gen/D-GEN-ICT_SDGS.01-2017-PDF-E.pdf; or World Bank (2016), "World Development Report 2016: Digital Dividends.," http://www.worldbank.org/en/publication/wdr2016.

[109] See Zurich (2015), "Risk Nexus: Overcome by cyber risks? Economic benefits and costs of alternate cyber futures," Report prepared by the Atlantic Council and Zurich Insurance Group (Zurich), September 2015, available at http://publications.atlanticcouncil.org/cyberrisks//risk-nexus-september-2015-overcome-by-cyber-risks.pdf.

[110] See AustCyber (2020), "Australia's Digital Trust Report," available at https://www.austcyber.com/resource/digitaltrustreport2020. Report July 2020, 52 pages. The report estimates that 22% of the Australian economy is supported by digital activity, which accounted for 6% of GDP directly. Sectors include: $317 billion Digital Activity -- $16B cybersecurity, $35B online retail, $2.7B digital health, $0.7B Solar power, $3.9B spac,e etc. (page 11).

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

estimated that a four-week digital interruption due to a widespread cyber-attack would cost 1.5% of Australia's annual GDP.[111] That is an estimate of the direct effects of a successful attack and an increase in cyber-risk means that such an outcome is more likely to occur.

What both of these studies highlight is the potential for large adverse impacts if digital security is compromised and therefore the importance of enhancing trust in digital security. Unfortunately, they do not provide useful guidance on how to quantify how TOLA may increase cyber-risk other than to suggest that the effects might be very large, and economy-wide in their impact.[112]

It is also feasible to consider that there may be regional or sector-specific adverse effects resulting from asymmetric threats to trust. For example, the Australian ICT sectors may be expected to suffer a greater adverse shock associated with TOLA in the near-term, associated with less trust of their products and services than the ICT sectors in other nations that are not directly impacted. That could adversely impact the international competitiveness of Australia's ICT sector. One could also drill down below the national level to look at sub-segments of the ICT sectors and other sectors that are heterogeneously dependent to greater or lesser extents on using encrypted data that would be vulnerable due to TOLA.

At the firm level, one might anticipate that TOLA could result in a variety of direct or indirect effects. For example, the reduction in aggregate demand for a firm's products due to the reduction in market trust would shrink the pie for all firms. Additionally, the extent to which a firm suffered an even greater loss of trust might reduce that firm's market share of the lower aggregate demand. The effects of reduced data security might range from minor (e.g., the loss of a few sales for a few products) to major (e.g., the existential threat to a firm's future business if TOLA leads market participants to distrust the firm's commitment to transparency and securing customer data).

This last outcome is a relevant concern for firms whose business models are premised on open source software and off-the-shelf/mass-market services and products (i.e., services and products that are not customised to an individual customer basis). Committing to open source as a key component of the business model and platform commits the firm to a level of transparency that is fundamentally incompatible with the TOLA restrictions limiting companies 'abilities to disclose changes to their offerings, and code that might be needed in order to respond to a TOLA notice.

[111] Ibid., page 5. The report estimates AU$30 billion and 163,000 jobs would be lost as result of the wide-spread attack.

[112] The impact might be large if it resulted in a single data breach with a large, wide-spread impact, if it resulted in many more successful breaches that were each small but large in aggregate impact, or some combination of both. The point is that cybersecurity vulnerabilities may result in multiple types of harm that differ in the severity and scope of those harms. Absent a model of the threat landscape and the likelihood of particular threats being successful, it is not feasible to reliably forecast the harm that is expected to result.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

In assessing the economic impact of TOLA, an individual company needs to assess the likelihood that they might receive a TOLA Request or Notice that will impact its operations, how that would affect their operations, and what their options for responding are. This is similar to the way in which companies should assess their cyber-risk and determine their optimal strategies for investing in information security (InfoSec) products and services like firewalls, traffic monitoring services, and other internal cybersecurity resources, including cyber insurance (CyberIns) to address any residual cyber-risk that cannot be adequately addressed by improved cybersecurity processes.[113] Some of the ways that an individual firm might incur adverse impacts from TOLA are addressed in the following sub-sections.

5.3. Increase in Business Uncertainty

TOLA increases regulatory uncertainty, as already noted. Increased technical, market, or regulatory uncertainty increases the riskiness of irreversible investments, which can delay or deter such investments. Measuring the impact of business uncertainty is difficult in general, and not practical for the effect of a particular piece of legislation such as TOLA.

An indication of the potential importance of legislation that impacts the regulatory uncertainty associated with the use of encryption technology, however, is available from the only two studies conducted to date that sought to estimate the economic impact of encryption technology. Those studies were conducted by the National Institute of Standards and Technology (NIST) in the U.S. in 2001 and 2018.

In the NIST (2001) Encryption Impact Study,[114] the researchers sought to estimate the economic contribution that promotion of the Data Encryption Standard (DES) by NIST added to the U.S. economy. They concluded that NIST's efforts accelerated adoption

[113] Making investment decisions about InfoSec/CyberIns is information intensive, and hence, expensive in its own right. Arora et al. (2004), Hubbard & Seiersen (2016), Jones (2005), Gordon & Loeb (2002) and others have proposed decision theoretic tools and methods to assist in estimating cyber costs and the benefits of alternative cybersecurity strategies to assist in investment decision-making. See Arora, A., D. Hall, C. Piato, D. Ramsey and R. Telang (2004) "Measuring the Risk-Based Value of IT Security Solutions." *IT Professional*, 6(6), 35-42; Hubbard, D. W. and R. Seiersen (2016). How to measure anything in cybersecurity risk, John Wiley & Sons: New York, 2016; and Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC), 5*(4), 438-457. To understand some of the challenges associated with assessing the economic impact of cybercrime, see Wolff, Josephine and William Lehr (2017), "Degrees of Ignorance About the Costs of Data Breaches: What Policymakers Can and Can't Do About the Lack of Good Empirical Data," 45th Research Conference on Communications, Information and Internet Policy (TPRC45), September 2017, Alexandria, VA, available at SSRN: https://ssrn.com/abstract=2943867.

[114] See Leech, D. and M. Chinworth (2001), "The Economic Impacts of NIST's Data Encryption Standard (DES) Program," study prepared for U.S. National Institute of Standards and Technology (NIST) Program Office Strategic Planning and Economic Analysis Group, October 2001, available at https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=918355 (hereafter, NIST 2001 Encryption Impact study).

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

of DES by several years, resulting in net benefits of between $USD 345 million to $USD 1,190 million associated with lower costs for managing third-party bank data.[115]

A NIST (2018) follow-on study looked at the economic impact of the Advanced Encryption Standard (AES) that NIST also played a role in promoting.[116] The later study relied on a survey-based approach to derive estimates of how AES helped reduce the costs of firms active in deploying encryption technologies because of the existence of a federal standard. In the NIST (2018) study, they again posited a counterfactual world in which the evolution to the more efficient AES standard would have been slower.

In this case, the researchers benefited from being able to directly model the performance improvements that AES offered relative to the standard it was replacing. The NIST (2018) study estimated that the internal rate of return on NIST's investment in promoting AES was 81%, significantly more than NIST's 7% cost of capital (under government regulations), and the aggregate net benefits to the economy exceeded $USD 250 billion once all direct and indirect spillover effects are computed.

Both of these studies concluded that a small investment in accelerating the deployment of encryption capabilities resulted in very large gains to the economy. This suggests that viewing TOLA as an intervention that has the potential to delay deployment of enhanced encryption techniques (by slowing adoption or tilting adoption towards less secure encryption) could have a large negative impact. Also, in both cases, one might understand NIST's efforts in promoting acceptance of an industry standard as acting so as to reduce business uncertainty.

5.4. Damage to Business Brand

Firms establish their brand through advertising and the reputation they build by how their products compare in the marketplace to competing offers from other firms. The better the brand, the easier it is for the company to sell its products and earn sales revenue, to defend itself against competitors or respond to adverse market changes, and

[115] The goal of the study was to demonstrate how NIST contributed to economic growth. The case study documented NIST's role in promoting earlier adoption of an industry encryption standard than would have occurred otherwise. The DES standard was adopted in 1977 and the study looked at adoption behaviour from 1977-1982. The researchers initially tried to collect survey data to directly measure impacts and that proved to be unsuccessful. The alternative they eventually used was to compute the impact based on specific industry outcomes based on the costs avoided by retail-banks in the US which were able to switch to electronic transactions (lower cost) more quickly than would have been the case otherwise. They estimated the cost avoidance benefits of electronic transactions as they were realised over time (actual world) and compared those to two scenarios of but-for world (benefits would have been delayed by 3 to 6 years) and computed NPV of scenarios to estimate net effect of NIST efforts.

[116] See Leech, D. and John Scott (2018), "The Economic Impacts of the Advanced Encryption Standard, 1996-2017," prepared for the National Institute of Standards and Technology, NIST GCR 18-017, available at https://doi.org/10.6028/NIST.GCR.18-017.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

the more attractive the company is to investors. All other things being unchanged or constant, a better brand image is associated with higher sales over time and hence a higher market value (which reflects the market's assessment of discounted value of expected future firm profits). It is an intangible asset that cannot be measured directly but is assessed by reference to changes in other measurable indicia like sales, profits, market value, or surveys of investor or customer perceptions.

Anything that threatens the relative perception of trust in a company can damage its brand, and hence its sales prospects and business value. Although customers, business partners, investors, and firm insiders may be able to qualitatively assess whether TOLA has had a significant impact on the firm's brand or not, that effect cannot be quantified directly.

