Australian Taxpayers' Alliance
P.O. Box A2208
Sydney South NSW 1235
www.taxpayers.org.au
enquiries@taxpayers.org.au
(02) 8964 8651

SUBMISSION REGARDING:

Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018

BY THE AUSTRALIAN TAXPAYERS' ALLIANCE

Introduction

1. The Australian Taxpayers' Alliance (ATA) is a unique grassroots advocacy and activist organisation comprised of over 75,000 members dedicated to standing up for hardworking Australian taxpayers. We oppose the high taxes, wasteful spending, and crippling red tape that is hurting Australian families and businesses, and provide a voice for everyone who opposes the big-government agenda. Part of that agenda includes standing up for Australians' civil liberties and the rule of law, as both are inextricably linked to our prosperity as a nation.

2. The ATA is concerned that the *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (Ch) will undermine the rule of law, threaten our national security, and unnecessarily harm Australians' privacy and online security. If enacted, the Bill may also impose an unworkably complex burden on businesses and discourage tech entrepreneurship and investment in Australia. The ATA is also concerned that the Bill may encourage over-reach by law enforcement and allow access to information without a warrant by foreign law enforcement agencies. Further, the ATA has specific concerns about the broad definitions in the Bill and the excessively harsh punishments imposed by it. In addition, the ATA believes that current law enforcement powers are more than sufficient to afford Australian law enforcement agencies access to data and information where appropriate. The Bill is fundamentally flawed and should not be enacted.

Summary of the Bill

3. The Bill's purposes are:

   3.1. To require domestic and offshore communications providers to assist Australian law enforcement and security agencies—specifically by requiring them to provide access to encrypted customer information where practicable. Communications providers may include software developers and sub-contractors.

   3.2. To introduce new "computer access" warrants for law enforcement that will enable them to covertly obtain evidence directly from a device;

   3.3. To strengthen the ability of law enforcement and security authorities to overtly access data through the existing search and seizure warrants.

4. The Bill sets out to achieve these goals as follows:

4.1. **Schedule 1** empowers ASIO, ASIS, and ASD to issue voluntary "technical assistance requests" to domestic and foreign communications providers. The term "designated communications provider" is very broadly defined, and includes contractors who install services, as well as software developers. Further, the Director-General of Security may issue "technical assistance notices" that force communication providers to assist if it is deemed that the assistance is "reasonable, proportionate, practicable and technically feasible." Additionally, the Attorney General to issue "technical capability notice" to force communication providers to build new features that can help law enforcement. However, providers cannot be asked to "remove features." Penalties, including criminal penalties of up to X years, apply to anyone who refuses to comply with these notices.

4.2. **Schedule 2** empowers, federal, state, and territory law enforcement agencies to obtain so-called "computer access warrants." Previously, only ASIO could apply for such warrants. which allow for the searching the content of electronic devices. This is in addition to existing "surveillance device warrants" which allow for monitoring input and output from devices. ASIO is also granted additional powers to intercept communications while using a "computer access warrant" without a separate surveillance warrant.

4.3. **Schedule 3** allows ASIO to temporarily remove devices or "things" from properties, and to be able to hide that it had accessed a device after the warrant expires. This Schedule also allows other law enforcement agencies to collect information from computers under an "covert search warrant" remotely, without having to access the location. The Bill also increases the amount of time a device can be withheld for analysis from 14 days to 30 days and increases the penalty for refusing to provide access to a device under a search warrant from 2 years to 5 years.

4.4. **Schedule 4** empowers the Australian Border Force to obtain a search warrant to access a "computer or data storage device" remotely, rather than obtain a search warrant to search a premises. The Bill also extends the examination time for electronic devices from 72 hours to 30 days. The Bill also increases the maximum sentence for non-compliance with a warrant by a person from 6 months to 5 years. In cases of serious criminal investigations, the Bill increases the penalty for "aggravated non-compliance" from 2 years to 10 years.

