Submission to PJCIS

on the Inquiry into the

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

October 2018

This submission is endorsed by:

Australian Privacy Foundation
Digital Rights Watch
Electronic Frontiers Australia
Future Wise
Access Now
Blueprint for Free Speech
GetUp!

Dr Adam Molnar
Lizzie O'Shea
Dr Monique Mann
Angus Murray
Peter Tonoli
Bruno Watt
Dr Suelette Dreyfus

Contents

Overview

We welcome the opportunity to provide comment to the Parliamentary Joint Committee on Intelligence and Security (the Committee) on the Telecommunications and Other Legislation (Assistance and Access) Bill 2018 (the Assistance and Access Bill).

Although the Committee has chosen to allow an extremely limited period for review of the relatively lengthy Bill, its content and the significant issues that exist within its terms, has caused many Australians to be concerned about the future of their rights and freedoms.

This submission is made jointly with the assistance of and on behalf of the organisations and contributors below.

Endorsements

Australian Privacy Foundation

The Australian Privacy Foundation is the primary association dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues which pose a threat to the freedom and privacy of Australians.

Digital Rights Watch

Digital Rights Watch is a charity organisation founded in 2016 whose mission is to ensure that people in Australia are equipped, empowered and enabled to uphold their digital rights. We stand for Privacy, Democracy, Fairness & Freedom in a digital age. We believe that digital rights are human rights which see their expression online. We educate, campaign, lobby and advocate for a digital environment where individuals have the power to maintain their human rights.

Electronic Frontiers Australia

Electronic Frontiers Australia Inc. (“EFA”) is a non-profit national organisation that has been promoting and protecting digital rights (civil liberties) in Australia since it was established in January 1994. EFA serves to protect and promote the civil liberties of users of computer based communications systems and of those affected by their use.

Future Wise

Future Wise is an independent policy and advocacy organisation, founded in 2014, which focuses on the interactions between technology, healthcare, education and their effects on society.

Access Now

Access Now is an international organisation that defends and extends the digital rights of users at risk around the world. By combining innovative policy, user engagement, and direct technical support, we fight for open and secure communications for all.

Blueprint for Free Speech

Blueprint for Free Speech is an Australian-based, international not-for-profit organisation supporting freedom of expression.

GetUp!

GetUp is one of Australia's largest campaigning communities, with over 1 million members. GetUp creates a thriving democracy by giving everyday people the chance to make extraordinary impact – online, across the airwaves, and in the streets. GetUp members want to create a country of active citizens, not passive consumers, and they set our movement's agenda on issues they care about, in the fields of Climate Justice, Human Rights, Racial Justice, Economic Fairness and Democratic Integrity.

Contributors

Dr Adam Molnar

is a Lecturer in Criminology at Deakin University, where he is a member of the Alfred Deakin Institute for Citizenship and Globalisation and the Centre for Cybersecurity Research and Innovation. He conducts research at the nexus of technology and law enforcement, with a particular focus on access and use of digital evidence and the associated impacts for rights, due process, and information security.

Lizzie O'Shea

is a lawyer and writer. She has a background working in public interest litigation and recently served as the Human Rights and Corporate Responsibility Fellow at Columbia University in New York. Lizzie is a board member of Digital Rights Watch.

Dr Monique Mann

is the Vice Chancellor's Research Fellow in Technology and Regulation at the Faculty of Law, QUT. Dr Mann is advancing a program of socio-legal research on the privacy and human rights implications police technology and transnational online policing. She is on the Board of Directors and Co-Chair of the Surveillance Committee of the Australian Privacy Foundation and the Advisory Council of Digital Rights Watch Australia.

Angus Murray

is a practicing solicitor and human rights advocate. He is a Vice-President of the Queensland Council for Civil Liberties and the Chair of Electronic Frontiers Australia's Policy Committee. His academic work has focused on the interaction between the right to privacy and the enforcement of intellectual property law.

Peter Tonoli

is an information technology specialist at the University of Melbourne, and Senior Technical Fellow at Blueprint For Free Speech. Peter's interests include teaching journalists how to protect their sources, and teaching young adults in safeguarding their online privacy. Peter is a board member of Electronic Frontiers Australia, and Director of Internet Australia.

Bruno Watt

is a cloud, web and security architect with extensive experience in operations, engineering and architecture. His academic work has focused on standardisation in software engineering practises, automation and API architecture. He has worked on the front lines of the emerging cloud in Infrastructure, FinTech and Cybersecurity spaces. He is the Managing Director of a small Cloud Architecture consultancy, Hypermedia Tech.

Dr Suelette Dreyfus

is a Specialist at the School of Computing and Information Systems, The University of Melbourne. Her research examines technologies that can improve institutional accountability and transparency, as well as studying public attitudes to digital and non-digital integrity systems. She is also Executive Director of Blueprint for Free Speech.

Introduction

On 14 August 2018, the Department of Home Affairs released an exposure draft of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* ("**the Bill**"). By gaining access to an exceedingly broadly defined class of 'designated communication providers' and encrypted data, the Bill aims to limit the exploitation of communications technology by terrorist organisations, child sex offenders and criminal organisations. Whilst the protection of the Australian community is vital, it is incumbent on Government to ensure that this is achieved in a manner which is necessary and proportionate and that does not threaten to do more harm to security than good.

Submissions to the exposure draft closed on the 10th of September 2018. Less than two weeks after the close of submissions, the Minister of Home Affairs Peter Dutton introduced a largely unchanged bill, which was immediately referred to the Parliamentary Joint Committee on Intelligence and Security. It is clear from this incredibly short turnaround from the closing of submissions on the exposure draft and the introduction of the Bill into the Lower House that the Australian Government had absolutely no intention of meaningfully engaging with experts or civil society on an issue that is central to Australia's digital critical infrastructure. The actions by the Australian Government in this "consultative process" show an alarming disregard of, and disrespect for, the fundamental principles of a liberal democratic society. The Bill is being pushed forward with minimal consultation, and in the face of widespread criticism from both Australian and international civil society, as well as the community of academic experts with deep knowledge in this field. Additionally there have been substantial concerns raised by technology companies large and small, and industry associations, many of whom provide significant employment and technology innovation.

This Bill creates extremely broad powers with almost no oversight and without any substantive justification. The possibility that such powers might be needed in future is not a proper basis for the making of laws. Among other things, the Bill effectively enacts insecurity by design, which will almost certainly create additional obstacles and exclusions for Australian companies seeking to operate in EU markets.