Under some interpretations of TOLA, the potential adverse impact of TOLA could be viewed as an existential threat for some firms whose brand is highly dependent on the firms 'commitment to cybersecurity and/or business models that depend on open source software. For example, a cybersecurity vendor of encryption technology might find its core product undermined by the creation of a capability in Australia that threatens its service offering. In another case, it could undo the business model for a firm that builds its business model on committing to transparent, open-source software that does not discriminate among end-users. Being required to alter the code for a target and then not be able to disclose those modifications to the rest of its customers (due to TOLA's non-disclosure requirements) would be inconsistent with a foundational component of its business model. And, in yet another case, a firm that builds its business model on proprietary code may see a core asset undermined if TOLA forces the firm to disclose source code that might leak into the public domain.

5.5. Lost Sales

Although the direct impact on a business's brand image cannot be directly quantified in dollars, the impact on sales often can be. A firm may be able to trace a particular event as adversely impacting the purchasing behaviour of specific customers or towards particular products. A firm may observe that customers buy less of a firm's offerings because the customers indicate they are concerned about TOLA's threat to data security.

Those lost sales may reflect reduced consumption by buyers (e.g., reflecting the reduction in aggregate demand in a less trustworthy world) or sales that shift to a competitor. The competitor may be another firm in the same market (Australia) or off-shore. The changes in customer purchasing behaviour and hence firm sales may be traceable to specific subsets of products to a greater or lesser degree. Firms often directly contact actual and potential customers to identify what they care about and why they purchase what they do. Firms may also infer that from what customers purchase and from third-party market intelligence that seeks to estimate the value to customers of different security related features.

Although, in principle, sales data is one of the sources of direct outcome effects that may be most readily observable, attributing changes in sales due to specific legislation

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

like TOLA is always challenging. First, there are many factors that may impact the behaviour of customers, and separating out the effects of those factors may not be feasible. Second, when the effects are anticipated in the future, the added challenges of forecasting uncertain future events must be considered. Third, customers are not always truthful in explaining why they purchase what they do. They may not want to share the information because they do not want to offend their supplier or because they are concerned that revealing too much information may endanger their bargaining position. Regardless of the cause for reduced sales, the reduction in sales typically translates to reduced profits (under the reasonable assumption that firms would avoid incremental sales that do not bring sufficient revenue to cover their incremental costs),[117] and a reduced future stream of profits translates into a lower economic value for the firm.

Although it is challenging to consider how one might assess lost sales, there are a number of reasons to anticipate why the risk of a significant potential adverse impact on sales may be substantial. For example, in July 2020, the European Court of Justice issued a widely-anticipated decision that invalidated reliance on a workaround that allowed US and European businesses to exchange customer data that did not violate European privacy regulations, raising the threat that companies exchanging data between the US and Europe either increase data protection or cease the exchanges.[118]

TOLA may be seen as threatening the ability to meet the more stringent data protection standards adopted by the European Union and therefore pose a threat to the ability of businesses to exchange data between Australia and the European Union. Moreover, to the extent TOLA is indicative of further expansions of government powers in Australia, or elsewhere, to compel access to confidential data, that could lead to further disruptions in data flows.[119] Since international data exchanges are critical to the healthy working of the global digital economy, the breakdown in such exchanges has the potential to have a disastrous impact on global digital commerce.

5.6. Operating Cost increases due to TOLA

Firm costs may increase as a result of TOLA. First, there may be the direct costs incurred by a firm that receives a TOLA Request or Notice. The costs entailed would depend on whether compliance was voluntary (TOLA Requests) or mandatory (TOLA Notices) and the specific requirements of any TOLA Notice.

TOLA has provisions intended to mitigate the direct costs of responding to TOLA notices by (a) enabling recipients to recover incremental costs of responding; and (b)

[117] Here, we are ignoring such short-term strategies as loss-leader sales or business operations during a temporary downturn.

[118] See "The 'Schrems II' decision: EU-US data transfers in question," iapp Privacy Tracker, available at https://iapp.org/news/a/the-schrems-ii-decision-eu-us-data-transfers-in-question/.

[119] For example, New Zealand has an adequacy decision from the EU and TOLA may adversely impact decisions by New Zealand entities to make use of hosting or other services provided by Australian firms subject to TOLA (see "Adequacy Decisions," European Union, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en).

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

by limiting the scope of TOLA requests to those that would not result in any introduction of systemic vulnerabilities. Given the difficulty of estimating the full costs of responding to TOLA requests or notices, which include both direct and indirect effects, it is reasonable to expect that DCPs would be sceptical of the commitment to reimburse the full costs of TOLA's impact, or even the full direct costs of responding to a TOLA notice.

Additionally, we note the history of how oversight has been less than fully effective in limiting the scope of government agencies acting under new grants of authority.[120] As a result, it is reasonable to expect that DCPs and other firms impacted by TOLA remain uncertain as to the effectiveness of the oversight provisions in light of the lack of transparency, the vagueness of portions of the legislation, and other potential problems. After estimating the direct costs of responding to any TOLA Request or Notice, the firm would need to weigh that by against probability of receiving such a Request or Notice. The lower the probability that the firm will receive a Request or Notice, the lower the expected direct cost that will be incurred as a result.

Moreover, although compliance with TOLA Requests is voluntary, it is reasonable to anticipate that some recipients may perceive them as foreshadowing subsequent TOLA Notices. Thus, the view that TOLA Requests have significantly less economic impact than TOLA Notices is debatable.

Second, even firms that may never receive a TOLA Request or Notice may suffer brand image or customer relationship issues that may induce the firm to incur additional costs to address. They may feel compelled to increase brand image advertising and direct marketing to offset perceived risks to their brand image or sales prospects. They may need to spend additional resources addressing customers 'real or perceived concerns about the impact of TOLA on the security of their data and online trust.

Third, firms may be concerned that the security of services or products provided by their vendors or the security of the firm's internal operations in Australia are threatened by TOLA. Firms may re-evaluate their vendor relations and outsourcing options (e.g.,

[120] See extensive economics literature in public choice, and regulatory economics on regulatory creep which has a long history going back at least to Adam Smith's "Wealth of Nations," but most notably includes the work of George J. Stigler, "The Theory of Economic Regulation," The Bell Journal of Economics and Management Science Vol. 2, No. 1 (Spring, 1971), pp. 3-21; and Peltzman, S. (1976), "Towards a More General Theory of Regulation," Journal of Law and Economics, 19, 211–48. See also the economic theory of bureaucracies, including regulatory agencies, including the budget maximising thesis of William Niskanen, "Bureaucracy and Public Economics" (Cheltenham, UK: Edward Elgar, 1994 that can drive regulatory creep. See also Helm, Dieter. (2006) "Regulatory Reform, Capture, and the Regulatory Burden," Oxford Review of Economic Policy, 22 (2), 169; and Dal Bó, E. (2006), "Regulatory Capture: A Review," Oxford Review of Economic Policy, 22(2), 203–25. For Government recognition of the problem see, UK Cabinet Office Report - Better Regulation Task Force and Regulatory Creep Sub-Group - 2004: "Avoiding Regulatory Creep," which defined regulatory creep as the process by which regulation is developed or enforced in a less than transparent fashion and not in accordance with their five principles of good regulation: proportionality, accountability, consistency, transparency, and targeting.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

for cloud services to manage customer data or confidential firm data) in light of heightened concerns that those data could be vulnerable because of TOLA-induced behavioural responses by vendor partners.

This could result in firms shifting outsourcing and vending relationships offshore to avoid TOLA. Adjusting vendor relations or shifting internal firm operations from Australia will incur adjustment costs that ought to be directly attributable to TOLA, while also resulting in adverse spillover effects on other Australian digital sector participants, thereby adding to the indirect effects of TOLA.

Fourth, firms may shift from their optimal cybersecurity strategy due to the constraints imposed by TOLA. This would likely manifest as increased InfoSec and CyberIns costs to offset or address the increased cyber-risk associated with TOLA. One way in which firms estimate cyber-risk is by estimating the threat from different types of attacks. One of the most difficult threats to address are insider threats, or cybercrimes perpetrated by otherwise trustworthy employees.

For example, a common source of data breaches is disgruntled or corrupted employees motivated by the desire for revenge or illicit gains bypassing internal security defences to exfiltrate data.[121] The best firewall in the world does not stop an employee who carries confidential data files home on a USB drive or as paper files.

TOLA might be viewed as increasing insider threats since they have the potential of bringing the authority of the State to bear to induce an otherwise trustworthy employee to bypass the firm's security protocols. The lack of transparency and restrictions on what information recipients of a TOLA notice may share, potentially with third parties (such as legal counsel) or other employees within the firm may further exacerbate this insider threat risk.

To assess the potential impacts of TOLA on a firm's InfoSec and CyberIns operating and capital costs, it is necessary to know how the firm uses encryption both for its data in motion and data at rest, and as noted earlier, the options for modifying InfoSec and CyberIns strategies to address TOLA. In addition to dividing the data security challenges into those related to data in motion (e.g., electronic communication services like telephony, email, chat, messaging, remote terminal access, etc.) versus data at rest (e.g., confidential data files, security credentials, etc.), it will be important to learn how encryption is used internally by the firm, in its relationships with supply-chain partners like upstream vendors, and with its customers. In each of the six cases, different

[121] Although there are no reliable statistics on what percent of data breaches are due to insider threats, it is widely accepted within the security community that employees who fail to follow security procedures on purpose or by accident are generally believed to be a major source of data breaches, but since most data breaches are not reported and statistics of those reported are incomplete, it is not known what percent are internal. One survey reported that "66% of organizations consider malicious insider attacks or accidental breaches more likely than external attacks" (see https://techjury.net/blog/insider-threat-statistics/#gref, Aug 2020)

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

economic considerations and options may be relevant (and additional cases may be needed to address different product, market, or customer segments).[122]

Fifth, in response to increased national efforts to protect their citizens 'data from foreign surveillance, digital enterprises may be compelled to invest in greater data localisation efforts. For example, following the breakdown of the prior agreement providing a safe-harbour for international data exchanges within the European Union after the Schrems I decision in 2015, Microsoft invested in providing a data-localisation solution in Germany that was subsequently abandoned in 2016 once a new safe-harbour sharing agreement was adopted by the industry.[123]

In abandoning the interim solution, Microsoft signalled the higher costs and reduced customer efficiency resulting of adopting a data-localisation solution. Such solutions increase costs and decrease efficiency by limiting the ability of multinational enterprises to realise scale and scope economies. The cost of updating software (including distributing software patches to address new security issues) is increased because the costs of creating per-market differentiated responses are incurred, along with the added overhead costs associated with managing a more complex updating process.