4.5. **Schedule 5** protects persons or organisations who assist ASIO, either on an unsolicited basis or voluntarily after a request from the Director-General, from civil liability. The Schedule also empowers ASIO to force a person with a knowledge of a computer or computer system to assist the agency in accessing it, provided ASIO has first obtained an order from the Attorney-General empowering it to do so. The maximum punishment for non-compliance is 5 years' imprisonment.

The ATA's Concerns

Once unlocked, the "back door" cannot be locked again

5. First and foremost, it must be emphasised that this legislation is premised on the unworkable premise that law enforcement can be afforded access to encrypted communications without generally undermining their confidentiality. The creation of 'backdoor' hacks to access data, if they are in fact workable, can and will invariably be discovered by non-governmental agencies. As the saying goes, 'two can keep a secret if one is dead': knowledge, particularly in

governmental agencies and amongst tech industry insiders, can and will spread about backdoor methods of accessing encrypted communications. Once it does, those encryption methods will be rendered worthless—potentially wiping away billions from the economy as sensitive data is hacked for nefarious purposes, such as fraud or intelligence gathering by criminal gangs or hostile powers. Far from opening up a 'backdoor' to safeguard our security, this Bill opens up a Pandora's box. It poses an unacceptable risk to our national security, our economy and our privacy.

6. While the Bill's provisions pretend to avoid this problem by suggesting that no request for assistance or modification can have the effect of requiring a communications provider to generally decrypt their data or services,[1] the unavoidable truth is that there is no such thing as an isolated back door in computer programming or software. Programming language is built on code that can be accessed, copied and adapted by programmers. That means that every back door that is implemented offers a programming "pathway" for others to copy and adapt, allowing a wider hack to occur. Once unlocked, the backdoor simply cannot be locked again. Taken literally, this provision of the Bill would obviate any and all requests for assistance made by the government of the day. Communication providers may choose to cooperate nevertheless in the face of political pressure, but this should not be mistaken as proof that the Bill's provisions are workable.

7. It is also important to stress that there are many legitimate purposes for confidential, encrypted communications to occur. Politicians should be well aware of this: media reports indicate that the recent federal spill motion involved a campaign undertaken, among other things, by Whatsapp message.[2] It is unlikely that these methods would have been used if they were not encrypted and secure.

Unworkable imposts on business

8. The premise of the compulsory "technical assistance notices" and "technical capability notices" in Schedule 1 is that they will only be issued if the request is "(r)easonable, proportionate, practicable and technically feasible". However, this is not clearly defined, and left completely up to the judgement of the Director-General of Security or the chief officer of the intercepting agency. Bureaucrats and their subordinates are unlikely to know whether the encryption systems and software are capable of being used or for that matter modified in a manner that allows them to assist law enforcement in a manner that is in fact 'reasonable, proportionate and technically feasible.' This creates extraordinary uncertainty for any business that has received a technical assistance or technical capability notice notice.

9. The Bill may have severe financial impacts on companies reliant on encryption for their business models. Smaller businesses may effectively suspend their operations for days or months as their senior managers and programmers work to assess whether or not they can comply with these requests and attempt to do so by redeveloping their software. It is difficult to see how start-ups, for example, could cope with the burden imposed by this notice. This may cripple that business' operations or, if the business is facing financial difficulty, cause it to enter into insolvency or liquidation. Larger businesses may also struggle with the compliance burden posed by technical assistance or modification requests.

[1] See s317ZG, p48 of the Bill.

[2] See e.g. "Leaked WhatsApp messages reveal Julie Bishop's leadership bid scuppered by colleagues", *The Guardian*, 26 Aug 2018, https://www.theguardian.com/australia-news/2018/aug/26/julie-bishops-leadership-bid-scuppered-by-colleagues-messages-show

10. *Litigation costs for taxpayers and the public.* Larger tech businesses and multinational companies may have the resources to contest the validity of these notices in Court. Invariably, they will do so on the grounds that the requests made are not 'proportionate, practicable and technically feasible.' Potentially, millions of dollars or more and months or years of time may be wasted by businesses, litigants, law enforcement and the legal system every time an assistance notice or capability notice is issued. The complexity of the issues posed by the legislation are outlined below:

    10.1. The Bill invites highly complex, fact-based disputes over whether a request from the Attorney-General constitutes a request for "assistance" or "modifications", as well as whether the request involves the removal of a pre-existing "feature" in the software. Invariably, companies may query the validity of requests for assistance or modifications will undermine the security of their customers' data and their business model and will not be 'proportionate, practicable or technically feasible' in the circumstances.