We recommend that the Australian Parliament reject the Bill wholesale, as this is the most appropriate response to the draft in the view of the authors of this submission.

The remainder of this submission should be read with this recommendation in mind.

We have numerous serious concerns with specific elements of this Bill, in particular that it:

1. Introduces a seemingly scopeless definition of “designated communication providers”;
2. Increases the obligations on communication providers to assist with law enforcement agencies;
3. Increases the powers of law enforcement to use and apply the currently available search and seizure warrants; and
4. Introduces covert computer access warrants enabling law enforcement to search computers and electronic devices without due consideration of the ancillary risks to cybersecurity, due process, and and human rights.

The Bill grants the Director-General of Security, the chief officer of an interception agency and the Attorney-General additional powers to issue new types of orders. These include, directly and indirectly, forcing communications and technology companies to provide information about how networks are built and how information is stored, or to directly access encrypted data if they have a key. Taking this further, the Bill also grants the power to compel companies to engage in actively building new tools and mechanisms at the request of law enforcement agencies.

There is no warrant or oversight process proposed other than that these orders must be “reasonable and proportionate.” While the government has pointed to the potential for people to challenge in the courts, there is no outline of what this process will be or how the courts will be equipped to handle them. Indeed, this would require knowledge of the use and deployment of these new powers and, within the ambit of the Bill, it seems unlikely that this would be possible for end-users affected by the operation of this Bill. The powers within the Bill prevent people from revealing any information about any order they receive – with fines and jail time for those who do speak out.

The legislation also does not seem to be limited by what “assistance” organisations can be ordered to do. The government claims the legislation specifically forbids activities that would provide a ‘systemic weakness or vulnerability’ into an encrypted system. However, the kind of operation that the government is planning doesn’t require an active creation of a weakness, instead opting for an end-point activation.

Most encrypted services allow you to have multiple devices such as a phone and a computer, which can be end-to-end encrypted between all endpoints. If the government could secretly add a new device to that conversation without your knowledge, it would be building a new door into that encrypted communication.

An organization, whether Australian or not, that fails to comply with a notice can be fined $10,000,000. An individual can be fined up to $50,000 and, depending on the circumstances, can face up to 10 years in prison. The Bill’s wide remit means companies with even minimal connection to Australia could be subject to notices and the corresponding punishment.

This submission contains 38 recommendations pertaining to specific measures in schedules 1, 2 and 3 of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*.

Schedule 1
Obligations to Provide Information

The definition of designated communications provider is too broad

The Bill creates a new and broadly defined concept of “designated communications provider” pursuant to section 317C. It covers all the entities that would be expected for the purposes of achieving the objects of the Bill, such as software developers and hardware manufacturers. Pursuant to s. 317D(2), it also covers anyone who hosts a website in Australia.

The scope of the powers included in the Bill would allow an agency to seek access from any person providing or facilitating the provision of material over the internet. The list of possible entities is endless, and may include banks, media companies, specific journalists, insurers, civil society organisations, law firms, universities and most small and large businesses.

This has been confirmed by the office of the former-Law Enforcement and Cyber Security Minister, Angus Taylor. In a comment to the Australian Financial Review, a spokesperson confirmed that the laws would apply to "any entity operating a website".[1] She indicated that “[t]he scope of the laws is deliberately broad to adequately reflect the range of entities that contribute to the supply of communications in Australia.” [2]

The justification for this position appears to be that such broad reaching powers would better protect the integrity of communications systems. The spokesperson further noted that “securing assistance at different points in the communications supply chain, and from different providers in this chain, assists agencies to access evidence of criminal conduct without fundamentally impacting the security of communications." This position, however, is misguided and underestimates the risk of such a provision. The nature of the powers set out in the Bill are so broad in potential application that they undermine trust in all range of digital services and opens up the potential for abuse and misuse.

There is also a real prospect that, due to the potential compliance costs associated with voluntary assistance and compliance with technical assistance notice and technical capability notices, there will be a substantial financial cost to Australian consumers. It is not clear from the Bill how the compliance costs will be met by start-up and small web and application based businesses. It is submitted that the Committee ought to clearly clarify that the Bill may stifle the innovation culture that Government has attempted to establish in Australia.

---

[1] Cyber security laws to cover all businesses, Angus Taylor confirms
https://www.afr.com/news/cyber-security-laws-to-cover-all-businesses-angus-taylor-confirms-20180814-h13zdo

[2] Ibid.

Recommendation 1

The scope of the application of “designated communication provider" as well as "eligible activities" should be significantly reduced, and be defined in a way that is referable to the objects of the proposed law.

The list of acts or things is too broad

The list of “*acts or things”* that a designated communications provider can be asked to do under section 317E is broad. It encompasses numerous activities that could serve to undermine the strength of encrypted systems (notwithstanding section 317ZG addressed below). The list does not bear any relation to the object of the Bill. It should be narrowed and reduced in scope, to indicate that the act or thing must be targeted for a specific purpose, rather than generating a generalised capacity.

Indeed, the provisions governing technical capability notices are the most broad of all, given that the list of acts or things does not apply to technical capability notices (the possible acts or things are not limited to this list under section 317T (7)).

Recommendation 2

The list of acts or things should be reduced in scope, and be targeted to avoid creating a general capacity to undermine encryption.

Recommendation 3

The statutory list of act or things should be exhaustive for the purposes of technical assistance notices and technical capability notices.

There is insufficient oversight in the Bill for such broad powers and only limited reporting provisions

There is no provision for judicial oversight in respect of the giving of technical assistance requests under Division 2, technical assistance notices under Division 3 or technical capability notices under Division 4. This is a significant difference when compared to the *Investigatory Powers Act 2016* (UK), which contains a similar legal framework but is subject to judicial oversight. This is out of step with what the public would expect for such a serious set of powers. It opens up the powers to abuse and limits that capacity for decision makers to be held accountable for decisions made under these divisions.

Indeed, there is no way for any user of any digital platform or product to know whether the company responsible for this service or product has be issued with or complied with a request or or notice. There is only very limited reporting requirement under section 317ZS in respect of

technical assistance requests, technical assistance notices and technical capability notices. There are no reporting requirements in respect of requests or notices that were renewed, varied or expired, let alone to which agency and for what purpose. There are no reporting requirements for technical assistance notices and technical capability notices that have been revoked. This makes it impossible for the public to know the extent to which these powers have been used and whether they are fit for purpose.