5.7. Reduction in future growth opportunities due to TOLA

Finally, TOLA may cause firms to re-think their strategic investment plans regarding the development and release of new products and features. This could lead firms to alter their release plans or the pricing for new value-enhancing products and feature sets. It may lead firms to decide not to offer certain products in Australia to protect them from the impact of TOLA. In addition to reducing the firm's future sales and growth potential

[122] The six cases are for (data at rest/data in motion uses) x (Internal/Vendor Relations/Customers).

[123] See "Microsoft Cloud Germany opens using a Data Trustee Model," eWeek, 22 September 2016, available at https://www.eweek.com/cloud/microsoft-cloud-germany-opens-using-data-trustee-model for trade press article from 2016 when Microsoft announced the new arrangement; and https://mspoweruser.com/microsoft-is-discontinuing-the-german-data-trustee-model/ from 2018 when Microsoft announced that it was stopping its data localization effort. Although Microsoft does not identify the cost implications of putting in place and then abandoning its data-trustee model, it is reasonable to anticipate that project cost millions of dollars. Following the most recent Schrems II decision, striking down the safe-harbour that had been put in place a few years after Schrems I, Microsoft reasserted its commitment to protecting the confidentiality of its customer's data (see "New steps to defend your data," Microsoft Blog, 19 November 2019, available at https://blogs.microsoft.com/on-the-issues/2020/11/19/defending-your-data-edpb-gdpr/). See "Schrems I," Baker McKenzie Data Protection, December 2019, available at https://www.bakermckenzie.com/en/-/media/files/insight/publications/2019/12/schrems-ibackgroundv6.pdf for background on the Schrems I decision and for the actual decision, see https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62014CJ0362&from=EN. For July 2020 Schrems II decision, see https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

(or producer surplus), this also denies consumers the benefits of expanded choice and so reduces consumer surplus.

Less investment in new and more secure products may translate into less investment in business capacity, including investment in R&D and product innovation. These investments may be postponed or foregone altogether or may be shifted outside of Australia. In any case, there is a direct and indirect loss to the Australian economy.

5.8. Long-term and global impacts

Although TOLA was passed in 2018, two years later, TOLA remains subject to challenges that render its long-term future uncertain. If TOLA does indeed pose a threat to wider-adoption and security of encryption services, and hence to digital security and hence trust in digital commerce, wider adoption of TOLA-like legislation globally will amplify the adverse impact. On the other hand, if continued challenges to TOLA and concerns over the threat it poses to digital security sufficiently reduce the likelihood that the capabilities enabled by TOLA are utilised, then the adverse impacts described above will be temporary and avoided.

At this stage, it is impossible to forecast which of those scenarios is most likely.

5.9. Summing Up

The direct and indirect economic impacts of TOLA may be viewed as due to TOLA's effects on reducing trust in cybersecurity. The direct costs associated with responding to TOLA Requests and Notices are likely the smallest and least important source of total costs since the number of actual TOLA recipients is likely to remain small.

The indirect effects, however, will include the impact TOLA has on all sectors of the economy as potential direct recipients (which includes all DCPs) and the firms and customers they interact with respond to the increased cyber-risk posed by TOLA. Those total costs are expected to accumulate over time as indirect effects spillover in ripples across the ICT sector in Australia, from the ICT sector to other sectors of the Australian economy, and to global economies and then back again through the feedback loops that comprise our interconnected global economic ecosystem.

The Zurich (2015) study [124] and the AustCyber (2020) report [125] indicate that the potential indirect harms resulting from a threat to digital trust would be measured in the billions of dollars. Although that does not provide even an order of magnitude estimate of the aggregate costs of TOLA, it is sufficient to demonstrate that the potential for nationally, and indeed, internationally consequential harms is large.

There is both anecdotal and partial empirical evidence to suggest that the impact of TOLA may result in significant indirect effects. Solid qualitative arguments also

[124] See Note 92 *supra*.

[125] See Note 93 *supra*.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

suggest that the potential adverse impacts (net costs) of TOLA may indeed be large. However, there is no direct empirical evidence to quantify those effects.

We have scoured publicly available research and have found no relevant empirical studies or adequate data with which to develop empirical estimates. To address this challenge, as part of this project we have undertaken new primary research collecting the opinions of large foreign multi-national technology companies, and a large number and wide array of Australian firms on the likely effects of TOLA on their businesses, whether they believe any of the impacts noted above have been experienced, and if so, any estimates they have of the dollar impacts.

This research involved two elements. First, in-depth videoconference interviews with leading multinational communications providers regulated by TOLA. Second, an anonymous survey of a larger number of communications providers regulated by TOLA and related firms affected by TOLA in Australia. The results of this work are set out in the next chapter. In summary, it supports the conclusion that the net economic impact of TOLA has been negative and that TOLA poses a risk of substantial harms in the future.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

6. Empirical Research Results

As part of our analysis of the economic impact of TOLA, we (1) conducted in-depth confidential interviews by videoconference with nine major firms with operations in Australia that are directly impacted by TOLA (i.e., may be regarded as DCPs whose staff may be recipients of TOLA notices); and (2) launched an anonymous survey of firms operating in Australia that may be directly or indirectly impacted by TOLA.

As we explain further in the summary to this section, the results of the interviews and anonymous survey provide (limited) empirical support for and are wholly consistent with our assessment of the economic impact of TOLA. The high-level insights gained include:

1. Expectation that TOLA will have adverse impact on businesses and their customers that is broad-based (*i.e.*, not just limited to firms in the ICT sectors).
2. That most of the expected harms will be indirect and associated with the threat that TOLA poses for customer and industry partner perceptions of digital trust.
3. Significant uncertainty about TOLA and its effects continues.
4. Direct empirical evidence of economic costs (or benefits) is quite limited, but we attribute that to (a) opacity with which TOLA activities are shrouded due to the non-disclosure provisions; (b) limited time since TOLA's passage and continuing controversy suppressing LEIAs use of TOLA authority; and (c) expectation that impacts are most likely to be indirect and in the future.
5. The limited direct evidence we did observe supports the conclusion that company-specific benefits are likely small, while company-specific costs may be quite large.[126]
6. The available empirical data does not provide a large enough sample to be a reliable basis for estimating the aggregate economic impact of TOLA.

The nine information technology (IT) companies selected for in-depth interviews included six major multinational technology companies with total revenues of just over US$ 1 Trillion.[127] The three other companies included an Australian telecommunications carrier and two Australian electronic service providers. Of the latter, one was an Australian owned exporter and the other a foreign investor and importer of innovative services into Australia.

The anonymous survey was designed and launched, under the direction of LECA, by Clarity Strategic Research (Sydney).[128] The survey was launched during December 2020 and resulted in responses from 79 firms. Although, as we explained earlier, the potential economic impact of TOLA is economy-wide and that it is reasonable to anticipate that the most significant economic impacts may be indirect, we targeted the

[126] Our interview and survey research focused on impacts that respondents had first-hand knowledge of.

[127] To provide some perspective, this total revenue estimate is equivalent to nearly three quarters of Australian GDP.

[128] See https://claritystrategicresearch.com.au/.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

survey to professionals with expertise in IT. We did that since it is reasonable to expect that IT professionals are more likely to be informed about TOLA and the implications of policies impacting the use of encryption technologies. Given the short time and limited resources available to undertake the survey, we were assisted in targeting survey recipients by several Australian trade associations who agreed to assist us in reaching out to their combined membership of 16,000 IT professionals. Those included the Australian Cyber Security Growth Network (AustCyber),[129] the Australian Information Industry Association (AIIA),[130] the Communications Alliance,[131] and the Information Technology Professionals Association (ITPA).[132]

Our survey approach built on the approach of two earlier surveys. The first was launched by AustCyber in 2018 on the eve of the passage of TOLA; while the second was launched by the Communications Alliance and ITPA in 2019 after TOLA had been in force for one year. The survey results reported here offer another snapshot of industry perceptions and experiences two years after passage of TOLA. A key result that emerges from this analysis is the remarkable similarity in terms of what industry participants anticipated would be the effects of TOLA and what they report have been their experiences and expectations going forward. As we will explain further below, the majority of survey respondents expected adverse economic impacts from TOLA before its passage and those expectations have been realised, with further adverse impacts expected in the future.

Before discussing the results from our in-depth interviews and survey, we briefly summarise the results from the two earlier surveys.

6.1. AustCyber (2018)

Prior to TOLA's passage in 2018, AustCyber engaged the Australian Strategic Policy Institute's (ASPI) International Cyber Policy Centre to conduct an online survey of Australian industry. The survey was launched in November 2018 and the results were published in December 2018.[133] The survey was submitted to 512 IT firms with operations in Australia and 63 responses were received. Of those, 76% "reported concern about the bill" and "some of the issues raised as key concerns by respondents were about perceptions and lack of clarity" with respect to what TOLA might require of firms.[134] For example, 57% of respondents expected TOLA to have a negative impact on their business in Australia, and of those, 69% expected the impact to last

[129] See https://www.austcyber.com/.

[130] See https://www.aiia.com.au/.

[131] See https://www.commsalliance.com.au/.

[132] See https://www.itpa.org.au/.

[133] See ASPI (2018), "Perceptions survey: Industry Views on the Economic Implications of the Assistance and Access Bill 2018," Survey funded by AustCyber and executed by ASPI, 22 December 2018 available at https://www.austcyber.com/resources/perceptions-survey.

