SENETAS
Security without compromise

13 September 2019

Mr James Renwick CSC, SC
Independent National Security Legislation Monitor
3-5 National Circuit
Barton ACT 2602

Dear Mr Renwick,

Submission to INSLM - Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018

Senetas Corporation welcomes the decision to undertake a review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (the **Act**) by the INSLM, and we appreciate the opportunity to provide a submission for your consideration in relation to this unprecedented legislation.

The attached submission is structured around the three key issues included in the terms of reference for your review.

This submission provides further evidence of the weaknesses in the legislation and implications for the Australian technology and telecommunications industry. Senetas has previously urged the Government to reconsider the Act in its entirety as part of a collaborative consultation process which takes into account the views of all relevant stakeholders and persons that may be affected by the Act and balances all competing interests, including the national interest.

One of the challenges that the industry is already facing, in terms of this legislation, is the relatively unique matter of its interpretation. Ordinarily legislation that is the subject of differing views as to the meaning of specific aspects will be resolved in public or ultimately in the courts. It is now becoming increasingly clear that the views held by the Department of Home Affairs (and to some extent other Government agencies) about the meaning of specific clauses, and/or how they are to be implemented, differs from that of the industry and others. Unfortunately, given the secrecy provisions of the Act there is no satisfactory way of challenging and resolving these differing views, with the Department effectively requiring that its view prevails. This issue is touched on in our submission but may also form a useful area of focus for further discussion. There is certainly no doubt that it adds further complexity to the challenge you face in undertaking this review.

Senetas recognizes the important role the INSLM plays in providing advice to parliament in relation to this legislation and is available to provide any further information or evidence at a future hearing.

Yours Sincerely

[redacted]

[redacted]

Francis W. Galbally
Chairman
Senetas Corporation Ltd

Andrew Wilson
Chief Executive Officer
Senetas Corporation Ltd

SENETAS CORPORATION LIMITED
312 Kingsway, South Melbourne, VIC, 3205, Australia
T +61 (03) 9868 4555 F +61 (03) 9821 4899
E info@senetas.com
www.senetas.com

ABN 33 006 067 607

Submission to the INSLM - Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018

Summary of relevant issues identified in past submissions

At the outset, Senetas would like to outline a small number of the more critical concerns and observations made in previous written and verbal submissions to the reviews undertaken by the JPCIS in 2018 and 2019. These have been specifically identified as falling within the terms of reference for the INSLM review. Despite claims made by the government, and the Department of Home Affairs, Senetas does not consider these issues to have been adequately addressed or rectified either prior to the passage of the Act or since. Many industry and other non-government parties, involved in this matter, share similar views on these. In particularly we strongly support and endorse the comments made by the Law Council of Australia, Communications Alliance, Ai Group, AIIA, AMTA, DIGI and IPTA, Associate Professor Vanessa Teague and Dr Chris Culnane.

Senetas' earlier submissions covered a number of substantive areas of concern. The amendments made to the Bill in December 2018, essentially failed to address these issues or actually made the situation worse (e.g. late changes to definitions). Despite these same issues resurfacing in the JPCIS review in early 2019, no action has been taken to address them.

The table below summarises those critical areas of concern previously raised by Senetas, where these also touch directly on the terms of reference for the review being undertaken by the INSLM.

Issue/Concern	**Response/Outcome**
1. The Bill/Act risked damaging Australian developers' and manufacturers' reputations in international markets leading to lost exports, jobs, technical expertise, etc.	This risk has been realised. Based on widespread media coverage in international markets, the Act has damaged the reputation and trust held of Australian technology developers' and manufacturers. This is negatively impacting exports, local R&D, manufacturing, Start-Ups and Education. The Department has acknowledged this in its latest JPCIS submission.
2. The Act increases the risk of compromising the security and privacy of citizens and businesses as a consequence of weaker cyber security practices and easier access to new tools for cyber criminals.	Despite evidence of this occurring internationally, the Department has simply stated that this won't happen[i]. The response fails to address entirely the ways this could occur let alone the catastrophic consequences.
3. Poor integration testing of capabilities could lead to unforeseen consequences, including the potential for large scale network outages impacting internet service in Australia and throughout the world.	Little or no action taken. The Risk remains unmitigated and the revised secrecy provisions potentially elevate likelihood. See also Issue #1 below.
4. The legislation risks compromising critical encryption systems by introducing "systemic weaknesses" into products and the internet as a whole.	Despite claims to the contrary, as a consequence of the definition, the legislation specifically allows for systemic weaknesses and backdoors to be introduced into technology products and services.

