UNITED NATIONS
HUMAN RIGHTS
SPECIAL PROCEDURES
SPECIAL RAPPORTEURS, INDEPENDENT EXPERTS & WORKING GROUPS

PALAIS DES NATIONS • 1211 GENEVA 10, SWITZERLAND
www.ohchr.org • TEL: +41 22 917 9543 / +41 22 917 9738 • FAX: +41 22 917 9008 • E-MAIL: registry@ohchr.org

Mandate of the Special Rapporteur on the right to privacy

REFERENCE:
OL AUS 6/2018

12 October 2018

Excellency,

I have the honour to address you in my capacity as Special Rapporteur on the right to privacy, pursuant to Human Rights Council resolution 37/2.

My mandate is focused upon, amongst other things, 'challenges in relation to the right to privacy and to make recommendations to ensure its promotion and protection, including in connection with the challenges arising from new technologies'.[1] In this vein, I write in relation to the proposed Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (the Assistance and Access Bill). I draw upon the detailed work I have been undertaking in security and surveillance, and corporations' use of personal data. I have been ably assisted by two taskforces whose members are experts drawn from across the world, and from both the public and private sectors (including the major tech companies).

The significance of this Bill and its profound impact upon human rights, most specifically, the right to privacy, has prompted me after careful consideration to write directly to you. I will also provide my submission to the responsible Minister the Hon. Peter Dutton MP and the Joint Parliamentary Committee on Intelligence and Security and the Parliamentary Committee on Human Rights. This is due to my concerns, not just about the Assistance and Access Bill, but the larger context from which the Bill derives and within which it will be decided.

I note since the attacks on the United States of America on 11 September 2001, 70 counter-terrorism laws have been enacted by the Australian Parliament.[2] Concern has been expressed at the international level about trends in Australia's human rights

1 Human Rights Council Resolution 28/16

2 Williams, G., Dean, the Anthony Mason Professor, Scientia Professor at UNSW Law, *National security isn't served by convenient bipartisanship*, The Australian June 11, 2018 https://www.theaustralian.com.au/opinion/national-security-isnt-served-by-convenient-bipartisanship/news-story/0262c591634cbd6ee5cdfbbaad9ed5d8.

Her Excellency
Ms. Julie Bishop
Minister for Foreign Affairs

performance. This includes the United Nations Human Rights Committee who requested the Australian Government to reconsider the legality of its power in certain areas.[3] And most recently, by the incoming United Nations High Commissioner for Human Rights, Michelle Bachelet.[4]

The context for the Assistance and Access Bill includes other legislation that has been, or is planned for introduction into the Australian Parliament by the Australian Government, as well as those proposed by other Members of the Parliament.

A number of Australian Bills challenging basic liberties and human rights including the right to privacy, have been passed. I note amongst others, that the amendments to the *Telecommunication Intercept and Access Act 1979*. These have been criticised as too broad and potentially undermining the privacy of Australians.[5]

Other examples from the more recent legislative program include the Foreign Influence Transparency Scheme Bill 2018; Communications Legislation Amendment (Online Content Services and Other Measures) Bill 2017; Australian Border Force Amendment (Protected Information) Bill 2017; Criminal Code Amendment (High Risk Terrorist Offenders) Bill 2016, and Counter-Terrorism Legislation Amendment Bill (No.1) 2016.

I note also that the Joint Parliamentary Committee on Intelligence and Security has been reviewing the Identity-matching Services Bill 2018; the Australian Passports Amendment (Identity-matching Services) Bill 2018; the National Security legislation Amendment (Espionage and Foreign Interference) Bill 2017; ASIO's Questioning and Detention Powers 2018; Police Stop, Search and Seize Powers, the control order regime and the preventive detention order regime, as well as the Home Affairs and Integrity Agency legislation Amendment Bill.[6] All of which have direct or indirect impacts on human rights and civil liberties.