[134] ASPI (2018), Note 7 *supra*, page 3.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

more than two years;[135] and 65% of the respondents that self-identified as being exporters expected TOLA to have a negative impact on firm exports.[136]

The 76% of respondents that reported they had concerns about TOLA prior to its passage, identified the following key concerns:[137]

Table 6.1: Concerns from AustCyber Survey	%
Lack of clarity around definitions	81%
Potential conflict between Australian laws and foreign countries	73%
Perception that your company's product is less secure	71%
The cost of complying with notices	52%
Erosion of Company capability	50%
The Impact on company revenue	46%
Reduced attractiveness of your company to potential investors	46%
Potential loss all intellectual property	44%
Inability to enforce penalties when companies are established in other countries but provide services to Australia	40%
Brand damage to your company	40%
Impact on supply chain	38%
Reduced attractiveness of your company to potential buyers	33%
Reduced transparency man industry disappoints	33%
Risk of losing existing customers	31%
Other Concerns	23%

Moreover, although the draft legislation indicated that the government would reimburse firms for costs incurred in complying with the legislation, only 5% of the firms expected to be fully reimbursed for TOLA-related compliance costs.[138]

[135] ASPI (2018), Note 7 *supra*, page 8. Only 7% expected a positive impact, 22% expected no impact, and 14% were unsure.

[136] ASPI (2018), Note 7 *supra*, page 7. 51% of respondents reported being exporters, and of those, only 4% expected TOLA to have a positive impact, 17% expected TOLA to have no impact, and 13% were unsure of the impact on firm exports.

[137] ASPI (2018), Note 7 *supra*, page 23. The percentages are computed based on the responses from the 48 firms that indicated they had concerns about TOLA.

[138] ASPI (2018), Note 7 *supra*, page 27.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

6.2. Innovation Australia Survey

The second survey was undertaken in 2019 by Innovation Australia (InnovationAus), an independent publication focused on Australian public policy and business innovation issues,[139] StartupAus, a non-profit advocacy group for start-ups in the tech community in Australia,[140] the Communications Alliance, and ITPA. The results were published in December 2019 after TOLA had been in effect for one year.[141]

The InnovationAus survey was conducted from 5-12 December 2019 to coincide with the anniversary of parliamentary approval of TOLA. The survey received 70 responses from Communications Alliance and ITPA members. Of those, 40% reported that TOLA had resulted in their company having lost business and 51% reported that TOLA had a very negative impact on the reputation of Australian technology companies in global markets.[142] Additionally, following passage of TOLA, 57% of respondents thought their organisation was less likely to perform development operations in Australia.[143]

6.3. Summary of qualitative video-conference interviews

As described, we conducted in depth interviews with nine DCPs that have operations in Australia and had significant experience with how their businesses confronted TOLA and what they thought it meant for the prospects of their business in Australia and beyond.

In all cases, the interviewees were clear that they would oppose any requests from the government that sought to induce them to create "backdoors" in their security processes. Complying with such a request would weaken the security they already provide and would be contrary to their public commitments to their customers and others to protect the legal rights and confidentiality of data under their control. That includes requests that would embed a capability to break or circumvent encryption in any products that currently include that capability or that they would market as having that capability.

---

[139] See https://www.innovationaus.com/.

[140] See https://startupaus.org/.

[141] InnovAus (2019), "Industry Pulse – Encryption Laws – Survey Results," published by InnovAus, StartupAus, Communications Alliance, and ITPA, 18 December 2019, available at https://www.innovationaus.com/wp-content/uploads/2019/12/Encryption_Law_Survey_Results.pdf.

[142] InnovAus (2019), Note 176 *supra*, page 3. In addition to the 51% who thought the reputation impact was very negative, 44% thought it would be somewhat negative, and only 3% expected no impact (0% were positive). Also, 61% of respondents indicated that international or domestic customers had expressed concerns about TOLA.

[143] InnovAus (2019), Note 176 *supra*, page 4. Only 30% expected no impact on development plans and 7% that TOLA would enhance their development plans in Australia. Also, 51% of respondents that reported having development operations in Australia expected TOLA to make it less likely they would increase employment associated with those operations.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

All interviewees also were clear that they already are compliant with lawful government requests for access to data under existing Australian laws and regulations. That said, only one of the interviewees indicated that they saw TOLA as improving the legal situation with respect to government data access. That interviewee saw the safe harbour that TOLA grants for respondents to lawful access requests as an improvement over the pre-TOLA situation. This is because they felt that TOLA provides additional clarity regarding process and liability protection relative to the pre-existing framework, which was more fragmented and hence bureaucratically confusing and burdensome, or at least, that has been their experience thus far. Additionally, the provisions for reimbursing direct costs associated with responding to TOLA requests has worked well for them thus far. This single responding company who was supportive of TOLA does not see TOLA as potentially posing a risk of requiring them to break encryption, disclose confidential source code, or significantly threaten their brand messaging to enterprise or consumer customers in Australia or abroad.

The other eight responding companies, however, held negative impressions of TOLA. They saw it as a potential threat to the security and growth in demand for the range of information services they offer and could impose higher costs in addressing those amplified security risks. A key reason for this perception was the consensus conclusion that TOLA's breadth, inadequacy in the oversight provisions, and ambiguity in the terms of what might be required as well as the lack of transparency, posed a threat to the security of digital data at rest or in motion. The comments offered echoed many of the same concerns raised as part of the consultation prior to TOLA's passage[144] and reflected in the subsequent reviews, including the review by the Independent National Security Legislation Monitor (INSLM) that was published in July 2020.[145] Although the Australian Government has sought to address many of these concerns as being unfounded "myths,"[146] the INSLM review recommended a range of reforms to strengthen TOLA oversight and further clarification of some of the terms of TOLA.

In spite of continued government assurances that TOLA would not be abused and that its application would be narrowly constrained to apply only in a limited set of severe contexts such as those involving the prosecution of egregious crimes like international terrorism, child sexual abuse material, or human trafficking, many respondents were not fully convinced, having witnessed the failure of analogous oversight provisions applied in other contexts in Australia and abroad. There was a concern that the capability to expand government authority to access confidential data in ambiguous

[144] See https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/TelcoAmendmentBill2018/Submissions.

[145] See "Trust but Verify: a report concerning the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 and related matters," Australian Independent National Security Monitor (INSM), June 2020, available at https://www.inslm.gov.au/sites/default/files/2020-07/INSLM_Review_TOLA_related_matters.pdf.

[146] See "Assistance and Access: Common myths and misconceptions," available at https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/myths-assistance-access-act.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

ways would require continued vigilance (and increased cost for DCPs) to protect against mission-creep and abuses that the oversight provisions are intended to prevent.

During the lead up to the passage of TOLA and in the first period following its passage, several respondents highlighted the concern that TOLA might subject them to an untenable position (because of the confusing and restrictive provisions regarding what information about TOLA requests might be shared by recipients of such requests). For example, there was the concern that an employee that received a TOLA notice might be unable to share such information with top management without facing legal sanctions. That scenario would expose employees and their company to unacceptable legal liability.

Subsequent discussions with regulatory authorities responsible for TOLA by the respondents have led them to discount that risk; however, the fact that it even arose is indicative of the confusion and legal (and hence business) uncertainty that TOLA has prompted since it was first proposed and that continues to this day. Additionally, this outlook could change as leadership and personnel within those regulatory authorities change over and hold differing views, as it is not explicit in the language of the Act.

Several respondents indicated that a requirement to break or circumvent encryption for one of their products would be infeasible to do in a way that targeted an individual, and hence would introduce a systemic vulnerability that would spillover to adversely impact the security of the product or service for other users. This is especially true of DCPs that rely on and provide services that are based on open source or depend on encryption and security protections that are not customisable on an individual user basis. Some DCPs may also rely on services of this type, even if they themselves do not provide them.

Were such a provider to be required to break the security of a product under TOLA, that could constitute an existential threat that would necessitate the company pulling its operations and product/service sales out of Australia. A number of the respondents who recognised that risk commented that they would oppose complying with any such request to the full extent of their legal abilities to appeal and challenge the request, escalating such efforts to whatever level needed.

Regardless of the reality of certain extreme scenarios of how TOLA might be abused, the mere perception that it weakens security was a worry for DCPs. Their concern was that stakeholders would view DCPs' products and services as less secure because they were subject to TOLA, and this reduced security could lead to data leakages and security breaches, not just in Australia, but elsewhere. The perception that TOLA represents bad security policy was viewed by all but one of the respondents to our interviews as a potential threat to their brands that they would need to carefully monitor and consider in their future strategic plans for developing and providing security-enabled products for sale in Australia.

Multiple respondents noted that TOLA, and what it signalled about a potentially worsening climate for government interference and regulation of security products, would be a factor in their future plans to build their development and sales operations

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

in Australia. For example, it would be a factor in their selection of vendors for services such as data centres located in Australia that would be subject to TOLA. Moreover, since the recipients of TOLA notices are legally precluded from sharing information about the TOLA notices they receive, their customers might not know which DCPs had received such notices and what their responses may have been.

One interviewee is an Australian-based DCP that was growing rapidly and looking to expand into international markets that it perceived as offering a billion dollar opportunity. After TOLA, the adverse brand impact on their products led them to abandon plans for expanding their export sales, foreclosing an important growth opportunity for that company. The interviewee noted that they lost business with existing customers who decided to move their business to other providers whose offerings were believed to be beyond the reach of TOLA.

Several respondents noted that the concern over the security of customer data had been raised by their customers and was a factor they had to address in thinking about future plans. They have had to reassure customers of their commitments to protecting the confidentiality of data.

With the exception of the one case noted above, most respondents indicated that the costs imposed by TOLA thus far have not been excessive, although most expressed skepticism that the reimbursement provisions for TOLA-related expenses would immunise them against adverse cost impacts. The respondents expected that the most significant TOLA-related costs would likely be indirect (e.g., damage to brand image or reduced demand for Australian DCP services or products) rather than direct (e.g., employee resources devoted to complying with a specific request).