The Bill allows for the disclosure of aggregate statistical information in respect of technical assistance requests, technical assistance notices and technical capability notices under section 317ZF(13). However this is not a requirement, it only creates authority to disclose the information and it cannot be broken down by agency or in any other way. This means that the statistics become almost meaningless as a tool of public accountability.

The relevant objective for which request and notices are given (see section 317E(5), 317L(2) and 317T(3)) is too broad. It includes enforcing the criminal laws in force in a foreign country, without reference to any analysis as to whether those laws are also criminal laws in Australia. This is a serious problem and has the potential to violate Australia's long-standing position on issues such as the death penalty.. This represents overreach and foreshadows a rightful concern about "scope creep" associated with the object and intent of the Bill.

Recommendation 4

Technical assistance requests, technical assistance notices and technical capability notices should be subject to judicial oversight.

Recommendation 5

Section 317ZS should be redrafted to include technical assistance requests.

Recommendation 6

There should be regular public reporting requirements in addition to section 317ZS in respect of how and when technical assistance requests, technical assistance notices and technical capability notices have been renewed, varied and expired, whether they were complied with, and whether they have been revoked.

Recommendation 7

There should be regular public reporting requirements in respect of technical assistance requests that have been refused and have been substantially reproduced in a subsequent technical assistance notice.

Recommendation 8

Reporting under section 317ZF(13) should be made mandatory.

Recommendation 9

The definition of relevant objective should be reduced in scope.

The list of interception agencies is too broad

The list of interception agencies includes, among other bodies, the Police Force of a State or the Northern Territory and various state anti-corruption commissions. The chief officer of an interception agency can issue technical assistance requests and technical assistance notices directly, without any oversight even of the Attorney General, let alone a judicial officer. (Technical capability notices are channelled through the Attorney General under s 317T.)

It is unclear whether any steps have been taken to ensure that such officers have the requisite training or resources in place to understand cryptography and the risks to encrypted systems that may arise as result of such a request or notice. There is also no evidence that the interception agencies have appropriately secure methods for the storage of any information about assistance provided under the Bill, to avoid such information falling into the wrong hands. For these reasons, all requests and notices should be approved by the Attorney General.

Recommendation 10

All requests and notices sought by an interception agency should be made by the Attorney General (as is currently the case for technical assistance notices under s317T).

There is no requirement to consider the public interest in the decision-making criteria

There is no decision-making criteria for technical assistance requests at all.

The decision-making criteria set out for technical assistance notices and technical capability notices is too narrow (sections 317P and 317Q(10); sections 317V and 317X(4)). The decision-making criteria do not incorporate any kind of consideration of the public interest. Nor is the scope of what is reasonable and proportionate defined. While we note the inclusion of further criteria under s 317AZZ for technical assistance notices and s 317RA for technical capability notices, these are insufficient as there is no mention of the public interest or best practice in respect of digital security. Further, this provision does not apply to technical assistance requests, without explanation.

Australians have legitimate reasons for being concerned that such decisions may differ from commonly held views of what is reasonable and proportionate. Recent events that substantiate this claim include the controversy concerning the public disclosure of a writer’s personal information after she wrote an article critical of Centrelink’s debt recovery program and the scandal associated with the Australian Federal Police accessing a journalist’s metadata to identify and prosecute the journalist's sources.

The public has repeatedly demonstrated it is concerned about the way in which government makes use of broad ranging powers to access and analyse information, exercised without scrutiny or safeguards.

The decision-making criteria does not also consider the impact of the notice on the integrity of digital infrastructure or consideration of best practice. Such a consideration might require consultation with technology professionals, which would be a useful contribution to the decision making process in such a technical field (this is addressed further below).

Recommendation 11

There should be decision-making criteria for technical assistance requests.

Recommendation 12

The decision-making criteria should include consideration of the public interest and the impact on the integrity of Australia's digital infrastructure, and should provide for the decision maker to consult with technical professionals with suitable qualifications in making a decision.

Recommendation 13

s. 317P(a) should be amended to include an obligation that the requirements imposed by any notice is reasonable and proportionate to the legitimate privacy expectations of the subject individual and the Australian community.

The consultation and assessment provisions included in the Bill are too narrow

Section 317W sets out a consultation provision for technical capability notices which allows for the recipient of the notice, jointly with the Attorney General, to appoint a person to assess whether the proposed technical capability notice would contravene section 317ZG. This provision is designed to substantiate the protection offered by section 317ZG, which is a welcomed update from the exposure draft. However, the provision is too limited in scope and needs to be refined.

The consultation and assessment process should also apply to technical assistance notices. In the context of our submission in respect of interception agencies (see Recommendations above), we submit that all provisions that apply in respect of the giving, consulting and assessing of technical capability notices also apply to technical assistance requests.

The costs of appointing a person to provide an assessment of a notice may fall to the designated communications provider under these provisions, as there is no guarantee that the Commonwealth will pay them. This may create a disincentive, particularly among smaller businesses, to appoint a person to assess the notice. This disincentive should be removed in order to promote best practice in relation to consultation and assessment.

Recommendation 14

The provisions applicable for the giving, consulting and assessing included of technical capability notices should also apply to technical assistance notices.

Recommendation 15

The costs of consultation should be borne by the Commonwealth.

The compliance and enforcement provisions make no provision for the public interest

Sections 317ZA and 317ZB require that carriers or carriage service providers and designated communications providers comply with technical assistance notices and technical capability notices, and make failure to do so a civil penalty provision. The civil penalty provisions also extend to any person who does certain things under section 317ZA(2). This provision does not include any knowledge requirement (in relation to the technical assistance notices and technical capability notices). This creates the potential for a person to be be unknowingly in breach of section 317ZA(2) and still be subject to a civil penalty provision.

There is no provision for refusing to comply with technical assistance notices and technical capability notices on the basis of the public interest, in general or specifically.

Further, certain disclosures about technical assistance requests, technical assistance notices and technical capability notices that are made by specific people under Division 6 are also subject to the penalty of imprisonment. Again, there is no provision for making disclosures in the public interest. In particular, we note that any person appointed to assess a technical capability notice under s 317W(7) is also captured by this provision, which is alarming given that there may be cases in which their recommendations have been ignored.

These are highly risky provisions in a context in which broad powers are being granted to give such notices, creating the potential for abuse. The protection of the public interest, including the protection of digital infrastructure, should be a defence to the civil liability provisions under Division 5 and 6.

Recommendation 16

Section 317ZA(2) be redrafted to specifically include a subjective knowledge requirement.

Recommendation 17

The requirement to comply with technical assistance notices and technical capability notices should include a public interest component, including as a basis for refusing to comply with such a notice.