Additionally, I have noted the public commentary on the dynamics of bi-partisanship in this Joint Parliamentary Committee and its perceived impact on the introduction of new national security measures.[7]

---

3 In 2009, the United Nations Human Rights Committee commented on the vagueness of the definition of 'terrorist act' within counter-terrorism legislation (Anti-Terrorism Act (No. 2) 2005) and requested that Australia reconsider the legality of its power to detain people without access to a lawyer and in conditions of secrecy. The Committee was also particularly concerned at the reversal of the burden of proof contrary to the right to be presumed innocent; the fact that "exceptional circumstances", to rebut the presumption of bail relating to terrorism offences, are not defined in the Crimes Act, and; the expanded powers of the Australian Security Intelligence Organization (ASIO), including so far unused powers to detain persons without access to a lawyer and in conditions of secrecy for up to seven-day renewable periods.

4 https://www.theguardian.com/law/2018/sep/11/affront-to-human-rights-top-un-official-slams-australias-offshore-detention?utm_source=esp&utm_medium=Email&utm_campaign=Australia%27s+Morning+Mail+2017&utm_term=285283&subid=25666105&CMP=MorningMail_AU

5 Wilson, M., and Mann, M. *Police want to read encrypted messages, but they already have significant power to access our data*. The Conversation, 7 September 2017 viewed 10 September 2018 at https://theconversation.com/police-want-to-read-encrypted-messages-but-they-already-have-significant-power-to-access-our-data-82891

6 Australian Parliament, Joint Parliamentary Committee on Intelligence and Security at https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/completed_inquiries

7 Williams, G. as above in Footnote 2.

In contrast to this legislative program, I note that the proposed introduction of legislation for an Australian Bill of Rights 2017 is not proceeding. Nor is the Independent National Security Legislation Monitor (Improved Oversight and Resourcing) Bill 2014, or the Intelligence Services Amendment (Enhanced Parliamentary Oversight of Intelligence Agencies) Bill 2018.[8] Bills which, while not proposed by the Government, are relevant to the mix of measures that facilitate national security including managing their potential adverse impacts upon the democratic principles of the society the Bills seek to protect.

The Australian Assistance and Access Bill

In Australia, as I understand it, the legal basis for information collection remains in the *Telecommunication Intercept and Access Act 1979* and the *Intelligence Services Act 2001*. Both were designed before information was routinely encrypted. In relation to the 2015 amendments to the telecommunication interceptions legislation, I note the Second Reading Speech given by the then Minister of Communications, the Honourable Malcolm Turnbull, MP, stressed that service providers will not be required to retain content, the substance of any communication including subject lines, social media posts, web browsing history, location records, and so forth.[9] Interviews and public statements by the Minister and the then Attorney General asserted that it was not the content that was important.[10]

The 2015 amendment of the *Telecommunication Intercept and Access Act 1979*, with its unprecedented requirement that metadata be retained for up to two years, was said to come with "new, enhanced safeguards including independent oversight, review after three years....", and the "government's commitment to ensuring that access to sensitive and personal information by agencies is strictly controlled through robust accountability processes." Lastly, I note that then, as now, national security is invoked as the justification for incursions into the right to privacy and other democratic freedoms, such as freedom of expression.[11]

The need for the Assistance and Access Bill is said to arise from the challenges posed by encryption to law enforcement although the exact nature of these challenges is unspecified.

---

8 https://www.aph.gov.au/Parliamentary%20Business/Bills%20Legislation/Bills%20not%20passed%20current%20Parliament. The Intelligence Services Amendment (Enhanced Parliamentary Oversight of Intelligence Agencies) Bill 2018 as referred to the Senate Standing Committees on Finance and Administration, while listed in the 'Bills Not Progressing'.https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Finance_and_Public_Administration/IntelligenceServices

9 Australian Parliament Hansard, House of Representatives, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 Second Reading Speech Thursday, 30 October 2014 Thursday, 30 October 2014 HOUSE OF REPRESENTATIVES, p12560, the Minister of Communications, Turnbull, Malcolm, MP. http://parlinfo.aph.gov.au/parlInfo/genpdf/chamber/hansardr/4a3ea2e7-05f5-4423-88aa-f33e93256485/0010/hansard_frag.pdf;fileType=application%2Fpdf

10 Suzor. N., Pappalardo, K. and McIntosh, N., *The passage of Australia's data retention regime: national security, human rights, and media scrutiny,* Internet Policy review, Journal of Internet Regulation, Vol 6, Issue 1, March 2017.