Most respondents had adopted additional TOLA-related process protections (with attendant costs),[147] but most did not indicate that TOLA had already resulted in their changing the design of their product offerings or in their staffing decisions with respect to locating those in Australia or abroad. However, the additional TOLA-related process protections indicate that those sorts of decisions may become factors in the future. Several respondents commented that the lack of evidence of significant direct costs from TOLA was not surprising in light of the limited exercise in TOLA authority since TOLA's passage. They attributed that to the fact that it takes time for the effects of new legislation to be felt, along with continuing controversy about and calls for amendments to TOLA.

Moreover, a number saw TOLA as an unfortunate step in a direction that, were it to become more widespread with copycat legislation being adopted more widely, would further amplify the global threat to greater data security that TOLA already poses.

[147] For example, several respondents mentioned that those process protections included adding another layer of process review for investment and product development plans to address the potential impact of TOLA.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

Finally, in light of the July 2020 decision (Schrems II)[148] in the European Union, striking down the safe-harbour Privacy Shield solution that had been adopted to protect international data sharing arrangements from running afoul of European Union data protection laws, a number of respondents indicated that they were concerned that TOLA might pose a risk to international data flows to and from Australia. Any such threat, if it proves warranted, could impose significant costs on the smooth operation of global data and communication markets.

6.4. LECA Survey Results

6.4.1. Respondents to the online survey

As noted above, there were 79 respondents to the survey conducted by LECA with assistance from Clarity Strategic Research. Similar to the composition of the two earlier surveys noted above, the respondents represented firms with operations in Australia from across multiple sectors of the economy and representing a range of sizes (measured either on the basis of employees or revenues):

- 54 of the firms were headquartered in Australia (68% or 54/79);
- Respondent companies ranged in size from less than 10 employees (34% or 27/79) to greater than 500 employees (28% or 22/79);
- A sizeable proportion reported that all of their employees were located in Australia (46% or 36/79), while another smaller, but still sizeable proportion (27% or 21/79) reported less than half of their employees as being located in Australia.
- When classified on the basis of total firm revenues, 43% (or 34/79) of the firms are small (<AU$5m) while 13% (or 10/79) are large (>AU$5,000m).
- Not surprisingly, most of the respondents identified their firms as operating in IT-related businesses (54% or 43/79), with many of those active across multiple lines of IT business.
- Of the firms that were not in IT-related businesses (43% or 34/79), the respondents identified their firms as operating in Services (44% or 15/34), Public Administration & Safety (18% or 6/34) or other sectors (38% or 13/34), ranging from Manufacturing to Education.[149]
- The job titles of the respondents indicated that virtually all, if not all, were involved in IT-related jobs, which is not surprising given who the survey was sent to.

These results are summarised in the following tables:

Table 6.2: QA1i: Where is the company headquartered?

	Count	%
Australia	54	68%
Elsewhere	23	29%

[148] See "The 'Schrems II' decision: EU-US data transfers in question," July 16, 2020, available at https://iapp.org/news/a/the-schrems-ii-decision-eu-us-data-transfers-in-question/.

[149] Two (3% of the 79) respondents did not provide an answer.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

No answer	2	3%
Total	79	100%

Table 6.3: QA3i: How many employees globally (approximately)?		
Global Employees (#)	Count	%
No answer	10	13%
0-10	27	34%
11-499	20	25%
500+	22	28%
Total	79	100%

Table 6.4: Share Employees in Australia	Count	%
No answer	12	15%
10% or less	16	20%
10<%<100	15	19%
100%	36	46%
Total	79	100%
0%	4	5%
<50%	21	27%

Table 6.5: Is the firm an IT business?		
Sector	Count	%
No answer	2	3%
IT Sector	43	54%
Not-IT	34	43%
Total	79	100%

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

Table 6.5B: Headquarter location and line of business				
	Line of Business			
Location Headquarters	ICT	Not ICT	No Answer	Total
Australia	31 (39%)	23 (29%)	0 (0%)	54 (68%)
Not in Australia	12 (15%)	10 (13%)	1 (1%)	23 (29%)
No Answer	0 (0%)	1 (1%)	1 (1%)	2 (3%)
Total	43 (54%)	34 (43%)	2 (3%)	79 (100%)

Table 6.6: IT Lines of Business		
	Code	Count
Telecommunications Network Operations, Equipment & Services	1-3, 10,13	18
Internet Service Provider, Web Search Portals, other Internet Services	4-5	7
Electronic Storage Services	6	6
Software developer, supplier	7-8	25
Computer equipment manufacturing and sales	9-12, 13-14	17
Other IT (specify)	97	13
Don’t know, won’t say	98-99	3
Total		89

Table 6.7: Non-IT firm Lines of Business			
Sector	Code	Count	%
Services	10, 12, 18	12	46%
Public Admin & Safety	14	6	23%
Other (Manufacturing, Construction, Education)	3, 5, 7, 15	8	31%
Total		26	100%

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

6.4.2. Importance of encryption services for business

Survey respondents overwhelmingly indicated that encryption services and capabilities were very or quite important for their businesses in multiple ways -- for both communications (data in motion) and stored data (data at rest) for use internally and in business dealings with upstream vendors/suppliers and customers. 96% (or 76/79) of respondents indicated that encryption services were very or quite important for at least one usage category.[150] Moreover Table 6.8 demonstrates that well over 85% (or 67/79) of respondents regarded encryption services and capabilities as very or quite important for most of the usage contexts taken separately, and of those, well over 53% (or 42/79) responded that encryption services and capabilities were very important.

Additionally, respondents indicated that they acquired the needed encryption capabilities in a variety of ways: sometimes developing them in-house and sometimes relying on third-party vendors of general purpose products and services (i.e., encryption capabilities may be an embedded feature of an IT product or service) or specialty encryption service providers. The methods of acquiring the capabilities may differ across use (i.e., data in motion or data at rest, used internally, with vendors/suppliers, or with customers). A number of respondents used different approaches in the different contexts and sometimes used multiple approaches in particular contexts. Although our anonymous survey results do not allow us to track co-dependencies among firms in our survey (i.e., some respondents may be consumers and/or providers of encryption services to other respondents), it is clear that the use of encryption capabilities and services is widespread across different IT businesses and across the non-IT businesses in our survey.

These results are indicative of the wide-spread dependence placed on encryption services by all kinds of businesses across the economy and of the potentially tangled web of repercussions that may be transmitted across firms in Australia and internationally if the encryption capabilities of even a subset of firms are threatened. The propagation of such adverse effects through the economy could amplify and augment the adverse direct impact. Unfortunately, the small number of survey responses received and the lack of better data on the trade in goods and services dependent on encrypted capabilities does not allow us to estimate or model the ways in which direct and indirect effects might reverberate through the economy.

Table 6.8: How important are encryption services and capabilities for your business?

	Very or quite important	Not very (at all) important	Don't know or no answer	Total	% Col (a) who responded

[150] Only one respondent indicated that they do not use encryption services, only one other respondent indicated that encryption services were not either very or quite important for at least one of the usage categories, and only one other respondent preferred not to say in all of the usage categories, representing just 4% (or 3/76) of the total respondents.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

		or not used			Very important
	(a)	(b)	(c)	(a)+(b)+(c)	
Internal company communications	85%	14%	1%	100%	53%
Internal company data holdings	92%	6%	1%	100%	73%
Communications (data in motion) with vendors and suppliers	90%	9%	1%	100%	59%
Data holdings (data at rest) held by vendors and suppliers	91%	6%	3%	100%	70%
Communications (data in motion) with your customers	91%	8%	1%	100%	65%
Data holdings (data at rest) in products/services your company provides to its customers	87%	11%	1%	100%	71%

6.4.3. TOLA awareness, familiarity and attitude

Of the 79 Respondents, 58 indicated they had heard of TOLA. Those 58 respondents are mostly from firms with headquarters in Australia (68%) whose primary business is IT-based (60% or 35/58); and 40% (or 23/58) of the respondents indicated that they were very or quite familiar with the TOLA legislation.

Table 6.9: TOLA Awareness of Respondents by Location Headquarters

	Aware	Not Aware/ No Answer	Total
Australia	42 (53%)	12 (15%)	54 (68%)
Not in Australia	16 (20%)	9 (11%)	25 (32%)
Total	**58 (73%)**	21 (27%)	79 (100%)

Table 6.10: TOLA Awareness of Respondents by Type of Business

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

	Aware	Not Aware/ No Answer	Total
IT	35 (44%)	8 (10%)	43 (54%)
Not IT	23 (29%)	13 (16%)	36 (46%)
Total	**58 (73%)**	21 (27%)	79 (100%)

Table 6.11: Level of Familiarity with TOLA		
Very/Quite familiar	23	40%
Not very familiar	29	50%
Not familiar	4	7%
No answer	2	3%
Total	58	100%

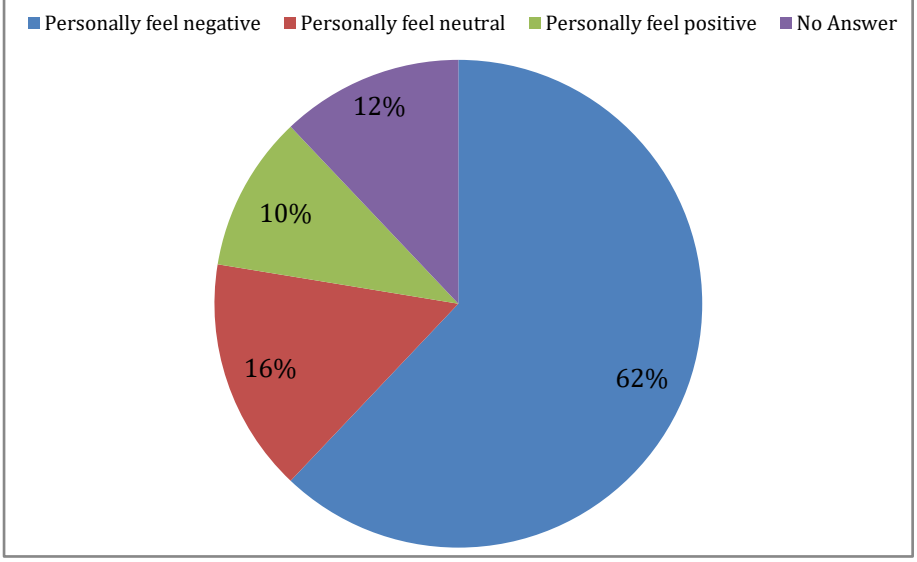
6.4.4. Respondent attitudes towards TOLA

Amongst those aware of TOLA, a large proportion (62% or 36/58) feel very or quite negative about the changes it made to the *Telecommunications Act 1997*. Only 10% (or 6/58) felt positively. The graph below summarises the familiarity and attitudes relating to TOLA of the 58 respondents who were aware of the Act.