1. The Act demonstrably fails to protect the rights of individuals (and businesses).

The Government and the Department of Home Affairs claim that the legislation contains a range of safeguards and does not allow the introduction of "backdoors", compromise critical encryption systems or introduce any "systemic weaknesses" into products. This claim does not stand up to scrutiny. The supposed guarantees offered by Section 317ZG of the Act are undermined and made worthless by virtue of the perverse definition of "systemic weakness" and "systemic vulnerability" introduced without consultation with industry immediately prior to the legislation passing the lower house.

The consequences of this situation are potentially catastrophic – to individuals, businesses both in Australia and across the world.

Evidence supporting this position

Notwithstanding extensive discussion concerning the absence of any definition of these terms during the course of the Committee's review of the Bill in late 2018, the Government amended the draft bill to introduce definitions for these terms immediately prior to the legislation passing the lower house. As far as Senetas is aware, the wording of these definitions was developed without consultation with industry, and certainly does not reflect their common meaning.

To aid in understanding, the definitions as they appear in the Act at Section 317B are:

> ***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.*

Firstly, these definitions are perverse. They bear no correlation with the common meaning of the terms as used by industry, academics or technology experts for decades.

As noted by the Law Council in its original submission (#5), these definitions *"… simply allow for the introduction of any weakness or vulnerability as requested"* and *"their very intention is to introduce a diminution in security standards…".*

It is as if the Government has chosen a definition of a well understood concept and refashioned it in such a way as to increase the likelihood of the very risk that the industry was concerned about being realised.

As if to demonstrate this further, the advice contained on the Department's web site[ii] concerning the supposed limitations and safeguards, includes the following, quite misleading advice:

What is a systemic weakness

Section 317B defines a systemic weakness/vulnerability as 'a weakness/vulnerability' that affects a *whole class* of technology...'. The term 'class of technology' is deliberately broad and captures general items of technology across and within a category of product. It encompasses, for example, mobile phone technology, a particular model of mobile phone, a particular type of operating system within that phone model or a particular type of software installed on an operating system. The wide scope is intended to protect the services and devices used by the whole, or legitimate segments of, the general public and business community.

Further elements of the definition clarify that the inherently targeted surveillance activities of agencies are not captured by this definition. However, new subsections 317ZG(4A), (4B) and (4C) make clear that even requirements to assist in these legitimate and authorised agency activities must not have the inadvertent effect of weakening information security. That is, industry cannot be asked to do things that would be likely to create a material risk of unauthorised access to the information of a person not connected to an investigation.

The intent and application of the protection is to provide for targeted, proportionate access and prevent weakening cybersecurity.

While one could comment on the incomplete definition in the first paragraph, the critical wording contained in this advice is in the first sentence of the second paragraph. This confirms precisely that the concerns expressed by the Law Council are indeed valid – i.e. that the *"…surveillance activities…are not captured by this definition."* The implications are therefore that any surveillance activity undertaken under this legislation is not subject to the safeguards afforded to any clause that relies on the definitions.

In relation to the remainder of the 2nd paragraph above, as noted in a number of submissions, including that of the Law Council, the phrasing of two equivalent sub-sections included in Section 317ZG (in respect of systemic weaknesses and systemic vulnerabilities) would seem, in part, to include words closer to the normal use of the terms — but which arguably renders those sections inconsistent with the definitions of systemic weakness and systemic vulnerability at 317B.

> *"(4A) In a case where a weakness is selectively introduced to one or more target technologies that are connected with a particular person, the reference in paragraph (1)(a) to implement or build a systemic weakness into a form of electronic protection includes a reference to any act or thing that will, or is likely to, jeopardise the security of any information held by any other person."*

The wording of this sub-section includes the use of the terms "weakness" and "systemic weakness". It is not at all clear how the recursive use of "systemic weakness" assists here in providing a safeguard to *"persons not connected to an investigation"*. In relation to the person under investigation, the definition states that *"it is immaterial whether the person can be identified*". Given the definition, combined with its appearance in this sub-clause, how are one set of persons deemed to be excluded? The word "weakness" used on its own is also undefined. Does this imply that only weaknesses that are not systemic are relevant, or is it meant to imply that any limitations or flaw that is introduced could meet the threshold of jeopardising the security of a person's information? These additional sub-sections are confusing, inconsistent and provide no comfort.