Recommendation 18

Disclosures about technical assistance requests, technical assistance notices and technical capability notices -- including made by persons involved in assessing technical capability notices -- made in the public interest should be excluded from the application of Division 6.

The limits imposed on the powers set out under the Bill are insufficient to protect the public interest

Division 7 sets some limits on the powers conferred by the Bill. Technical assistance requests are not included in the scope of Division 7, and there is no clear justification for this.

The Bill limits the capacity to issue technical assistance notices and technical capability notices that have the effect of creating a systemic weakness or preserving systemic vulnerability under section 317ZG. Systemic weakness is not defined. While we note there are potential difficulties in defining such a term, the absence of a definition renders the section virtually meaningless. Consultation with appropriately qualified experts in cryptography may be a useful addition into the regime as a safeguard. Further, the limit does not impose any requirement on any agency to disclose systemic vulnerabilities to designated communications providers.

An example of the importance of agencies disclosing systemic vulnerabilities to communications providers is the case of the WannaCry Ransomware Attack. WannaCry was a computer worm with embedded ransomware which infected over 300,000 computers worldwide, including National Health Service computers in the UK. This meant medical professionals were unable to access records, and ambulances were diverted, among other things. WannaCry propagated through the internet, using a systemic vulnerability in Microsoft Windows, called ETERNALBLUE, internally discovered and developed by the US National Security Agency. ETERNALBLUE was then surreptitiously leaked from the NSA, and publicly released. If the NSA had disclosed, on initial discovery, the ETERNALBLUE vulnerability to Microsoft, it is likely that there would have been significantly lower impact on computers worldwide.

Section 317ZG does not create a defence to the civil penalty provision associated with a failure to comply with technical assistance notices and technical capability notices, which might be expected if this limit was designed to be meaningful.

Recommendation 19

Systemic weakness should be defined.

Recommendation 20

Technical assistance requests should be included in the application of Division 7.

Recommendation 21

The Bill should specifically require that agencies disclose systemic vulnerabilities if they are identified.

Recommendation 22

Section 317ZG should be redrafted to serve as a defence to compliance with technical assistance notices and technical capability notices.

Recommendation 23

A TAN or TCN must not have the effect of requiring the DCP to implement or build a systemic weakness, systemic weakness or anything that compromises the integrity of the service.

Schedule 2
Covert Computer Access Warrants

The use of computer access warrants, more commonly referred to as 'government hacking' or 'computer network operations', are among the most intrusive investigatory powers that governments have at their disposal. The increased use of encryption technologies has been cited by law enforcement as a primary barrier to lawful access to digital evidence, which as a result, has informed a strong push among governments around the world to rapidly formalise new hacking powers in order to access digital evidence.[3]

While we appreciate the extent to which encrypted communications can sometimes introduce friction into intelligence and criminal investigations, we encourage much greater evidence-based discussion on these matters as a vital starting point for any legislative reform. Recent survey research from the US-based Centre for Strategic & International Studies indicates that a number of other issues are more likely to frustrate law enforcement's ability to effectively access, analyse, and utilise digital evidence in their cases.[4] These included an "inability to effectively identify which service providers have access to relevant data" and additional "difficulties in obtaining sought-after data". These two challenges "ranked significantly higher" than any other challenge including frictions brought about through the use of encryption technologies.[5]

Furthermore, the use of hacking introduces a number of ancillary risks to the security of digital communications that everyday law-abiding Australians rely upon. The potential ramifications of a policy that disproportionately and unnecessarily favours computer network operations reach well beyond the intended target.[6] A clear eyed assessment of these risks and impacts have thus far been missing from public debate to determine the necessity and scope for measures proposed in Schedule 2.

[3] IACP Summit Report. 2015. Data, Privacy and Public Safety: A Law Enforcement Perspective on the Challenges of Gathering Electronic Evidence. http://www.theiacp.org/portals/0/documents/pdfs/IACPSummitReportGoingDark.pdf
[4] Carter, W.A. and Daskal, J.C. 2018. "Low Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge", CSIS, Report available at: https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180725_Carter_DigitalEvidence.pdf?tAGR_DvxRdp0RspiGYNGcGKTUjrGY3rN
[5] Carter and Daskal, p.5
[6] Pfefferkorn, R. 2018. Security Risks of Government Hacking. The Centre for Internet and Society at Stanford Law School. Report. https://cyberlaw.stanford.edu/publications/security-risks-government-hacking

We insist that legislative forbearance be exercised concerning Schedule 2 which includes a prohibition on any new provisions regarding the government use of computer access warrants, until a broad based expert working group can be formed to establish clearer protocols that include:

- the codification of government hacking powers in ways that introduce meaningful test for necessity and proportionality to mitigate dangerous and avoidable risks to cybersecurity security, human rights, and the privacy of law-abiding Australians
- the identification of higher-priority and less intrusive alternatives for accessing digital evidence, including enhanced education and training between the public and private sectors regarding existing lawful access to digital evidence
- an establishment of a comprehensive vulnerability equities management scheme
- purpose-built laws and policies to inform improvements in the adequacy of judicial review, oversight, and accountability
- clear measures to mitigate foreign policy implications

We insist that Schedule 2 be dealt with in a separate legislative Bill than Schedule 1. However, in a very tight schedule to provide response, we offer more specific comments on Schedule 2 below to be considered in a separate and discrete debate and discussion concerning government use of intrusive hacking powers.

Amendments to ASIO Act 1979

The proposed provisions in Part 1 s.4 are designed to "allow for interception where necessary to execute an identified person warrant in relation to accessing data held in computers" (EM, p.55). While we do not oppose the general need to introduce greater clarity and administrative efficiencies into statute with regards to investigatory powers concerning digital evidence (in this instance, streamlining the warrant process rather than sometimes requiring two separate warrants under different authorities of the Telecommunications (Interception and Access) Act 1979 (TIAA) and ASIO Act, a number of outstanding problems remain. The introduction of clarity into the warrant process should not overlook additional considerations in other areas of the ASIO Act 1979.

Ministerial Authorisation

Warrants conferred under the ASIO Act should be scrutinised and authorised by judicial authority rather than the Attorney-General. Procedural reliance on ministerial authorisation between Director-General and Attorney General to acquire warrants under the TIAA or ASIO Act entails an insufficient separation of powers that departs from accepted convention concerning checks and balances in modern liberal democratic societies. We propose s.25(a) of the ASIO Act as well as s.9 and S.9a of the TIAA 1979 (Part 2.2 Warrants) be amended to reflect a meaningful separation of powers, where the Director-General seeks warrant from an appropriate judicial authority.