Table 6.12: Respondents' feelings about TOLA	
Very Positive	0%
Quite Positive	10%
Neutral	16%
Quite Negative	26%
Very Negative	36%
No Answer	12%
Total	100%

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

Figure 6.1
For those 58 Cases aware of TOLA ACT



When asked about how respondents thought TOLA impacted various policy issues, the majority of respondents believed that TOLA has had an adverse impact on Australia's foreign relations and the security and integrity of digital data, and of greatest importance here, an adverse impact on Australia's economy. Respondents had mixed feelings regarding the impact on Australia's national security. The most significant positive impact of TOLA (but still far less than a majority) was on enforcing criminal law in Australia (see Table 6.13).

Table 6.13: Respondent expectations about impact of TOLA on issues

	Negative	No Impact	Positive	No Answer	Total
Australia's national security	33%	22%	24%	21%	100%
Australia's foreign relations	53%	7%	9%	31%	100%
Australia's national economic well-being	52%	10%	16%	22%	100%
The security and integrity of information that is processed, stored or communicated by electronic or similar means	59%	12%	10%	19%	100%
Enforcing the criminal law in Australia	12%	29%	34%	24%	100%
Enforcing the criminal law in other countries	10%	50%	7%	33%	100%

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

6.4.5. TOLA impacts on respondents 'businesses

When asked about whether TOLA had impacted their businesses in various ways, 41% of the respondents answered that TOLA had impacted their business in one or more ways (Table 6.14A), and, on average 18% of respondents who knew about TOLA (58 of the 79) answered that TOLA had impacted their business for each of the categories (Table 6.14B).

Table 6.14A: Firms reporting multiple category impacts

No impact	59%
One category of impact	5%
Two or more categories of impact	36%

Table 6.14B: Has TOLA had an impact on business?

	Yes impact	No impact	Don't know	No Answer	Total
Sales	16%	47%	31%	7%	100%
Reputation Business	14%	45%	36%	5%	100%
Vendor Relations	16%	52%	28%	5%	100%
Customer Relations	16%	48%	31%	5%	100%
Product Dvlp, Marketing Decisions	31%	43%	22%	3%	100%
OPEX/CAPEX	21%	45%	33%	2%	100%
Other areas Business	21%	40%	36%	3%	100%
Average	19%	46%	31%	4%	

When further queried about whether the impacts had been positive or negative to date and about respondents 'expectations for impacts in the future on a range of business issues, respondents who had seen an impact, once again highlighted the broad range of impacts (see Table 6.15A, 6.15B, and 6.15C). Although most firms have not reported experiencing an impact (Table 6.14), of those that do in a category, those that experienced a negative impact outnumber those that experienced a positive impact in every category. Moreover, negative effects are predicted to continue into the future across all 15 impact areas, and for the great majority of negative effects (11 of the 15 impact areas or for 73%) there are more firms expecting negative effects in the future than had experienced negative effects to date (Table 6.15C) – rising from 18% to 20%. Thus, the survey respondents 'expectations are consistent with the view that economic

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

impacts will continue, or perhaps even get worse, in the future. Finally, overall, 36% (or 21/58) of the firms experienced a negative impact on their business in one or more of the areas to date and expected in the future (Table 6.15D).

Table 6.15A: Firms that Experienced Impact to date (since 2018)

Share of Firms that Experiences Impact	Negative	No Impact	Positive	No Answer	Total
Your total revenue globally	10%	12%	3%	74%	100%
Your revenue from encrypted services globally	9%	16%	2%	74%	100%
The global operating costs of your business, including compliance and remediation	16%	14%	2%	69%	100%
Your global investment in encrypted services	21%	9%	3%	67%	100%
The global level of your investment and funding	17%	9%	3%	71%	100%
Your global expenditure on innovation strategy in relation to encrypted services	21%	7%	5%	67%	100%
Your global investment in new product development	22%	7%	2%	69%	100%
Your global Research & Development expenditure	19%	9%	3%	69%	100%
The global value of your brand or reputation	19%	10%	3%	67%	100%
The global value of your other Intellectual Property (patents, copyright, etc.)	14%	14%	2%	71%	100%
Your ability globally to attract good staff to work for your business	12%	17%	2%	69%	100%
Your ability globally to buy the encrypted products and services your business needs	10%	17%	3%	69%	100%
The confidentiality, security, or privacy of your encrypted services globally	28%	9%	2%	62%	100%
The risk environment for your business globally	36%	2%	2%	60%	100%
Levels of employment in encrypted services globally	14%	9%	3%	74%	100%

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

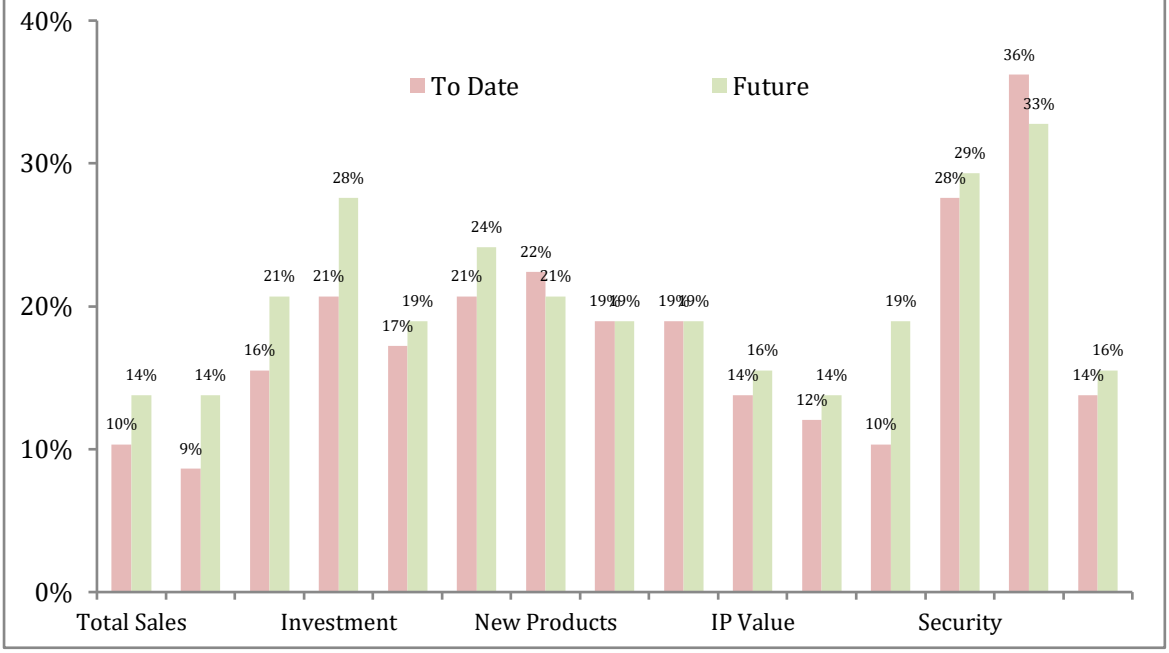
Table 6.15B: Firms that Expect to Experience Impact in Future					
Share of Firms that Experiences Impact	Negative	No Impact	Positive	No Answer	Total
Your total revenue globally	14%	7%	7%	72%	100%
Your revenue from encrypted services globally	14%	9%	2%	76%	100%
The global operating costs of your business, including compliance and remediation	21%	10%	2%	67%	100%
Your global investment in encrypted services	28%	9%	0%	64%	100%
The global level of your investment and funding	19%	9%	3%	69%	100%
Your global expenditure on innovation strategy in relation to encrypted services	24%	9%	0%	67%	100%
Your global investment in new product development	21%	7%	3%	69%	100%
Your global Research & Development expenditure	19%	12%	2%	67%	100%
The global value of your brand or reputation	19%	9%	5%	67%	100%
The global value of your other Intellectual Property (patents, copyright, etc.)	16%	14%	0%	71%	100%
Your ability globally to attract good staff to work for your business	14%	16%	5%	66%	100%
Your ability globally to buy the encrypted products and services your business needs	19%	12%	2%	67%	100%
The confidentiality, security, or privacy of your encrypted services globally	29%	5%	3%	62%	100%
The risk environment for your business globally	33%	2%	2%	64%	100%
Levels of employment in encrypted services globally	16%	7%	3%	74%	100%

Table 6.15C: Firms that experienced to date or expect to experience in the future Negative impacts of TOLA for their business		
Share of Firms that Experiences Impact	To date	Future
Your total revenue globally	10%	14%