11 Second Reading Speech as above.

Encryption has both positive and negative aspects. As stated by the Australian Department of Home Affairs, encryption can "protect private, commercial and Government data and make the communications and devices of all people more secure. However, these security measures are also being employed by terrorists, child sex offenders and criminal organisations to mask illegal conduct."[12]

Unfortunately, measures to address the challenges of encryption, can similarly have both positive and negative effects. This duality requires precision in legislative drafting if unintended adverse consequences are to be avoided.

I am familiar with the public commentary on the Assistance and Access Bill and am aware that submissions have been made by both domestic and international authors. I note most particularly that of the Australian Human Rights Commission and also that of the coalition of civil society organisations comprising Digital Rights Watch with the Australian Privacy Foundation, Electronic Frontiers Australia, Future Wise, The Queensland Council for Civil Liberties, The New South Wales Council for Civil Liberties, Access Now and Blueprint for Free Speech made a joint submission to this consultation. I commend the points and recommendations provided by these submissions – amongst others. They are well made and require serious consideration and adoption.

I especially commend the points made by my colleague, Professor David Kaye, Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, whose letter dated 11 September 2018 I attach as an annexe in an attempt not to replicate too many of his comments in my own.

In my considered view, the Assistance and Access Bill is an example of a poorly conceived national security measure that is equally as likely to endanger security as not; it is technologically questionable if it can achieve its aims and avoid introducing vulnerabilities to the cybersecurity of all devices irrespective of whether they are mobiles, tablets, watches, cars, etc., and it unduly undermines human rights including the right to privacy. It is out of step with international rulings raising the related issue of how the Australian Government would enforce this law on transnational technology companies.

My submission concentrates upon the following points:

1. Lack of Independent Judicial Oversight

The weak oversight and accountability structures described are not fit for a Bill which proposes such sweeping and covert powers.

The Assistance and Access Bill allows agencies and the Attorney-General to issue notices without judicial oversight. This mechanism has been integral to other legislation in the interests of national security, and is even more relevant to this legislation. In particular, review needs to be undertaken by a judge who by his or her independence from government, provides the greatest authority and legitimacy.

[12] https://www.homeaffairs.gov.au/about/consultations/assistance-and-access-bill-2018

The Explanatory document lists ten limitations and safeguards.[13] The number does not disguise the reality that these 'safeguards' are illusory rather than substantive. Also, they are partial in their application, only applying to Technical Assistance Notices and Technical Capability Notices.[14] This is inadequate when the weight of the Bill is upon creating incentives for providers to be pressed into providing voluntary assistance under the Technical Assistance Requests but wherein the constraints imposed elsewhere do not apply.

The limitations and safeguards revolve around the 'decision maker'. The 'decision makers' can be the Attorney General, the head of the interception agency or delegate.[15] It is asserted that "The people who occupy these positions are trusted to exercise suitable judgment about the propriety of requests and well equipped to consider the reasonableness and proportionality of any requirements." While heart-warming that such a state of trust exists in Australia, greater confidence would be generated in domestic and international quarters if the legislation established an independent mechanism that verifies proper conduct and use of these far-reaching powers by such decision makers.