It is our view that as new intrusive government powers are proposed, and as traditional rights are increasingly challenged through the technological complexities accommodate our everyday lives, equal weight to appropriate checks and balances should accompany these developments.

Recommendation 24

Require Director-General of ASIO to receive authorisation for computer access warrants through judicial authority, subject to clearer set of encoded protocols to enhance adequacy and minimise impacts on privacy rights cybersecurity of law-abiding Australians.

ASIO threshold requirements for Computer Access Warrants are weak

The test issue for the issuance of a warrant from the AG under s.25(a) of the ASIO Act 1979 is whether “he or she is satisfied that there are reasonable grounds for believing that access by the Organisation to data held in a computer (the target computer) will substantially assist the collection of intelligence” relation to a “security matter” (ASIO Act. s.25(a). To the extent that computer access warrants entail incredibly intrusive powers that yield serious collateral risks for the security and integrity of information communication infrastructures as a whole, these powers should be a last resort. In a country such as Australia that is unable to rely on clarity and policy guidance provided through judicial input via a formal bill of rights, the weighty demands placed on lawmakers to formalise rights-respecting norms within primary legislation amidst a rapidly evolving technological environment is untenable.

It is our view that primary legislation include revised thresholds that will condition any search and seizure powers an acceptable and limited manner. The threshold for ‘identified person warrants’, which requires a reasonable suspicion standard, which at a bear minimum, should be similarly applied to standard computer access warrants under s.25(a). Most importantly, as we elaborate on below, government should consider the utility and value of a formal bill of rights within wider technological developments that influence law enforcement and national security issues.

Legal Definition of Computer in ASIO Act and Surveillance Devices Act undermines proportionality and introduces unnecessary risks to cybersecurity

ASIO’s powers for computer access warrants were introduced as recently as 2014, in the National Security Legislation Amendment Bill (no.1). Part of these amendments involved the revision of the legal definition of a “computer” to include “one or more computers”, one or more computer systems”, “one or more computer networks”, or “any combination of the above” (ASIO Act, s.22). The warrants also authorised ASIO to use “any other computer or communication in transit to add, copy, delete or alter data...for the purposes of obtaining access to data relevant to the security matter and held on the target computer (National Security Legislation Amendment Bill (No.1) 2014 Explanatory Memorandum).

On the basis of this definition, in principle, a single computer access warrant can authorise authorities' use of invasive activities across of a broad range of devices and networks, from personal devices (such as mobile devices and tablets), to shared devices in a home such as Internet of Things (IoT) and routers, as well as entire businesses, university networks, telecommunications companies, or core internet infrastructure. The warrants also let ASIO use "any other computer or communication in transit to add, copy, delete, or alter data...for the purpose of obtaining access to data relevant to the security matter and held on the target computer" (National Security Legislation Amendment Bill (No.1) 2014, Explanatory Memorandum). The only binding limitation on ASIO powers under s.25(a) is if the operation would "cause any other material loss or damage to other persons lawfully using a computer". However, it remains to be defined what constitutes "material loss or damage" as it is unfortunately not set out in the Act.

As a jurisdiction without a formal bill of rights, Australia has few limitations regarding proportionality when it comes to the breadth and intrusiveness associated with how searches are facilitated through vastly different types of devices, networks, or infrastructure that are accessed during the execution of a computer access warrant.

If these powers are to be used, we insist that there must be greater granularity in the legal definition of "computer" as a means to codify a test for proportionality in such a way that offsets unnecessary and serious unintended consequences that can carry broad negative impact. For instance, while it may, under strict circumstances, be appropriate to remotely access an end-point device, remote access and interference with cloud-based services, businesses, or other 'server-' or 'router-side' shared networks should be avoided.

At the very least, we insist that far greater efforts must be made to understand and codify a range of factors informed by an evidence-based understanding of the ancillary impacts of computer network operations for cybersecurity and human rights. We insist that, in the present, legislative forbearance on this issue is both reasonable and necessary so that these issues can be addressed and included in future legislation.

Recommendation 25

Place a moratorium on government use of computer access warrants except in the most serious cases until further clarity on the ancillary security risks and impacts can be clarified through the clearer protocols proposed in Recommendations 10-20.

Recommendation 26

Provide further definitional clarity on "material loss or damage to other persons lawfully using a computer under" s.25(a) of the ASIO Act 1979.

Reporting Requirements

We support existing requirements in the ASIO Act that require the Director-General to report about instances where warrants issued under s.25, 25a, 27a, 27c, or 29, which have "materially interfered with, interrupted or obstructed the lawful use by other persons of a computer or other electronic equipment or a data storage device", including the addition of associated "concealment activities" (34(2)(b)). However, we insist that the Minister is not the appropriate venue for this reporting. We recommend that this reporting should be made directly to the Inspector-General of Intelligence and Security (IGIS) as well as the Parliamentary Joint Committee on Security and Intelligence (PJCIS).

Recommendation 27

The Director-General must report the above mentioned instances issued under s.25, 25a, 27a, 27c, or 29 directly to the IGIS and PJCIS. Information about these occurrences should be included in the IGIS annual reports.

Amendments to the Surveillance Devices Act 2004

We welcome the Government's attempt to clarify the Surveillance Devices Act 2004 (SDA) in relation to the present technological environment. We are of the view that the current structure of warrant categories under the SDA are ill-suited to reflect the current technological environment as it relates to existing investigatory methods. However, while the move to introduce "computer data access operations" 3(aaaa) could be regarded as a positive step to introduce some clarity to the Act, a number of additional problems remain. Again, while we insist that Schedule 2 be dealt with in a separate Bill given the complexity and impact of the matters involved, we provide initial detail and recommendations for future consideration below.

New Legal Definition of "Computer" under the Surveillance Devices Act 2004

The introduction of the new warrant category under the SDA is supplemented with a new definition of computer, the wording of which is derived from s.22 of the ASIO Act (EM, p.63). In the section above on amendments to the ASIO Act, we have addressed the serious shortcomings of the definition of 'computer', particularly given its implication for the public interest in cybersecurity and privacy rights, particularly in a jurisdiction without a formal bill of rights to provide further clarity and guidance on necessity, proportionality, and intrusiveness. While this new definition of computer under the SDA "takes into account the increasing use of distributed and cloud-based services for processing and storing data, and networks of computers through which data commonly passes and on which it is stored." (p.63), the desire to access a range of "networks under one computer access warrant" raises serious security and human rights risks.