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

Your revenue from encrypted services globally	9%	14%
The global operating costs of your business, including compliance and remediation	16%	21%
Your global investment in encrypted services	21%	28%
The global level of your investment and funding	17%	19%
Your global expenditure on innovation strategy in relation to encrypted services	21%	24%
Your global investment in new product development	22%	21%
Your global Research & Development expenditure	19%	19%
The global value of your brand or reputation	19%	19%
The global value of your other Intellectual Property (patents, copyright, etc.)	14%	16%
Your ability globally to attract good staff to work for your business	12%	14%
Your ability globally to buy the encrypted products and services your business needs	10%	19%
The confidentiality, security, or privacy of your encrypted services globally	28%	29%
The risk environment for your business globally	36%	33%
Levels of employment in encrypted services globally	14%	16%
Average (of rows)	18%	20%

Figure 6.2
Negative Impact Past and Future
% of Firms Australian and Foreign



Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

Table 6.15D: Number of categories negative impacts experienced or expected		
Number of negative impact (globally and in Australia) Total cases aware of TOLA = 58	Number of Cases To date	Number of Cases in Future
0 (include No Answer) in all categories	37 (64%)	37 (64%)
1 of 15 categories	0 (0%)	0 (3%)
2 of 15 categories	2 (3%)	0 (0%)
3 of 15 categories	2 (3%)	2 (2%)
4 or more of 15 categories	17 (29%)	18 (31%)
Total	58 (100%)	58 (100%)
Negative impact in at least 1 of the 15 categories	21 (36%)	21 (36%)

6.5. Empirical Research Conclusions

In summary, the hypothetical economic risks that we outlined in Chapter 5 were echoed by the ICT firms we interviewed and in the responses to our surveys. In both cases, there was empirical support for the view that TOLA poses an economic threat to the business prospects of ICT firms and to the Australian and global economy.

The evidence was also indicative of the lack of empirical evidence thus far of significant economic costs (and even more so, of benefits) that may be directly attributed to TOLA. This lack of empirical evidence, however, is *not* evidence of a lack of an effect. Although it was worth looking for empirical evidence of costs having been incurred since 2018, we would have been surprised to find such evidence in light of the very limited TOLA activity that has been reported and the continuing challenges and controversy that render TOLA's future uncertain. Additionally, the non-disclosure rules and secrecy shrouding TOLA activity provide a significant barrier to collecting evidence of TOLA's economic impacts. Nevertheless, the limited evidence collected is telling. The fact that the single interviewee respondent that viewed the impact of TOLA mostly favourably saw its principal effect as rationalising existing legislation on government lawful access to digital data is consistent with the view that the direct benefits of TOLA are likely small. Conversely, the single respondent that was able to quantify the economic harm suffered by that respondent as a result of TOLA estimated that harm as being on the order of one billion dollars of lost export income is consistent with the expectation that the potential direct economic harms can be quite large.

Moreover, the size of the anonymous survey and the challenges that reliance on survey data impose on inferring economic impacts limit our ability to quantify the magnitude of the economic effects. However, the results are consistent with what was observed in the earlier surveys and demonstrates that the concerns that existed before TOLA passed remain concerns today; and, if those concerns are realised, then the adverse economic impacts could be extensive.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

The survey responses highlight the fact that the adverse impacts are broadly shared among both ICT and non-ICT firms and that many firms still do not understand the threat that TOLA poses for their business.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

7. Appendices Acronyms, Abbreviations & Definitions

7.1. Acronyms, Abbreviations & Definitions

- ASIO Act. The Australian Security Intelligence Organisation Act 1979
- ASIO. The Australian Security Intelligence Organisation, which is included in the list of Australian government agencies that can issue requests and/or notices under TOLA.
- Cth stands for Commonwealth, and used to distinguish Commonwealth legislation from State legislation
- DCP. Designated Communications Provider. DCPs, are a broadly construed construct under TOLA covering the entities to which TOLA applies, see the list of DCP categories in 317C of TOLA copied below.
- INSLM. Independent National Security Legislation Monitor (link), issued TOLA review report July 20, 2020 (link).
- PJCIS. Parliamentary Joint Committee on Intelligence and Security conducted an inquiry in TOLA before its enactment, and has since undertaken further reviews.
- TOLA. The *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, also known as the Encryption Act or the Assistance & Access Act (link). TOLA has been subject to review by INSLM. TOLA comprised of 5 schedules, with Schedule 1 (related to removal and circumvention of encryption or exceptional access) being focus of our work.
- TAR, TAN, TCN are three types of notices that may be issued under TOLA either orally or in writing (317H)
  - TAR = Technical Assistance Request may ask DCP to undertake voluntary actions (317L)
  - TAN = Technical Assistance Notice directs DCP to provide technical assistance (317M)
  - TCN = Technical Capability Notice directs DCP to undertake specific actions, including enabling a capability (317T)
- TIA. The Telecommunications (Interception and Access) Act 1979
- TA. The *Telecommunications Act 1997*
- SD Act. The Surveillance Devices Act 2004 (SD Act),
- MACMA. The Mutual Assistance in Criminal Matters Act 1987 (),
- ASIO Act. The Australian Security Intelligence Organisation Act 1979

7.2. Definitions from TOLA

317B Definitions

electronic protection includes:

a) authentication; and

b) encryption.

target technology:

(a) for the purposes of this Part, a particular carriage service, so far as the service is used, or is likely to be used, (whether directly or indirectly) by a particular person, is a ***target technology*** that is connected with that person; ands

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

(b) for the purposes of this Part, a particular electronic service, so far as the service is used, or is likely to be used, (whether directly or indirectly) by a particular person, is a ***target technology*** that is connected with that person; and

(c) for the purposes of this Part, particular software installed, or to be installed, on:
(i) a particular computer; or
(ii) a particular item of equipment;
used, or likely to be used, (whether directly or indirectly) by a particular person is a ***target technology*** that is connected with that person; and

(d) for the purposes of this Part, a particular update of software that has been installed on:
(i) a particular computer; or
(ii) a particular item of equipment;
used, or likely to be used, (whether directly or indirectly) by a particular person is a ***target technology*** that is connected with that person; and

(e) for the purposes of this Part, a particular item of customer equipment used, or likely to be used, (whether directly or indirectly) by a particular person is a ***target technology*** that is connected with that person; and

(f) for the purposes of this Part, a particular data processing device used, or likely to be used, (whether directly or indirectly) by a particular person is a ***target technology*** that is connected with that person.

For the purposes of paragraphs (a), (b), (c), (d), (e) and (f), it is immaterial whether the person can be identified.

Designated Communications Providers

317C Designated communications provider etc.

For the purposes of this Part, the following table defines:

(a) ***designated communications provider***; and

(b) the ***eligible activities*** of a designated communications provider.

Designated communications provider and eligible activities		
Item	**A person is a designated communications provider if ...**	**... and the eligible activities of the person are ...**
1	the person is a carrier or carriage service provider	(a) the operation by the person of telecommunications networks, or facilities, in Australia; or (b)

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

2	the person is a carriage service intermediary who arranges for the supply by a carriage service provider of listed carriage services	(a) the arranging by the person for the supply by the carriage service provider of listed carriage services; or (b) the operation by the carriage service provider of telecommunications networks, or facilities, in Australia; or (c) the supply by the carriage service provider of listed carriage services
3	the person provides a service that facilitates, or is ancillary or incidental to, the supply of a listed carriage service	the provision by the person of a service that facilitates, or is ancillary or incidental to, the supply of a listed carriage service
4	the person provides an electronic service that has one or more end-users in Australia	the provision by the person of an electronic service that has one or more end-users in Australia
5	the person provides a service that facilitates, or is ancillary or incidental to, the provision of an electronic service that has one or more end-users in Australia	the provision by the person of a service that facilitates, or is ancillary or incidental to, the provision of an electronic service that has one or more end-users in Australia
6	the person develops, supplies or updates software used, for use, or likely to be used, in connection with: (a) a listed carriage service; or (b) an electronic service that has one or more end-users in Australia	(a) the development by the person of any such software; or (b) the supply by the person of any such software; or (c) the updating by the person of any such software
7	the person manufactures, supplies, installs, maintains or operates a facility	(a) the manufacture by the person of a facility for use, or likely to be used, in Australia; or (b) the supply by the person of a facility for use, or likely to be used, in Australia; or (c) the installation by the person of a facility in Australia; or (d) the maintenance by the person of a facility in Australia; or (e) the operation by the person of a facility in Australia

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

Designated communications provider and eligible activities		
Item	**A person is a designated communications provider if ...**	**... and the eligible activities of the person are ...**
8	the person manufactures or supplies components for use, or likely to be used, in the manufacture of a facility for use, or likely to be used, in Australia	(a) the manufacture by the person of any such components; or (b) the supply by the person of any such components
9	the person connects a facility to a telecommunications network in Australia	the connection by the person of a facility to a telecommunications network in Australia
10	the person manufactures or supplies customer equipment for use, or likely to be used, in Australia	(a) the manufacture by the person of any such customer equipment; or (b) the supply by the person of any such customer equipment
11	the person 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	(a) the manufacture by the person of any such components; or (b) the supply by the person of any such components
12	the person: (a) installs or maintains customer equipment in Australia; and (b) does so otherwise than in the capacity of end-user of the equipment	(a) any such installation by the person of customer equipment; or (b) any such maintenance by the person of customer equipment
13	the person: (a) connects customer equipment to a telecommunications network in Australia; and (b) does so otherwise than in the capacity of end-user of the equipment	any such connection by the person of customer equipment to a telecommunications network in Australia

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

14	the person is a constitutional corporation who: (a) manufactures; or (b) supplies; or (c) installs; or (d) maintains; data processing devices	(a) the manufacture by the person of data processing devices for use, or likely to be used, in Australia; or (b) the supply by the person of data processing devices for use, or likely to be used, in Australia; or (c) the installation by the person of data processing devices in Australia; or (d) the maintenance by the person of data processing devices in Australia

Designated communications provider and eligible activities		
Item	**A person is a designated communications provider if ...**	**... and the eligible activities of the person are ...**
15	the person is a constitutional corporation who: (a) develops; or (b) supplies; or (c) updates; software that is capable of being installed on a computer, or other equipment, that is, or is likely to be, connected to a telecommunications network in Australia	(a) the development by the person of any such software; or (b) the supply by the person of any such software; or (c) the updating by the person of any such software

Note 1: See also sections 317HAA, 317MAA and 317TAA (provision of advice to designated communications providers).
Note 2: See also section 317ZT (alternative constitutional basis).

