LECA

Law & Economics Consulting Associates

The Economic Impact of Laws that Weaken Encryption
- *Executive Summary* -

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

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

[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 and referenced in Notes 110, 112 of the full report.

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

are likely to be broad-based and accumulate over time as effects ripple through the economy.

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

[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: http://publications.atlanticcouncil.org/cyberrisks//risk-nexus-september-2015-overcome-by-cyber-risks.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

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 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

[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/)

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

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] 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.

The full report is available here:
https://www.internetsociety.org/resources/doc/2021/the-economic-impact-of-laws-that-weaken-encryption/

[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.

[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.

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