    10.2. Courts may be effectively unable to genuinely assess whether companies may hold genuine, good faith views that they cannot render the assistance or make the modifications to their software sought by the government. The extraordinarily specialised nature of IT software programming will mean that initial opinions on the technical feasibility of giving "assistance" or engaging in seemingly 'simple' software modifications may vary widely.

    10.3. Fundamentally, only employees working within a company will have any real idea of what they themselves are capable of, including whether they can assist law enforcement. Even they can only guess at that by engaging in a costly preliminary scoping exercise which may prove wrong on further examination. Second-guessing their capabilities could also be a very risky, costly and uncertain endeavour, both for the company and for external industry experts. It will be even harder for those with no relevant knowledge of the field such as law enforcement, departmental bureaucrats, lawyers or judges.

    10.4. Companies with the resources to do so may well vigorously contest these notices given that the penalty for non-compliance would be up to $10 million per offence. On the other hand, multinational companies may simply 'wear the fine' if necessary as a cost of doing business, or simply exit the country.

    10.5. Companies that seek to comply with notices and fail to do so may also seek litigate their rights if agencies contest their ability to complete the request or modifications required of them, causing additional delay and expense.

    10.6. If the matter is litigated, expert evidence on IT and programming issues may need to be called upon by law enforcement, the company or the Courts to assess the practicability of giving assistance or making modifications to programs. This may result in the possible disclosure of sensitive source code or other trade secrets to the wider industry that may damage a company's future financial health or operations.

    Undermining tech and business investment in Australia.

11. The Bill may also have the effect of discouraging investment in Australia for the following additional reasons:

11.1. The introduction of this legislation alone could render this component of the tech industry would effectively be unwelcome and closed for business in Australia and directly lead to the shuttering of legitimate Australian tech encryption businesses.

11.2. Requiring businesses to disclose sensitive information and de-encrypt data belonging to their customers to assist law enforcement may completely undermine their business models, particularly where they promise security to their customers. Much as Amazon's American branch ceased to export goods to Australia following the introduction of recent GST reforms,[3] this legislation may even prompt some communications providers to consider whether to exit the Australian market entirely because of the threat posed by its introduction.

11.3. At least at first, it is likely that these notices will be issued to major 'communications providers' such as the various owners of Facebook Messenger, WhatsApp, Snapchat, Viber and similar programs variously owned by Facebook, Snap Inc. and other major technology companies. It might be assumed that these multinational companies have the resources to respond to notices issued by Australian law enforcement agencies. However, it must be emphasised that these programs and messaging software only exist, or at any rate at their current popularity level, because of the confidentiality of the communications to which they relate. The popularity of these programs could plummet if they are no longer confidential.

11.4. The existence of laws that make it possible for law enforcement to require these companies to de-encrypt their own software and communications will undermine investment in Australian tech companies and tech encryption companies in particular.

11.5. Australian investments in the broader multi-trillion dollar tech industry would also be threatened. Tech investments are in many respects completely reliant upon safe, secure encryption to keep trade secrets, customer information and sensitive data safe. All this would be undermined if the Bill were enacted.

11.6. Australian and foreign businesses may move to divest their sensitive data, tech operations or services overseas if Australia develops a reputation for being a place where it is unsafe for businesses to lawfully store trade secrets or other information. In plain terms, it is even possible that Facebook or other major encrypted messaging providers like WhatsApp or Viber will simply cease to offer their services here. There are already indications that Australia's reputation as a safe investment haven is suffering because of pre-existing powers enjoyed by the Australian Border Force to confiscate and search laptops and phones held by anyone arriving in Australia, as reported in news media recently.[4] Empowering agencies to de-encrypt data would worsen Australia's reputation as a safe place for business investment.