We appreciate any potential friction facing law enforcement access to digital evidence during the course of their investigation (again, with the caveat that the main obstacles concerning digital evidence according to a recent US study show that the main problems facing law enforcement when it comes to accessing and using digital evidence is a lack of education and training concerning how to use already existing powers)[7]. We fundamentally disagree, however, with the restrictive scope of the discussion as presented in the explanatory memorandum (EM) concerning administrative challenges in the warrant process. The EM and draft Bill present an either/or choice when it comes to the warrant regime. On the one hand, issue one warrant for one device which is administratively cumbersome and unreasonable. On the other, issue one warrant that can be used to access a multiplicity of devices and networks regardless of their location, ownership, or degree of connection to the target under investigation. This latter option is the preferred government solution as reflected in the amendments, however, there is a significant amount of unexplored terrain that exists between these polarities.

We insist that more granular attention be paid to the question of proportionality, limitations, as they relate to more evidence-based understanding of the ancillary impacts on cybersecurity, privacy, and human rights. To accomplish this in a evidence-based fashion, we call for a coordinated expert advisory board that includes experts from law enforcement, industry, academics, and civil society to engage in a more detailed consultative role to facilitate law enforcement interest while simultaneously ensuring any new provisions are acted upon in a way that is similarly consistent with cybersecurity, privacy, and civil liberties.

While it may, under the most strict circumstances and subject to serious crime thresholds (minimum 7 years imprisonment as penalty), be appropriate to hack an end-point device, the ability to have unrestrained access to a range of networks, such as routers in businesses, religious organisations, health care providers, news media organisations, global communications providers such as Skype or WhatsApp, or other collectively interfaced environments is inattentive to the disproportionate risks to human rights and collective cybersecurity associated with the use of such broad and intrusive powers.[8]

Recommendation 28

Engage in legislative forbearance on computer access warrants under the SDA until greater evidence-based clarity concerning ancillary costs can be ascertained through a broad based expert advisory board comprising of law enforcement, academics, industry, and civil society.

[7] Carter, W.A. and Daskal, J.C. 2018. “Low-Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge,” Centre For Strategic & International Studies, Washington, DC.
[8] Herpig, S. 2017. Government Hacking: Computer Security vs. Investigative Powers: a comparative problem analysis supported by the Transatlantic Cyber Forum. Siftung Neue Verantwortung. See: https://www.stiftung-nv.de/sites/default/files/snv_tcf_government_hacking-problem_analysis_0.pdf

Proportionality and Limitations on Computer Access Warrants Under the SDA

Where any limitations on the proportionality and intrusiveness of computer access warrants under the SDA 2004 do exist, they are primarily set out by the issuing authority (whether a judge, magistrate, or member of the AAT) when determining the application. The SDA stipulates that when a computer access warrant is sought, the issuing authority "must have regard to the extent to which the privacy of any person is likely to be affected and the existence of any alternative means of obtaining the evidence or information sought to be obtained."

These considerations before the court are important facet to mitigate unnecessary impacts on human rights and privacy. However, they are overwhelmingly dependent on the adequacy of judicial decision-making, namely, that the issuing authority is both made aware of, and is able to meaningfully comprehend the privacy risks as they relate to technical complexities involved in executing the warrant. We insist that much clearer informational guidance be provided to the issuing authority, so that an appropriate determination concerning the intrusiveness and alternative means of obtaining the evidence can be provided.

This could take the form of education and training programs for judges and magistrates at Australian universities, the National Judicial College of Australia, or an equivalent body, to ensure that the laws may be applied fairly, evenly, and with necessary regard to how complexities of the technological environment are inextricably related to ancillary implications for privacy and human rights. In addition, we insist that courts should more regularly retain the services of *amicus curiae* or a public interest advocate when law enforcement agencies are applying for a judicial warrant under the SDA (this point can be equally applied to the importance of maintaining judicial adequacy under the ASIO Act 1979, as well as the Telecommunications Interception and Access Act 1979).

Recommendation 29

Establish training and education programs on relevant technological matters that maintain judicial adequacy under determinations of computer access warrants.

Balancing secrecy and transparency concerning disclosure of computer access technologies and methods as public cybersecurity vulnerabilities

Amendments to Section 47A of the SDA refer to the "protection of computer access technologies and methods". The aim of this new section is to provide enhanced secrecy and protection based on law enforcement determinations of "sensitive information relating to computer access technologies and methods in order to prevent its release into the public domain" (EM, p.79).

Under this provision, law enforcement assumes that any “disclosure is inherently harmful”, on the basis that “law enforcement capabilities are fundamental to ongoing investigations and their ability, including over the long term, to protect essential public interests, including national security and public safety”.

We appreciate the importance of concerns regarding operational secrecy of criminal investigations, however, the view that any “disclosure is inherently harmful” presents a fundamentally misguided view on the relationship between investigatory priorities and public safety when vulnerabilities and malware are used in computer access warrants. The use of computer network operations are unavoidably connected to a criminal economy that trades in an illicit market for computer exploitation.[9] The same vulnerabilities and exploits that are held in secret and used for law enforcement purposes can be similarly be exploited by other malicious actors, including foreign states, organised crime groups, or criminal individuals.[10] There is a pressing need to have a clear, evidence-based risk management decision-making framework concerning the balance between the secrecy of investigatory methods and the importance of maintaining public safety through digital communications. Such a policy surrounding disclosure should not be determined on an ad hoc basis by law enforcement absent best-practice evidence-based criteria, and instead, should be subject to rigorous independent research and clear policy guidance.