The Assistance and Access Bill's Explanatory Document states that the decision maker reviews the individual circumstances of each notice. It is, in fact, largely irrelevant whether the decision maker reviews each and every matter when the decision maker leads or is a part of the entity proposing the intervention. The role of head of an agency does not confer automatically adequate 'oversight', and less so when the decision making power can be delegated, even if restricted to within the Senior Executive Service ranks.[16] Objective scrutiny independent from organisational pressures and culture is critical.

While I do not completely endorse the United Kingdom's Investigatory Powers Act 2016 which introduced mandatory decryption obligations as it has significant deficiencies, it did establish a reinforced judicial oversight regime, including an Investigatory Powers Commissioner. It is unclear to me what the justification is for Australia proposing a bill which, if enacted, will not have judicial oversight of the crucial function as part of the new regime.

A recent judgement of the European Court of Human Rights has stressed the importance of independent oversight:

"Review and supervision of secret surveillance measures might come into play at three stages: when the surveillance was first ordered, while it was being carried out, or after it had been terminated. As regards the first two stages, the very nature and logic of secret surveillance dictated that not only the surveillance itself but the accompanying

---

[13] Reasonable, proportionate, practical and technically feasible; Access dependent upon underlying warrant; Prohibition against systematic weakness; Revocation of Notices; Providers can fix existing systems; No extension of interception of data retention, definition of assistance requirements; Consultation with industry on new capabilities, and protection of information. Australian Department of Home Affairs, Assistance and Access Bill 2018 Explanatory Document August 2018, p9.

[14] Australian Department of Home Affairs, Assistance and Access Bill 2018 Explanatory Document August 2018, p9.

[15] Australian Department of Home Affairs, Assistance and Access Bill 2018 Explanatory Document August 2018, p11.

[16] Australian Department of Home Affairs, Assistance and Access Bill 2018 Explanatory Document August 2018, p9.

review should be effected without the individual's knowledge. Consequently, since the individual would necessarily be prevented from seeking an effective remedy of his or her own accord or from taking a direct part in any review proceedings, it was essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding his or her rights. In a field where abuse was potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it was in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure."[17]

The supposed safeguard 'Unauthorised disclosure of information about, or obtained under, a notice or request is an offence' is more reminiscent of government secrecy established to prevent scrutiny and accountability for actions in the name of protecting the national interest, amongst other things. In other parts of the world it is acknowledged that Government secrecy can destroy the legitimacy of government institutions and actions. It can hide abuses of fundamental rights of citizens, and "In fact, secret government tends to excess."[18]

The 'inherent Court review' process referred to in the Explanatory Document accompanying the Bill appears to be focussed on ensuring the processes undertaken are done so according to the law. While very important, this is not to be confused with ruling, for example, whether the public interest is being served by the actions contained in the Notices.[19]

Maximising accountability wherever possible through reasonable transparency is not evident in other parts of the Bill. For example, public reporting is only of numbers of Technical Assistance Notices and Technical Capability Notices given in that year. Technical Assistance Requests are excluded for some unexplained reason and information of frequency of compliance and penalties, of data breaches that may have arisen as a result of compliance with requests and notices, or even of the occasions of use of mechanisms such as Court review and arbitration, are not included. Such quantitative measures do not jeopardise law enforcement or intelligence operations.

The accountability and rigour induced by the described public reporting of performance is minimal.

---

17 European Court of Human Rights, Case of Big Brother Watch and Others v. the United Kingdom, Legal Summary, 13 September 2018.*(Applications nos. 58170/13, 62322/14 and 24960/15)* at https://hudoc.echr.coe.int/eng#{"itemid":["002-12080"]}

18 Manget, F.F., *Intelligence and the Rise of Judicial Intervention. Another System of Oversight*, June 27, 2008, US Center for Intelligence Studies, Central Intelligence Agency. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/96unclass/manget.htm

19 Australian Department of Home Affairs, Assistance and Access Bill 2018 Explanatory Document August 2018, "Inherent review by the courts. Australian courts will retain their inherent powers of judicial review of a decision of an agency head or the Attorney-General to issue a notice.