Undermining law enforcement accountability

[3] See "Amazon.com will stop shipping to Australia from July 1", *Australian Financial Review*, 31 Nay 2018, https://www.afr.com/business/retail/amazoncom-will-stop-shipping-to-australia-from-july-1-20180531-h10rzv

[4] See "Border Force rejects privacy breach claim", *The Australian* 18 Aug 2018, https://www.theaustralian.com.au/news/latest-news/man-accuses-customs-of-privacy-invasion/news-story/1e356a8302e81b55d4b5157f55db0f46

12. Worryingly, the Bill doubles the time that devices can be withheld for inspection. In the case of the Border Force, the Bill increases that time tenfold. This undermines the accountability required for agencies to justify their work. Simply put, law enforcement agencies should not be entitled to engage in unnecessarily long 'fishing expeditions' that involve withholding private property from the individuals to whom they belong without justification. Further, withholding property for excessive periods of time undermines the presumption of innocence and the property rights of the property owner. An extended period of confiscation could seriously inconvenience the property owner, interfering with their business and personal lives in the process. It should not be possible to extend withholding periods in the absence of a compelling reason and court order allowing for the extension of time.

Punitive and excessive punishments

13. No plausible justification has been presented for the increased penalties and maximum sentences for pre-existing offences presented in the Bill. It is not clear how and why these penalties will ensure compliance compared with lighter penalties already in force and there is no material to suggest that they will. In the absence of any material to suggest that current penalties for pre-existing offences are not working, lawmakers should not increase penalties. No such evidence has been offered by law enforcement to date.

14. The increases in prison sentences are punitive, especially in the case of the Border Force amendments in Schedule 4. Not handing a device over to Border Force in a non-serious criminal investigation should not be worth the new punishment of 5 years in prison (up from six months).

15. The Bill imposes punishments for non-cooperation with law enforcement but it is important to be mindful that there may be many legitimate reasons for non-cooperation, such as the unworkable character of any requests made by law enforcement.

Undermining the right to silence and right to notice of a warrant

16. Schedule 2 of the Bill empowers law enforcement agencies to secretly search the content of devices (instead of just ASIO). This is a dramatic expansion of law enforcement powers. Every individual deserves to know when the property is being interfered, not least because it may cause unintentional property damage or harm for which law enforcement agencies should be liable. Moreover, individuals have a right to know that they are being targeted by law enforcement officials. The presumption of innocence holds that people should be treated as innocent before proven guilty. That means that they should have a right to be informed when their property has been interfered with.

17. Empowering law enforcement agencies to force individuals to divulge passwords access codes to their personal phones or laptops under threat of criminal punishment of up to 5 years' imprisonment is profoundly troubling because it undermines the right to silence. No person should be forced to cooperate in their own prosecution by speaking to police. Compelling people to inform police of their passwords directly undermines the right to silence.

Law enforcement overreach: Compelling citizens to access private data on devices they do not own

18. Under the *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* s34AAA, the Director General may request the Attorney General to issue an order requiring any 'specified person' whom they reasonably believe possesses sufficient technical expertise, to

assist in accessing private data stored on devices or computer. Under s34AAA(2), this person may be the owner of the device, a systems administrator, an employee or contractor of the person or company that owns the device or even a mere user or former user of the device or computer. It is submitted that the effect of this section is to allow the Attorney General to compel a layperson with no connection to the alleged illegal activity to access or facilitate access to a third party's private data if the Director General has a suspicion that this person possesses sufficient technical expertise to do so. Although the law requires that this suspicion be 'reasonable', the layperson in question who does not possess technical expertise would need to challenge this claim in court at potentially great personal cost whereby the process would amount to unconscionable punishment for individuals who are not complicit in any alleged wrongdoing. Furthermore, even where the individual in question possesses sufficient expertise to facilitate access to the data, it is submitted that it is unethical for law enforcement agencies to compel ordinary citizens to effectively hack private devices under penalty of punitive sanction merely on the basis that they have used the device and may possess sufficient knowledge to enable access despite any conscientious objections they may have. For example, a layperson who happens to possess technical expertise in cybersecurity and uses a computer at a cybercafe without the knowledge that law enforcement agencies are seeking access to some private data also located on the computer/device, could theoretically be compelled under threat of criminal sanction to render services which they may have ethical reservations against, and without any requirement that their expertise or services be compensated per the market rate as they would if this person were hired by the law enforcement agency as an employee or contractor. It is submitted that such an effect is a perverse and unconscionable vesting of powers in law enforcement agencies to utilise coercive powers against individuals who have not committed and are not accused of committing a wrongdoing.