The legislation provides a mechanism to resolve a dispute between the parties in the context of the possibility of introducing a System Weakness into a target system. This mechanism relies on the appointment of a technical expert who, together with a retired judge, is able to provide independent advice to the agency and potentially Minister. Curiously, the Department is now attempting to undermine the value of this advice. Its latest submission to the PJCIS (#16) includes the following comments (at page 30):

> *171. The Department queries whether an assessor appointed for their technical expertise is well positioned to consider the reasonableness and proportionality of TCNs. This criteria goes to the broader circumstances of the requirements, like the details and needs of national security and law enforcement operations and broader questions of personal and social impact – not potential technical impact of requirements.*

This view represents a fundamental misstatement of the reason for having a technical advisor. They are primarily there to assess compliance with the law and consistency with issues such as "systemic weakness", "backdoor", technical complexity, risk of impact to third parties, etc. (See Section 317ZG and especially Subsection 317ZG(4C)). To suggest that this person's technical advice and opinion could be dismissed due to a perception that they lack an appreciation of the national security issues involved, represents a serious failure to recognise and respect the reliance placed on them, under the legislation, to determine the potential for a capability to compromise other systems. It does raise the question as to whether the Department is only paying "lip service" to the supposed safeguards.

While the focus has been on an intentional act or decision by an agency to compromise a system to provide access, perhaps the far more concerning matter should be the unintended consequences of actions pursued under the authority of the legislation.

For example, as noted in our submission to the JPCIS in November 2018, changes to communications systems, and to any devices or technologies forming part of the supply chain of such systems (without undertaking extensive regression and integration testing) could lead to any number of unforeseen consequences resulting from an inability to follow standard software development and testing procedures, including the potential to compromise the wider security of those systems and potentially make them unstable. This includes, for example, the potential for large scale network outages impacting internet service in Australia and throughout the world.

As noted by Telstra, in their submission to the committee's review of the draft Bill, it *"covers the entire communications services supply chain, making it possible a TA Notice or TC Notice could require 'modification' to a piece of network equipment or its operating software without the knowledge or awareness of other communications providers. For example, if a telecommunications provider (such as a carrier or carriage service provider) uses equipment or software supplied by a third party, that third party may have been separately required to provide technical assistance to an agency (potentially including the installation of software or equipment supplied by the agency) or to introduce new technical capability into their products. Given the secrecy provisions of the Bill, this could occur without the knowledge of the telecommunications provider and could result in an adverse impact to its network and/or customers' use of the network. Such adverse effects could include service degradation, network faults, or other impacts on its business, or on non-target customers."*

There is simply no way that an individual provider, supplying a single element of an integrated system, could possibly have visibility of the implications of making changes to their product on other elements of a complex system. Certainly, any independent technical expert appointed to make such an assessment would be incapable of doing so due to the complex interplay between the large range of technology providers and how these have been implemented. Over time, the risk of a small, and otherwise insignificant, change to a component of the network resulting in catastrophic failure is high. The

consequences to all parties (including government) are unpredictable. The existing definition completely fails to recognise this risk. More serious though, is that even were such a risk identified, the existing definitions would not necessarily prevent an agency proceeding to enforce a TCN.

No less authority than the Internet Architecture Board (IAB) confirms the validity of this concern. The IAB is chartered both as a committee of the Internet Engineering Task Force (IETF) and an advisory body of the Internet Society. The IETF is the global body that is responsible for all Internet standards. In its submission (#23), the IAB notes that *"Any method used to compel an infrastructure provider to break encryption or provide false trust arrangements introduces a systemic weakness, as it erodes trust in the Internet itself. In other words, the mere ability to compel Internet infrastructure providers' compliance introduces that vulnerability to the entire system, because it weakens that same trust."* It goes on to state that *"The IETF, in RFC 2804, has rejected the development of any system designed to aid state actors in compromise of the security of Internet communications. Compelling individual participants to act contrary to that consensus introduces doubts about the motivations of and influences upon a participant's actions, and therefore may disadvantage Australian participants in these processes."*

Failing to recognise the true meaning of a Systemic Vulnerability and Systemic Weakness within the context of the Act, exposes every technology user to quite unpredictable consequences. The fact that the definitions included in the Act are complex and inconsistent (both with the terminology and understanding of industry and experts, and with the provisions of the Act itself), also means that the Act suffers from ambiguity and difficulties in interpretation. This gives rise to further issues in respect of both enforcement by government and compliance by industry.