2. Definitional Problems

The Bill contains provisions which are vague, overly broad or not defined.

A key concept that is undefined is 'national security'. This notion is used on 11 occasions within the Bill. Importantly, it occurs in provisions specifying the parameters to be considered when issuing requests, or technical assistance notices and/or technical capability notices, in addition to specifying the (non-exhaustive) list of acts or things that can fall to communication providers when providing 'assistance'. As 'national security' is a reason given for the introduction of this Bill and a key parameter within it, the scope and meaning needs articulation if there is to be any guide as to when the Bill's powers are to activated. This Bill is inadequate with a definition of this key concept.

The same concerns apply around the vagueness of the scope and potentially broad capture of terms such as:

- "the interests of Australia's foreign relations or the interests of Australia's national economic well-being." This could be interpreted in all manner of ways and is unrestricted in terms of consideration of the severity of the risk to these interests or of the likelihood of their occurrence;

- "protecting the public revenue" is couched in a manner that could enable extension beyond national security or serious criminal matters;

- "designated communications provider" and "in so far as their services or products have a nexus to Australia". This could include telecommunication companies, internet service providers, email providers, social media platforms as well as a host of other services. An example of the width of capture is at s317C(a)(4) in which the person who provides an electronic service that has one or more end-users in Australia, is regarded as a 'designated communications provider'.

- The Bill also covers those who develop, supply or update software, and manufacture, supply, install or maintain data processing devices. The submission from Digital Rights Watch coalition, amongst others, raises pertinent observations on this point;

- The term 'systemic weakness' is not defined yet is one of the more contentious points due to its technical impact and ambiguity. It is a key concern to the industry.

The above points are not an exhaustive list but serve to illustrate why there is such significant confusion which is leading inevitably, to distrust of the Australian Government's intentions.

3. Technical Issues

The Australian Assistance and Access Bill allows the Director-General of Security or the chief officer of an interception agency to compel a provider to do an unlimited range of *acts or things*. That could mean anything from removing security measures to deleting messages or collecting extra data. It could require corporations to provide details about technical characteristics of their systems that could help agencies exploit weaknesses that have not been patched. It also includes installing software, and designing and building new systems. It can require service providers to hand source code over to the authorities. This latter proposal, that is, that agencies could ask for a company's source code to help them identify and exploit vulnerabilities in technology that the company is not aware of, raises serious issues concerning security, intellectual property and commercial interests, amongst others. While not completely or largely endorsing the United Kingdom's *Investigatory Powers Act,* I point out that even this most extensive piece of recent legislation does not require service providers to provide source code to the authorities.

The Assistance and Access Bill's provisions allow Technical Capability Notices to require a provider to develop "a large bespoke capability that would ordinarily be the subject of a significant procurement".[20] It seems providers are being positioned to develop new ways for law enforcement to collect information. While raising questions of whether this is an appropriate role for private enterprises, it is in effect, enabling Australian interception agencies to 'outsource' their hacking powers to providers offering services on the Internet.

Further, the Bill puts few limits or constraints on the assistance that telecommunication providers may be ordered to offer while making it an offence to disclose information about government agency activities without authorisation. These include but are not limited to, for example, removing one or more forms of electronic protection, and/or providing access to a customer's equipment [S317E(1)(e)(ii)]. These penalties are significant when there is no oversight of the public interest in serving the notices.[21]

Announcements in 2017 by the then Australian Prime Minister and in 2018 by the then responsible Minister, the Hon. Angus Taylor MP, stressed that there would be no 'backdoors', no weakening of encryption. Yet, the contents of encrypted messages are to be made accessible to interception agencies.[22]

The foundations for claims that no back doors have been created, can be gleaned from the Explanatory Document in combination with clauses within the Bill. The

---

[20] Australian Department of Home Affairs, Assistance and Access Bill 2018 Explanatory Document August 2018, p49.