Case Study: UK Investigative Powers Bill

19. The *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* is modelled on the UK's *Investigatory Powers Act* 2016, which introduced mandatory decryption obligations. Under the UK Act, the UK government could order telecommunication providers to remove any form of electronic protection applied on behalf of or by an operator. Like this UK law, the *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* places upon telecommunication providers, the onus to grant security agencies access to communications. For example, the bill allows the Director-General of Security or the chief officer of an agency to compel a provider to do an unlimited range of *acts or things*. This could impute a range of actions, from removing security measures to collecting additional data or deleting communications. Providers are also obligated to conceal any action taken covertly by law enforcement. Furthermore, the Attorney-General may issue a "technical capability notice" *directed towards ensuring that the provider is capable of giving certain types of help* to ASIO or an interception agency. In effect, providers will be required to develop new information gathering methods for enforcement agencies. Providers that breach the law risk potential punitive fines of $10 million AUD.

20. The UK Court of Appeal deemed the *Data Retention and Investigatory Powers Act* (DRIPA) – a previous law covering state surveillance which was expanded upon by the Investigatory Powers Act of 2016 – to be unlawful.[5] The court ruled that the legislation abrogated the rights of citizens

[5] *Secretary of State for the Home Department v Tom Watson MP & Ors.* [2018] EWCA Civ. 70. https://www.liberty-human-rights.org.uk/sites/default/files/Watson%20v%20SSHD.pdf

by collecting internet activity and phone records while allowing public agencies to grant themselves access to these personal details with no suspicion of serious crime and no independent vetting. As a result of this ruling, the legislation is currently undergoing amendments. The legislation has also been deemed incompatible with European law.[6]

21. Charity group Liberty which launched the successful legal challenge against the UK Act notes that it is "incompatible with people's fundamental rights because ministers can issue data retention orders without independent review and authorisation – and for reasons which have nothing to do with investigating serious crime."[7] The *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* similarly bestows such powers upon the Attorney General.

22. Although this ruling does not speak to the constitutionality of the legislation in Australia, it nonetheless demonstrates that such a law is incompatible with public expectations about the accountability of Ministers and law enforcement agencies as well as the ambit that the aforementioned have in impinging upon the private information of citizens or their consent in providing services such as data de-encryption such as that which is stipulated under S34AAA(2) of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*.

23. The ruling further demonstrates that the *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* will have the effect of giving Australian state agencies and Ministers far more draconian powers in unduly impinging upon private data and private businesses than those which have been deemed appropriate in comparable Western liberal jurisdictions. The *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* is hence undesirable from a public interest/public policy standpoint.

Conclusion

24. The Bill is unworkable, flawed, and unnecessarily complex. It may harm our economy, national security and privacy. It undermines the right to silence. Far from aiding law enforcement in its efforts, it has the potential to undercut those efforts by undermining trust in law enforcement and business confidence in our rule of law.

Prepared by Vladimir Vinokurov and Satyajeet 'Satya' Marar on behalf of The Australian Taxpayers' Alliance.

Satyajeet 'Satya' Marar
Director of Policy – Australian Taxpayers' Alliance (ATA)
[redacted]

[6] "UK has six months to rewrite snooper's charter, high court rules" *The Guardian* 27 April 2018. https://www.theguardian.com/technology/2018/apr/27/snoopers-charter-investigatory-powers-act-rewrite-high-court-rules

[7] Media Release: "Liberty wins first battle in landmark challenge to mass surveillance powers in the Investigatory Powers Act" 27 April 2018. https://www.libertyhumanrights.org.uk/news/press-releases-and-statements/liberty-wins-first-battle-landmark-challenge-mass-surveillance