Implications

Fundamentally, the most serious issue arising from the perverse definitions is the fact that they undermine the claimed safeguards of the legislation. The position adopted by the government and the Department is that the legislation prevents the introduction of a "backdoor", the compromise of encryption systems, or the introduction of a "weakness" into a system. This position is dependent on the definitions of "systemic weakness" and "systemic vulnerability" contained in the Act. Since they are fatally flawed, so are these claimed safeguards.

The secrecy provisions of the Act further increase the likelihood of a real systemic weakness and add further complexity as to how a response to correct it may be undertaken.

As outlined in our submissions to the JPCIS, the legislation compromises the security of citizens, businesses and governments as a consequence of weaker cyber security practices and easier access to more powerful and highly targeted tools for cyber criminals. There have been numerous reliable reports of the NSA having its "hacking tools" stolen and used or repurposed for use by cyber criminals or others. The tools and exploits developed as a result of this legislation will be created within the commercial organisations that own them – in Australia or overseas. As such, these tools exist within far less secure facilities than those of the NSA. The assurance given by the Department that they can be protected is worthless since they have no capacity to do so beyond their facility and certainly beyond Australia's borders.

Perhaps the most succinct statement regarding the impact of the legislation on the rights of individuals was made by the Reform Government Surveillance (RGS) coalition. The RGS represents many of the largest international technology companies – including Apple, Microsoft, Google, Facebook, Twitter, Dropbox and Linkedin. This statement described the legislation as undermining the cybersecurity, human rights and right to privacy of users. It also stated that the "new Australian law is deeply flawed".[iii]

Any claim that the Act contains adequate safeguards that protect the interests of individuals or businesses cannot be sustained.

2. The Act fails any test of being proportionate to the threat of terrorism or to the nation's security.

In October 2018, an Apple spokesperson speaking about the then proposed Bill, stated that "it would be wrong to weaken security for millions of law-abiding customers in order to investigate the very few who pose a threat."[iv]

No western democracy has actually adopted the extreme measures contained within this Act, and the related amendments to other legislation, in the absence of strong corresponding oversight. The Department is only able to identify two examples of nations that have enacted, what it identified as similar legislation – the UK and New Zealand. The suggestion that the Australian legislation is comparable to laws enacted in these countries completely overstates the reach and scope of those laws.

The reality is that the Australian legislation is routinely referred to as being "world-first", "world Leading" and "unprecedented" by most parties involved in this debate – in Australia and overseas. If it were thought to be proportionate to the threat of terrorism, then we should expect to see even stronger laws in countries subject to higher numbers of terrorist incidents or that feature more extreme violence.

The reality is that we do not see such examples, and, by any measure, the Act is not proportionate to the risk. Increasing the risk of harm to millions of law-abiding citizens of Australia, and indeed other nations, must be balanced against the marginal benefit derived from this legislation to protect against any potential terrorist threat.

Evidence supporting this position

The UK has for many decades suffered large numbers of violent terrorist incidents resulting in death and large-scale property damage. In comparison to Australia, the UK Investigatory Powers legislation, for example, includes a far narrower scope of obligations on commercial communications providers than that contained in our legislation. It includes an extensive range of real safeguards, such as oversight by an Independent Commission (with a staff of approximately 50), a Tribunal, a far stronger requirement for warrants with ongoing Judicial review of those warrants, explicit protection for journalists, and operates within the framework of the UK Human Rights Act and the European Privacy laws.

The threat and reality of terrorism in the UK far exceeds that of Australia – and yet somehow, we are told that we need to go beyond what even the UK has done. In comparison to how the UK is addressing its concerns, the Australian legislation stands out as an example of significant overreach. This hardly represents a "proportionate" response. It certainly explains why many have described it as being legislation that is "world first" but not with the connotation of being a good thing. It's also why many experts in this area were so shocked by the passing of the legislation in late 2018 – that Australia would see fit to go so far beyond internet and technology norms. The background to those views provides some useful insight.