[21] Anyone revealing information about data collection by the government can be imprisoned for five years. Penalties exist for con-compliance including for individuals for whom possible imprisonment of up to ten years may apply.

[22] Duckett, C. and Mclean, A. *The laws of Australia will trump the laws of mathematics: Turnbull*, ZDNet, 14 July 2017. https://www.zdnet.com/article/the-laws-of-australia-will-trump-the-laws-of-mathematics-turnbull/; Australian government committed to 'no backdoors': Taylor, ZDNet, 8 June 2018. https://www.zdnet.com/article/australian-government-committed-to-no-backdoors-taylor/

Explanatory Document explains "systemic refers to actions that impact a broader range of devices and service utilised by third-parties with no connection to an investigation and for whom law enforcement have no underlying lawful authority by which to access their personal data.". The Bill itself states that the prohibition against requiring a provider to introduce a systemic weakness includes "one or more actions that would render *systemic* methods of authentication or encryption less effective" (emphasis added).

From these points, it appears that public assertions that backdoors have not been created, rest upon the prohibition on agencies requiring providers to introduce or perform actions that weaken methods of encryption or authentication *across a range of devices,* although they can require a weakening for a particular device/s. The 'systemic weakness' provision, primarily located in 'Limitations' (Division 7 of the Bill), appears to be the legislative drafting of 'no backdoors'.[23]

As devices are rarely produced bespoke, and are increasingly interconnected,[24] it is extremely questionable whether containment to 'particular device/s' is possible. The technical and cyber security communities are becoming progressively concerned about the heightened risks of malware spreading laterally throughout IT environments – a risk that is growing with the convergence of cyber and electronics.[25] I note the 'Listed Acts or Things" at s317E(1) that can be required of designated communication providers are not limited to actions that relate only to isolated devices.

Stating that a provider cannot be required to introduce systemic weaknesses does not mean that the effect of the other actions or things the provider(s) can be compelled to do, will not introduce a weakness that extends beyond a particular device to others not the object of the surveillance activity. Nor does it mean that an action by an agency will not introduce, unintentionally, a 'systemic weakness'. As agencies can take devices and delete or add software it appears to be a significant gap that the Limitations do not prohibit entities from introducing a systemic weakness through their own actions.

It has been debated whether it is possible to access the content of encrypted messages other than at endpoints without weakening encryption; the general conclusion is that it is not. But if it should be, that is, by exceptional access whether through software updates, installing a new operating system, or employing some other solution meant to be employed on a case-by-case basis, the real challenge is ensuring that the system implementing the exceptional access method is secure.[26] And this security is not guaranteed.

In practical terms for providers, it is not clear whether a provider will be able to offer true end-to-end encryption to users and still be able to comply with the notices.

---

23 Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, Division 7 – Limitations, p52

24 *Telstra Security Report 2018,* March 2018, https://insight.telstra.com.au/secure-your-business/articles/inside-the-telstra-security-report-2018

25 *Telstra Security Report 2018,* March 2018, as above.

26 New America, *Coalition Raises Serious Concerns About Australian Draft Bill and Encryption Backdoors,* Press Release, 9 September 2018, p4.

Clarification is required also around the providers' ability to address introduced 'systemic weaknesses'.

Lastly, the constraints against introducing such systemic vulnerabilities set out in this 'Limitations' Division, are applied only to Technical Assistance Notices and Technical Capability Notices and not to Technical Assistance Requests.

While all Requests and Notices can be varied, Technical Capability Notices alone have a consultation period – for receipt and for variation of the Notice. Both timeframes are 28 days. There is no flexibility provided to allow for matters where 28 days may be insufficient to ensure complex technical issues are examined and advice tested prior to implementation to ensure the avoidance of adverse, unintended outcomes.

The Bill allows Requests and Notices to be given orally with a copy of the written record to be provided to the provider 'as soon as practicable'. The looseness of this timeframe is not appropriate to the seriousness of the interventions that can be requested or the potential impacts including those risks for providers, particularly when agencies are required for their own purposes to have such a Record prepared within 48 hours. A tight maximum time period needs to be established to protect both companies and individuals.