We insist that there must be a much more clear and independent evidence-based decision-making policy for guiding these considerations. Such a policy is more commonly known as a “Vulnerabilities Equities Policy” (VEP), which is designed to determine “whether, when, how, to whom, and to what degree the (US) Federal Government shares or releases information to a non-Federal entity about a vulnerability that is not publicly known”.[11] The US PATCH Act of 2017 is intended to guide sound legislative and policy development as a basis for balancing the needs of the intelligence community with transparency, accountability, trust, and public safety protections that are integral part of the security and integrity of information communication infrastructures. The US PATCH Act of 2017 includes considerations that include:

- Which technologies, products, systems, services, or applications are subject to the vulnerability;
- The potential risks of leaving the vulnerability unpatched or unmitigated
- The likelihood that a non-federal entity will discover the vulnerability; and
- Whether the vulnerability can be patched or otherwise mitigated.[12]

[9] Bellovin, S.M., Blaze, M., Clark, S. and Landau, S., 2014. Lawful hacking: Using existing vulnerabilities for wiretapping on the Internet. *Nw. J. Tech. & Intell. Prop.*, *12*, p.i.;
[10] Sales, N.A., 2018. Privatizing Cybersecurity. *UCLA L. Rev.*, *65*, p.620; Fidler, M., 2015. Regulating the Zero-Day Vulnerability Trade: A Preliminary Analysis. *ISJLP*, *11*, p.405.
[11] Caulfield, T., Ioannidis, C. and Pym, D., 2017, October. The US Vulnerabilities Equities Process: An Economic Perspective. In *International Conference on Decision and Game Theory for Security* (pp. 131-150). Springer, Cham.
[12] https://www.congress.gov/bill/115th-congress/house-bill/2481

Germany has dedicated an entire agency to manage and evaluate equities in vulnerability management and acquisition of government hacking tools.[13] We insist that similar discrete considerations be made to govern aspects associated with the execution of computer access warrants. Not only would an Australian VEP be an important step for maintaining an evidence-based decision making-criteria for determining public safety interests as they relate to both the investigation of serious crimes and cybersecurity, it could also be used to assist judicial determinations regarding computer access warrants under the ASIO Act, SDA, as well as more broadly as a useful instrument to guide cybersecurity policy more generally.

Recommendation 30

Establish a Vulnerabilities Equities Policy that consists of a broad-based body of experts to help guide knowledge about vulnerability management for future legislation and policy on a range of national security, public safety, and cybersecurity matters.

Reporting Under the SDA

A new subsection 49(2B) provides an obligation to report information pertaining to computer access warrants to the Minister. Under Paragraph 50(1)(g)(h) and (i), agencies are also required to report on “the number of warrants applied for and issued during the year and the number of emergency authorisations”, as well as the number of warrants and authorisations that were refused in that year, providing reasons for the refusal. The Attorney-General subsequently tables these reports on an annual basis to Parliament.

We welcome the requirement to similarly report on computer access warrants under the SDA. Given the technology-specific language of the warrant categories in the SDA, as innovations in the social and technological environment evolve it can become increasingly difficult to know how specific investigatory methods are meaningfully represented in the numerical figures of transparency reports. A disconnect between present day technical investigation methods and the warrant categories under the SDA remains a chronic impediment to meaningful understanding of the Minister’s annual reports. However, while the inclusion of a discrete category for computer access warrants provides some clarity in this regard the problem is owing to already existing practices in reporting.

In instances where authorities under the SDA apply for more than one category of warrant, they are reported under a category identified as “Composite / Multiple”. A brief examination of any SDA Annual Report shows a disproportionately high number of authorisations in the “Composite/Multiple” column compared with other warrant categories. Such manifold reporting undermines the ability for Australian Members of Parliament, as well as the public, to derive meaningful information from the reports.

[13] See: Central Authority for Information Technology in the Security Sphere (ZITiS) https://www.bmi.bund.de/DE/startseite/startseite-node.html;jsessionid=4E23A40881B9199883388AA0400E9781.2_cid295

Recommendation 31

Remove the “composite / multiple” reporting category for warrants, and ensure that any composite warrants are reflected in their singularly discrete categories to ensure more accurate reporting within the Minister’s SDA Annual Reports.

Enhanced Notification Regime for 3rd party impacts

Given imprecise legislative language in both the ASIO Act and SDA concerning the legal definition of “computer”, as well as the complex nature of executing computer access warrants as currently defined in relevant legislation, a number of ‘non-targeted’ parties (such as businesses, citizens, and government itself) can be impacted with government use of vulnerabilities and malware. While it is reasonable in certain instances that notice requirements be delayed through judicial authorisation in order to preserve the integrity of legitimate investigations, notification requirements remain an essential tool for transparency, accountability, and trust in government when such intrusive and potentially damaging powers are in use. Under the SDA there is no obligation to provide individual notice to either targeted or non-targeted parties whose personal property or business might be impacted through the use of a digital search. By contrast, Germany obligates relevant government bodies to notify both the target and all other affected parties impacted by a surveillance operations (which are, of course, subject to court approved delayed-notification if necessary). Obligation for a notification requirement in the context of computer access warrants would provide an requisite accountability mechanism that is necessary for complex investigations in online spaces.

Recommendation 32

Introduce a notification regime to inform affected parties about the use of a computer access warrant. Application for delayed notification regimes can be considered by an appropriate issuing authority based on reasonable criteria.

Amendments to the Telecommunications (Interception and Access) Act 1979

A number of amendments in the draft Bill pertain to the testing of interception technologies between security authorities and telecommunications carriers (Subsection 31(1), 31(A)1, 31(A)). These amendments are to provide authority for security authorities to work with carriers to test or develop interception technologies. Even though these practices are considered through the language of “ad hoc” “testing”, they can be just as intrusive depending on how they are performed.

In 2014, the Communications Security Establishment engaged in a “trial” exercise that facilitated the tracking of Canadian citizens through that country’s airport Wi-Fi check-points.

While this was similarly a “test”, it served as one of the most intrusive mass surveillance measures into the lives of Canadian citizens outside of conventional legislative and judicial protocol.[14] The definition of “test” should not be an excuse to evade proper mechanisms of transparency and accountability, which are essential for maintaining trust between the private sector, government, and law-abiding Australian citizens.

Recommendation 33

Greater oversight and accountability structures are required to facilitate any processes under Subsection 31(1).

Amendments to the *Mutual Assistance in Criminal Matters Act 1987* (Cth)

New ICTs present several challenges for the collection of digital evidence that may be stored extraterritorially in cloud computing services or on commercial servers located in other jurisdictions. Indeed, it is noted in the explanatory document that “investigations and prosecutions frequently involve criminal use of the internet and cross border storage of information. Australia’s mutual assistance framework is critical in enabling Australian and foreign authorities access to information necessary to conduct investigations and undertake criminal proceedings, amongst other things” (p. 61 of the Explanatory Document).

Proposed amendments to the Mutual Assistance in Criminal Matters Act 1987 (Cth) in concert with the other amendments in Schedule 2, aim to address the issue of trans-territoriality and ‘streamline’ processes for foreign law enforcement agencies to access information under the Surveillance Devices Act 2004 (Cth).

Amendments under part IIIBB - *Assistance in relation to data held in computers* “will allow foreign authorities to make a request to the Attorney-General to authorise an eligible law enforcement officer to apply for a computer access warrant for the purposes of obtaining evidence to assist in a foreign investigation or investigative proceeding.”