In early 2015, law enforcement agencies in the UK and US called for changes to the Internet to enable government access to systems and encrypted communications. In response to this, the Massachusetts Institute of Technology (MIT) published a paper in July 2015, written by a number of computer scientists and security experts, titled ***Keys Under the Doormats: Mandating insecurity by requiring government access to all data and communications***[v]. It is worth reviewing the core observations and findings of that paper as they remain as relevant today as they did four years ago. In essence this research showed that providing law enforcement agencies with exceptional access to systems would:

- make those systems less secure – increasing the risk to government, businesses and individuals that other parties could gain access to and/or compromise those systems;
- increase the likelihood of failure in fixed & mobile telecommunications and Internet based services in ways that would be difficult to predict and/or repair; and
- create a set of resources or targets that could be leveraged by cyber criminals and other bad actors to gain access to systems not previously able to be compromised.

The report goes on to note that the *"… analysis of law enforcement demands for exceptional access to private communications and data shows that such access will open doors through which criminals and malicious nation-states can attack the very individuals law enforcement seeks to defend. The costs would be substantial, the damage to innovation severe, and the consequences to economic growth difficult to predict."* In its conclusion, the report states that *"Absent a concrete technical proposal, and without adequate answers to the questions raised in this report, legislators should reject out of hand any proposal to return to the failed cryptography control policy of the 1990s."* These arguments have been previously presented to the Department and the JPCIS. Despite the nature of the authority behind them, and expert evidence contained in them, the government has never provided a compelling argument refuting the concerns.

Media coverage and commentary on the Australian legislation has not been limited simply to the technology press or the odd expert. Numerous articles have appeared in major newspapers such as ***The New York Times*** (NYT). In an article published on 22 January 2019, the NYT suggested that Australia had damaged phone security for the entire world. Based on expert opinion from the Open Technology Institute, it went on to state that the legislation represented *"…an encryption back door for the U.S."* In doing so, the articled outlined how Australia had in effect compromised the First Amendment to the US constitution (Freedom of Speech). The article quoted several Australian citizens, including:

- Mike Cannon-Brookes, (founder of one of Australia's largest IT companies, Atlassian) - *"All of Australian technology is tarnished by it."*
- In the context of comparing the Act to the legislative actions by other nations, Michelle Price, CEO of Australia Cyber Security Growth Network (formerly Senior Advisor, Domestic Cyber Policy at PM&C) said that *"…Australia's version has gone much further."*

There has been considerable commentary amongst the more influential international business journals. Specifically:

- The Nasdaq report - identifies both the extraterritorial nature of the law and its implications to Australian based companies. *"The long-term effects of these laws will surely be felt by the local economy, as innovative businesses are forced overseas or out of business."*
- The Economist – suggests that larger US firms may choose to exit the Australian Market to avoid damaging their global reputation. Clearly, this perspective will likely now cause foreign corporations to pause before investing here.
- The Nikkei Asian Review – describes the legislation as a *"shock to the global tech community"* and a threat to *"privacy and security"*. It identifies the blatant contradiction between the aims of the legislation and Australia's actions in relation to Huawei & ZTE.

A survey conducted by Vanafi of 384 IT security professionals, attending the Black Hat conference in the USA in 2019, found that 72% of respondents felt that providing government with access to encrypted personal data would not reduce the risk of terrorism.[vi]

At a recent public address, the Director General of ASIO, Mr Duncan Lewis observed that Terrorism – as a specific area of concern for his agency – was being overtaken by increased foreign interference. The one technology that we might expect could help protect our interests in this regard is strong encryption. As a consequence of this legislation we have effectively compromised our best protection and our own interests.

In the context of the business world, international credit and risk agency Fitch Solutions, was concerned that *"The new rules are negative for Australia's tech sector, but they will have the most impact globally, as they target international companies."* Fitch also expressed the view that *"Australia's unilateral decision is not the right way to proceed and will have an overall negative impact on security services."*

Implications

By any measure, Australia has adopted a particularly extreme legislative regime in order to gain access to data and communication systems used by individuals or organisations under investigation. Very few western democracies have felt it necessary or appropriate to match this approach – even in the face of much higher terrorist and/or national security threats. The implications of the legislation extend beyond Australia's own borders.