Lastly, agencies' use of vulnerabilities within devices has already been shown to present significant risks to agencies. In the United States, leaking of an agency's cyberweapons is reported to have damaged morale, slowed intelligence operations and resulted in hacking attacks on businesses and civilians worldwide.[27]

4. Law Enforcement for Foreign Countries

Notices can be issued not just to enforce domestic laws but to assist the enforcement of the criminal laws of foreign countries. The threshold for such assistance is set as criminal matters involving an offence against the law of a foreign country with a maximum penalty of imprisonment for three years or more, imprisonment for life or the death penalty.[28] These requests are decided by the Attorney General. There is no mention of equivalence with the Australian criminal framework, for instance, would Australia co-operate if the jurisdiction in question was seeking information about the sexuality of someone where being homosexual was punishable by a sufficient term of imprisonment? Or countries where there are restrictions on free speech or other examples that would be clear breaches of human rights?

Despite the Explanatory Document's reference to Australia's international obligations, such as those under Council of Europe Convention on Cybercrime, this provision raises questions. There are concerns about this mechanism becoming a potential 'workaround' mechanism for foreign countries where there is greater rigour in

[27] Shane, S., Perlroth, N. and Sanger, D.E. *Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core,* New York Times, Nov. 12, 2017 https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html

[28] Assistance and Access Bill, Part IIIBB 'Assistance in relation to Information held in computers', Explanatory Notes, p61.

the means to obtain information held on computers. In the absence of a prohibition on, or independent oversight to approve such requests, it will be important to establish conclusively that Australia is not becoming the 'launderer' of international requests for data particularly as Australia has no enforceable human rights protections at the federal level, nor is there a regional mechanism that could be brought into the equation.

The Australian Government might care to note the recent decision of the European Court of Human Rights on the sharing of intelligence and its statements on the purpose of combatting crime to be for "serious crime".[29]

Requiring companies to assist interception agencies to access communications for the purposes of assisting foreign countries, may place companies in the position of being requested to act in a way that may be illegal in other countries from where the foreign citizen originates, and where the companies operate.

5. Industry Consultation

My ongoing contact with communications providers, enabled by multiple interactions in multiple fora, has established that they want to assist law enforcement to effectively investigate serious crimes and prevent terrorism in the digital era. Many of these companies operate across multiple countries and have a significant investment in these complex issues as well as significant expertise. Their presence and stake in this issue, if not their bottom lines, are as significant as some countries.

Encryption is a core component of their operations and the services they offer to business and individual users. The companies advocate encryption as a way to protect data and thwart any TLS/SSL attacks.[30] Government moves to weaken encryption have major implications for their businesses including their role as 'corporate citizens'. Many companies have ongoing discussions with Governments about these issues and have made their stance on government activities such as surveillance and accessing citizens' data, public. A coalition of large companies (Google, DropBox, Twitter, Microsoft, EVERNOTE, Oath:, LinkedIn, SnapInc., and Facebook) have endorsed principles relevant to Government actions in surveillance and accessing data and which are compatible with good public policy making.[31]

At a consultation I held in early September with a number of the large tech companies, the Assistance and Access Bill was discussed. There was unease whether a

---

[29] European Court of Human Rights, Case of Big Brother Watch and Others v. the United Kingdom, Legal Summary, 13 September 2018. *(Applications nos. 58170/13, 62322/14 and 24960/15)* at https://hudoc.echr.coe.int/eng#{"itemid":["002-12080"]}

[30] *Telstra Security Report 2018,* March 2018, https://insight.telstra.com.au/secure-your-business/articles/inside-the-telstra-security-report-2018

[31] RGS Principles: Limiting Governments' Authority to Collect Users' Information; Oversight and Accountability; Transparency About Government Demands; Respecting the Free Flow of Information; Avoiding Conflicts Among Governments, and Ensuring Security and Privacy Through Strong Encryption at http://www.reformgovernmentsurveillance.com/principles/. The Reform Government Surveillance coalition aim is for the world's governments to address and reform the laws and practices regulating government surveillance of individuals and access to their information.

provider will be able to meet the needs of business and ordinary users for protection of their data when there is doubt as to whether they will be able to offer true end-to-end encryption while complying with Australian Requests and Notices.