The purpose is to allow for Australian law enforcement to undertake Computer Network Operations or arrange access to data and other telecommunications information held in a computer on *their behalf* (although not within the jurisdiction of Australia). These are subject to specific restrictions, as noted on p.60 of the Explanatory Document.

- The request must relate to a criminal matter in foreign country that is punishable by max of imprisonment for 3 years, imprisonment or death penalty (where the Attorney-General may refuse the request if death penalty is involved);
- An investigation must have commenced in requesting country;

[14] https://www.cbc.ca/news/politics/csec-used-airport-wi-fi-to-track-canadian-travellers-edward-snowden-documents-1.2517881

- The requesting country must specifically request that the AG arrange for access to data held on the target computer;
- Computer must meet definition of ‘target computer’, restricted under proposed section of 15CC(2) of the Mutual Assistance in Criminal Matters Act 1987 (Cth) and where it is defined under the Surveillance Devices 2004 (Cth) Act.

However, the proposed amendments will create a process that operates to undermine established Mutual Legal Assistance Treaty (MLAT) arrangements that are already in place. MLAT operate to ensure evidence is admissible in criminal trials, and to uphold and protect any individual's due process protections. This is because jurisdictional authority for law enforcement activity is determined by physical geography or territory and it is incorrect to assume that the Internet renders national borders irrelevant. Domestic law enforcement agencies must follow MLATs to protect individual and due process rights, and to ensure evidence is admissible in the context of criminal trials. Territorial controls are important in protecting suspects from unbridled transnational surveillance.

It is widely recognised that MLATs are cumbersome, time consuming and inefficient, with potential to delay, limit and compromise the collection of digital evidence in cases involving serious forms of transnational criminal offending. Yet, they are of central international importance, as the unilateral collection of evidence by one nation can have significant political and diplomatic ramifications if it is believed that the sovereignty of another nation is negatively affected. Further, methods of streamlining international cooperation should be backed by a strong human rights framework which is entirely absent in the Australian context.

While the Attorney-General can request that some undertakings be made (that the evidence is used solely for the purposes of the investigation for which it is being sought or the destruction of a document or thing containing data obtained as a result of access under the warrant), there is no way for Australia to enforce these once the data has been provided to foreign law enforcement agencies.

Recommendation 34

Uphold or improve Mutual Legal Assistance Treaty (MLAT) processes in the transfer of digital evidence to foreign law enforcement agencies. In the case of investigations with an extraterritorial element there must be recognition that Australian police and data analysis procedures comply with established MLAT procedures;

Recommendation 35

Do not allow foreign law enforcement agencies to collect or access information about Australian citizens in the investigation of offences against foreign laws, and;

Recommendation 36

Do not allow foreign law enforcement agencies to collect or access information in cases which involve the death penalty.

Schedule 3
Amendments to Crimes Act 1914

Executing Computer Access Warrants

As part of the introduction of revised computer access warrants for police, subsection 3F2A and 3F2B state that that "The executing officer or constable assisting may copy, delete or alter data if necessary" to carry out the warrant. Limits on these activities, “subsection 3F(2C) provides that subsections (2A) and (2B) do not authorise the addition, deletion or alteration of data when those actions are likely to interfere with communications in transit or the lawful use by other persons of a computer, unless it is necessary to do one or more things specified in the warrant,” and that “under no circumstances is it authorised for material loss or damage to be caused to other persons lawfully using a computer.”

The exception--“unless it is necessary to do one or more things specified in the warrant”--means that powers for disruption, so long as they are defined by an affiant in the warrant, are able to be pursued. So long as judges sign off in advance, these powers might be applied very broadly, so long as they don’t contribute to “material loss or damage”. As previously mentioned, further definition on what constitutes “material loss” or “damage” should be spelled out in legislation. The ancillary implications, even within these limits however, are still significant. Powers for disruption, even if considered to be “noble cause” activities and spelled out in the warrant, can still hold the capacity to taint prosecutions, impede free speech, and weaken cybersecurity. These activities, even if they are spelled out in the warrant, can incentivise police ‘disruption’ of suspected threats before crimes are committed, rather than pursuing the a conventional course of criminal justice where the desired outcome is a criminal trial based on gathered evidence in criminal investigation.

Recommendation 37

Provide further clarity and limitations on legal definition of “material loss”, “damage”. Furthermore, clearer limitations on the use of active powers should be spelled out in legislation.

Compelled Assistance to Access Data Held in a Computer or Device

Subsection 3LA(5) splits the existing offence under 3LA into a ‘simple offence’ and ‘aggravated offence’ category. The simple offence in 3LA increases the penalty from two years imprisonment to five years imprisonment. The aggravated offence refers to when a serious offence is being investigated and an individual refuses to or cannot comply, and is subject to 10 years imprisonment. The main justification for increasing these penalties are to “reflect the significant harm to investigations and prosecutions caused by a person failing to assist law enforcement” (EM, p.98). Several problems are associated with this proposal.

By rearticulating what a warrant is intended to do (ie, moving from ‘an onus on government to investigate and collect evidence’, to ‘an onus on a specified person that is required to present evidence’), the proposal raises very serious issues in instances where the specified person in the warrant is unable to, or cannot, provide assistance.

In an era where passwords and account credentials are routinely forgotten, or where an individual is locked out of a device due to security features from the product or service provider, or where an individual knows one part of the password but not the second factor (in contexts where 2 Factor Authentication is used), these laws hold serious risk to be misapplied with particularly damaging consequences. For this reason, other liberal democracies, such as Canada and the United States uphold an individual’s right to be free from government compelled speech, which maintains a privilege against self-incrimination. Moreover, it is imperative that government demonstrate the effectiveness and utility of already existing provisions in 3LA, particularly as a means to justify significant increases in associated penalties. Such a provision holds serious potential to negatively impact innocent persons.

Recommendation 38

Withdraw this provision and give further consideration to the risks of government compelled speech and a substantive right to be free from self-incrimination by lawmakers.

The organisations and contributors appreciate the Committee's consideration of this submission.

We wish to reiterate that though we welcome the use of an exposure draft and the opportunity to comment, and this subsequent committee process, the time available was constrained and other contributors and organisations have been unable to engage. We strongly encourage the Government and the Minister to make more time available for community participation as this legislation is being developed.

For any further information or follow-up, please contact Digital Rights Watch Campaign Manager David Paris to be directed to the submission contributor best able to assist you.