The evidence strongly suggests that the Act is not proportionate to the risk. Were this so, we would see similar approaches in wide use. A more accurate perspective, based on this evidence, is that its effect may actually be to increase the risk of harm to millions of law-abiding citizens of Australia, and other nations. To quote Senator Penny Wong, a member of the PJCIS at the time that the Bill was being considered by the Senate in December 2018, and reflecting on the evidence put to the committee, "*The Bill, as it is currently drafted, will make Australia less safe*"[vii]. The Bill that passed the Senate shortly

after this statement contained no amendments. No doubt the efforts by the non-government parties in early 2019 to introduce a range of amendments to the Act reflected their concerns also about the risks to the nation's interests. While these amendments passed the Senate, in February 2019, they have not become law.

The legislation is not, and never has been, proportionate to the risk – quite the opposite. Any benefits it may provide are more than offset by the risks it creates to the wider interests of the nation, its economy and impact on technology systems across the world.

3. Does the Act remain necessary?

The publicly expressed aims of the legislation are laudable and we support them. Unfortunately, however, the legislation enacted to give effect to those aims, is flawed. It has caused far more harm than the good sought to be achieved. In the absence of addressing the flaws, this will continue.

The consequences – initially described politely by some as being "unforeseen", are now very obvious. As outlined above, Australians are now less safe, as a result of this legislation. The cyber criminals, terrorists and paedophiles of this world have already moved on to simply use other technologies to securely communicate. Across the world, many technology companies have made changes to their products in ways to limit their exposure to Australian legislation. Whilst the criminals have moved on all law-abiding citizens are now LESS SAFE as a result of the legislation.

At the same time, many Australian based companies, such as Vault Systems, have been "*materially and detrimentally impacted by perception of the AA Act*"[viii]. Like countless other Australian companies, CEO Rupert Taylor-Price said that the AA Act was harming Australia's attractiveness for hosting data as multinational's moved to 'side step' the law.

With the original purpose of the legislation compromised, but the negative consequences likely to grow ever more serious, it is difficult to mount a compelling argument for the legislation remaining as it is.

Evidence supporting this position

In late 2018, the Minster, the Department and the Director General of ASIO, claimed that the passing of the legislation in early December 2018 was urgent and that further consideration of its impacts and consequences could not be allowed to delay its passing. It was suggested by these parties at the time that the Christmas/New Year holiday season represented a high-risk period and that the legislation was necessary to better protect the community. However, the Submission to the PJCIS by the Department of Communications in July 2019 states that the Department has yet to complete the development of guidelines in relation to the exercise of the authority of the Minister of Communications. Under the Act, the Communications Minister must authorize the issuing of a TCN (and other matters). The fact that there are no guidelines related to the use of this power - more than seven months after the legislation has been passed - must be of serious concern. It is understood that similar practical implementation issues are still being resolved within the Department of Home Affairs as well as in other agencies able to use this legislation.

Detective Superintendent Arthur Kopsias of the NSW Police is responsible in that state for enforcing this legislation. In an article published by the AFR on 12 March 2019, he commented that he was unaware of the provisions of the Act prior to it being passed. As a consequence, he didn't "have a clue how to implement it."

Clearly this must raise questions about the accuracy of the claimed need for urgency in passing the legislation, and more importantly, if it was actually necessary at all, given the failure of the bureaucracy to move quickly to bring it into force.

Most people are aware of the secure message capabilities of apps such as Telegram, WhatsApp and Signal. These companies, and many like them, have publicly stated that they won't be compromising their Apps, or their customer's desire for security, just because the Australian Government says so. Every terrorist and cyber-criminal on the planet understands this. The Act has created an incentive for the open source developer community to respond and thwart its intentions and there is simply no doubt that a significant effort is underway. Some companies, such as Nord VPN, made changes to their products within weeks to thwart the legislation. Initiatives like Solid and ActivityPub, are releasing new tools and platforms for use by the groups targeted by the Act – only these will be significantly more powerful ones.

The Chair of Internet Australia, and the nation's representative on the Internet's peak governance body, ISOC, has noted that even moderately competent Cyber Criminals will easily be able to thwart the intentions of the legislation by developing their own encryption platforms.

What the legislation has done is turbo charge these types of commercial and private initiatives. This is clearly not the outcome the government wanted, but it is a direct consequence of the limited consultation undertaken and the failure to listen to advice from industry.