317E Listed acts or things

(1) For the purposes of the application of this Part to a designated communications provider, ***listed act or thing*** means:
  (a) removing one or more forms of electronic protection that are or were applied by, or on behalf of, the provider; or
  (b) providing technical information; or
  (c) installing, maintaining, testing or using software or equipment; or
  (d) ensuring that information obtained in connection with the execution of a warrant or authorisation is given in a particular format; or
  (da) an act or thing done to assist in, or facilitate:

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

(i) giving effect to a warrant or authorisation under a law of the Commonwealth, a State or a Territory; or
(ii) the effective receipt of information in connection with a warrant or authorisation under a law of the Commonwealth, a State or a Territory; or

(e) facilitating or assisting access to whichever of the following are the subject of eligible activities of the provider:
(i) a facility;
(ii) customer equipment;
(iii) a data processing device;
(iv) a listed carriage service;
(v) a service that facilitates, or is ancillary or incidental to, the supply of a listed carriage service;
(vi) an electronic service;
(vii) a service that facilitates, or is ancillary or incidental to, the provision of an electronic service;
(viii) software used, for use, or likely to be used, in connection with a listed carriage service;
(ix) software used, for use, or likely to be used, in connection with an electronic service;
(x) software that is capable of being installed on a computer, or other equipment, that is, or is likely to be, connected to a telecommunications network; or

(f) assisting with the testing, modification, development or maintenance of a technology or capability; or

(g) notifying particular kinds of changes to, or developments affecting, eligible activities of the designated communications provider, if the changes are relevant to the execution of a warrant or authorisation; or

(h) modifying, or facilitating the modification of, any of the characteristics of a service provided by the designated communications provider; or

(i) substituting, or facilitating the substitution of, a service provided by the designated communications provider for:
(i) another service provided by the provider; or
(ii) a service provided by another designated communications provider; or

(j) an act or thing done to conceal the fact that anything has been done covertly in the performance of a function, or the exercise of a power, conferred by a law of the Commonwealth, a State or a Territory, so far as the function or power relates to:
(i) enforcing the criminal law, so far as it relates to serious Australian offences; or
(ii) assisting the enforcement of the criminal laws in force in a foreign country, so far as those laws relate to serious foreign offences; or
(iii) the interests of Australia's national security, the interests of Australia's foreign relations or the interests of Australia's national economic wellbeing.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

(2) Paragraph (1)(j) does not apply to:
(a) making a false or misleading statement; or
(b) engaging in dishonest conduct.

Terms of Compliance

317ZK Terms and conditions on which help is to be given etc.

Scope

1) This section applies if a designated communications provider is subject to a requirement under:
   a. a technical assistance notice; or
   b. a technical capability notice;

……

Terms and conditions

4) The designated communications provider must comply with the requirement on such terms and conditions as are:
   a. agreed between the following parties:
      i. the provider;
      ii. the applicable costs negotiator; or
   b. failing agreement, determined by an arbitrator appointed by the parties.

317V Decision making criteria

The Attorney General must not give a technical capability notice to a designated communications provider unless:

(a) the Attorney General is satisfied that the requirements imposed by the notice are reasonable and proportionate; and
(b) the Attorney General is satisfied that compliance with the notice is:
(i) practicable; and
(ii) technically feasible.

Note: See also section 317ZAA.

A provider is entitled to seek an assessment for compliance with the above and in carrying out an assessment in relation to a technical capability notice the assessors must:

(a) consider:
(i) whether the proposed technical capability notice would contravene section 317ZG; and
(ii) whether the requirements imposed by the proposed technical capability notice are reasonable and proportionate; and
(iii) whether compliance with the proposed technical capability notice is practicable; and
(iv) whether compliance with the proposed technical capability notice is technically feasible; and
(v) whether the proposed technical capability notice is the least intrusive measure that would be effective in achieving the

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

legitimate objective of the proposed technical capability notice; and

(b) give the greatest weight to the matter mentioned in subparagraph (a)(i).

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

8. About the Authors

8.1. George Barker

George Barker is a Director of LECA and an expert in economic analysis of law and regulation. Currently an Honorary Associate Professor at the Australian National University (ANU), and a member of Wolfson College, University of Oxford. He has taught regulatory economics to staff of Australian regulators and regulated firms, conducted public good research and given expert economic advice and testimony on a wide range of matters relating to regulation of the information and communications technology industry, (e.g. regulation of the internet, spectrum allocation and use, carriers, and carriage services, and network access), and utility industries (e.g. energy, and transport), as well as competition law, intellectual property, contracts, and tax law affecting a wide variety of other industries in Australia, Asia Pacific, North America, and Europe. Dr Barker has contributed to numerous competition and regulatory policy reviews in Australia, the Asia Pacific, North America and Europe. Dr Barker has given expert testimony globally before regulatory agencies, and before courts reviewing regulatory decisions on appeal - as well in arbitration cases in the Hague - and before Ministers and Parliaments engaged in inquiries, and reform processes in Australia, the UK, EU, New Zealand, China, Korea, Japan, and the Philippines. He has for example given expert testimony to US Federal Courts, the Federal Court of Australia, the High Court of New Zealand and his analysis has been cited in the UK House of Lords, by the High Court of England and Wales and by the European Commission. He was Director of the Centre for Law and Economics at Australian National University from 1997-2017 and was awarded the Olin Fellowship in Law and Economics at Cornell University USA in 2000, and has been a Visiting Fellow at the London School of Economics (LSE) (2015-2018), at the Centre for Law and Economics at University College London (2010-2015), at Oxford University 2008, and at the British Institute of International and Comparative Law (BIICL) (2009-present). He was Chief Analyst and Economic Advisor at the NZ Treasury 1984 -1997. He is on the Editorial Board of the European Journal of Law and Economics. He gained a DPhil in Economics from Oxford University in 1992, and holds a Master of Economics (Hons) and a Bachelor of Laws.

8.2. William Lehr

William Lehr is a telecommunications and Internet industry economist and consultant with over twenty-five years of experience. He regularly advises senior industry executives and policymakers in the U.S. and abroad on the market, industry, and policy implications of events relevant to the Internet ecosystem. He is a research scientist in the Computer Science and Artificial Intelligence Laboratory (CSAIL) at the Massachusetts Institute of Technology, currently engaged in a number of multidisciplinary research projects within the Advanced Networking Architecture Group in CSAIL. Dr. Lehr's research focuses on the economics and regulatory policy of the Internet infrastructure industries. He is engaged in multiple multidisciplinary research projects focusing on issues such as broadband Internet access, cybersecurity, next

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

generation network architectures, and spectrum management. In addition to his academic work, Dr. Lehr advises public and private sector clients in the US and abroad on ICT strategy and policy matters. Dr. Lehr holds a PhD in Economics from Stanford and an MBA in Finance from the Wharton School, and MSE, BA, and BS degrees from the University of Pennsylvania. For more information, see http://people.csail.mit.edu/wlehr/. For the purposes of this engagement, Dr. Lehr was appointed a Consulting Director at LECA.

8.3. Mark Loney

Mark Loney is a Consulting Director at LECA and an expert in advanced communications systems and technologies, public policy, and public sector management. Mark was a Senior Executive in the Australian Public Service for fifteen years and has been providing independent advice on spectrum management and telecommunications regulatory issues to international clients since 2019. An Executive Manager at the Australian Communications and Media Authority (ACMA) from 2005-2018, Mark played a key role in establishing Australia's converged communications regulator from 2004 to 2005. Mark led the development, implementation and delivery of regulatory arrangements for broadcasting, radiocommunications and telecommunications services for over twenty years in the Spectrum Management Agency, the Australian Communications Authority and the ACMA. Mark was Deputy Head of the Australian Delegation to the World Radiocommunication Conference 2003.

Mark joined the Australian Public Service in 1988 at the Department of Defence where he was involved in complex communications research for nearly 9 years. Since 2010, Mark has co-authored papers for IEEE conference series such as DySPAN as well as the Journal of Telecommunications Policy (TelPol). In 2014, Mark provided advice to the Government of Mongolia about rapid transition to next generation mobile networks (LTE/LTE Advanced) and associated issues such as backhaul and security requirements. Mark has a BA from Curtin University and has undertaken postgraduate studies at the Australian National University.

8.4. Doug Sicker

Douglas Sicker is a leading global expert from the USA on network technologies and their application and implications in other industries like wireless systems and cybersecurity both today and in the future. Doug is currently the Senior Associate Dean of Computing and computer science and electrical engineering Professor at University of Colorado, Denver | Anschutz Campus. Previously, Doug served as the Lord Endowed Chair in the School of Computer Science and in the College of Engineering at Carnegie Mellon University (CMU) and as a Department Head in Engineering. He was also recently the interim Director of CyLab at CMU that brings together experts from a variety of disciplines across the university to collaborate on cutting-edge research and education designed to help create a world in which technology can be trusted. Doug also serves as the Executive Director of the Broadband Internet Technical Advisory Group (BITAG). Doug has acted as the CTO to the

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

National Telecommunications and Information Administration (NTIA and the Federal Communications Commission (FCC), and as a senior advisor to the Department of Justice National Institute of Justice and was the Chair of the Network Reliability and Interoperability Council steering committee. Prior to that he was Director of Global Architecture at Level 3 Communications, Inc. Doug has published widely in the fields of networking, wireless systems, network security and network policy. For the purposes of this engagement, Dr. Sicker was appointed a Consulting Director at LECA.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718