At a JPCIS hearing in November 2018, Mark Dreyfus noted that "*One of the remarkable things about this bill is how consistent a lot of the criticism has been from a range of different stakeholders with vastly different interests. We have large multinational tech companies, smaller Australian based technology exporters, civil rights organisations, cybersecurity organisations and cybersecurity experts…*"

Implications

The weight of evidence questioning the appropriateness of this legislation is simply overwhelming and the expertise, independence and sheer volume of that criticism is beyond anything seen before in any legislation being debated/reviewed. Over the last 10 months there have been hundreds of submissions from eminent academics, multinational corporations, major Australian companies, Telecommunications providers, Internet research and governance organisations, Industry and Legal associations and technology experts. These have consistently criticized numerous aspects of the legislation.

The legislation represents an unacceptable risk to Australians' privacy, digital data, intellectual property, economic and financial interests and the critical infrastructure systems that underpin the operations of society and the state.

The Act is so demonstrably flawed that the only practical option is to see it withdrawn. The Government should then review its primary objectives and commence genuine engagement and consultation with all stakeholders – including consumers, business, industry representatives, Technology & Communications Organisations (including Australian SMEs), Internet Standards bodies and academia in order to achieve a workable way forward.

INSLM Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018

Sample media coverage in local and foreign press that has highlighted the nature of the legislation and the threat that it represents to other governments and commercial parties using or considering purchasing Australian technology products and telecommunications services.

https://www.stuff.co.nz/technology/109402792/nz-officials-consider-impact-of-australias-controversial-encryption-law

https://www.technologyreview.com/the-download/612562/this-is-how-australias-ban-on-encryption-could-endanger-us-all/

https://www.wired.com/story/most-dangerous-people-on-internet-2018/

https://www.nasdaq.com/article/australias-controversial-encryption-legislation-may-threaten-more-than-online-privacy-cm1067566

https://www.economist.com/asia/2018/12/15/an-australian-law-to-expose-vice-annoys-the-tech-world

https://asia.nikkei.com/Politics/Australia-shocks-global-tech-community-with-anti-encryption-law

https://www.scmp.com/business/companies/article/2179252/australias-new-telecom-bill-allowing-law-enforcement-access

https://www.smh.com.au/technology/negative-for-tech-sector-fitch-slams-australia-s-new-encryption-laws-20181213-p50m55.html

http://www.reformgovernmentsurveillance.com/rgs-statement-on-the-australian-parliaments-passage-of-assistance-and-access-bill/

https://www.nytimes com/2019/01/22/technology/australia-cellphone-encryption-security.html

https://www.innovationaus.com/2019/02/AA-laws-killing-us-overseas

https://www.innovationaus.com/2019/07/New-hurdle-for-encryption-laws

https://www.itwire.com/government-tech-policy/aiia-urges-govt-to-make-changes-in-encryption-law.html

https://www.zdnet.com/article/latest-technology-could-miss-australia-due-to-encryption-laws-telstra/

https://www.abc.net.au/news/science/2019-07-10/dutton-encryption-laws-australian-tech-sector-not-consulted-foi/11283864

https://www.zdnet.com/article/australian-government-spooks-and-industry-all-on-different-cyber-pages/

https://www.itnews.com au/news/amazon-blasts-australias-technically-flawed-anti-encryption-laws-527855

https://www.computerworld.com.au/article/663711/government-acknowledges-aussie-business-taken-hit-from-encryption-law/?fp=16&fpid=1

https://www.itwire.com/government-tech-policy/86618-issues-identified-in-encryption-law-frightening-ca-chief.html

---

ENDNOTES

[i] https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/myths-assistance-access-act (See section "Capabilities built by the Government will leak")

[ii] https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/assistance-and-access-limitations-safeguards

[iii] https://www.reformgovernmentsurveillance.com/rgs-statement-on-the-australian-parliaments-passage-of-assistance-and-access-bill/

[iv] https://www.voanews.com/silicon-valley-technology/australia-passes-worlds-first-encryption-busting-law

[v] https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf

[vi] https://www.itwire.com/security/government-mandated-encryption-backdoors-weaken-election-infrastructure-venafi-survey.html

[vii] https://www.perthnow.com.au/news/australia/new-law-puts-aussie-cyber-safety-at-risk-ng-b881038240z

[viii] https://www.itnews.com.au/news/vault-says-anti-encryption-laws-harming-its-tech-exports-527752