Amongst other concerns, the approach of the Australian Government was not seen to align with the principles endorsed by the coalition of large companies and referred to above. Specifically, the principles 'breached' by the proposed Australian Assistance and Access Bill concerned the principles of Oversight and accountability; Transparency about Government demands, and Ensuring security and privacy through strong encryption.

The Assistance and Access Bill was seen to also fail the Five Eyes Governments' principles contained in their recently released 'Statement of Principles on Access to Evidence and Encryption', that is:[32]

1. 'Mutual responsibility' – the feedback received was there is little in the Bill that is perceived to be mutual. The provisions and powers are weighted heavily in favour of Australian agencies as companies are fined heavily or jailed if they do not comply, and companies can neither reveal nor appeal Requests or Notices received;

2. 'Due process' – the processes in the Bill do not provide for independent oversight either before Requests or Notices are applied, or during, or after implementation, and assuming the Bill is enacted, there is no statutory review requirement to see if the Bill is meeting its aims or to assess its impacts; and

3. 'Freedom of choice' – the supposed freedom of choice is actually coercive. There is no true appeal mechanism, but there are onerous penalties for non-compliance ($10 million fines) or for revealing use of the Notices even if the disclosure was in the public interest for example, in relation to mis-uses of powers.

The civil liability indemnity provision for any company that suffers a data breach as a result of co-operating, does not negate the heavy handedness of the provisions.

Industry and communication providers are confused by the broad and vaguely scoped terms of the legislation. Such concerns are heightened by the uncertainty around the introduction of security vulnerabilities into their products. There are technical concerns around the assumption that it is possible to contain a vulnerability to one device or devices associated with one person. The strong feeling is that ultimately it would affect all users of that product and result in weaker security for everyone.

---

[32] That is, mutual responsibility; Rule of law and due process are paramount, and freedom of choice for lawful access solutions. https://www.homeaffairs.gov.au/about/national-security/five-country-ministerial-2018/access-evidence-encryption

These concerns are heightened by other provisions contained in the Bill. For example, the proposed provisions that mean companies could be 'flying blind' if, as proposed, an employee or contracted service provider is asked to provide assistance that requires, hypothetically, the handing over of machines or devices, or modification of software, and the company is not advised. Potentially, the company could be unaware the device had left their premises and was returned, modified in some way for example, having security measures removed, or with data deleted or software added to collect extra data. Or whether the employee unbeknownst to the company but in response to a Notice issued, has developed a new way for law enforcement to collect information and implemented it on company products or services.

Yet the company would be accountable to its shareholders and compliance bodies for its governance conduct and the performance of its devices. This is alarming as installing and using software may create, albeit unintentionally, a systemic weakness or vulnerability or cause the device to malfunction. This risk is even more pronounced if multiple interception agencies direct a variety of software be introduced into the same device. Providers will also be required to conceal any action taken covertly by the interception agencies.

Installing or deleting software may also cause a corporation providing internet platforms to be in breach of their data retention or interception obligations in other countries. The lack of mandated consultation preceding Technical Assistance Requests or Technical Assistance Notices does not provide confidence that such matters can be raised and resolution sought. Given the size of the individual users and companies customer base of large companies such as Facebook, Google, Microsoft and others, the risks were seen to have the potential of seriously undermining public trust in these corporations, their products and their services.

The lack of provision for a corporation to be able to appeal from an order issued by the Australian Government under this proposed legislation has also been raised to me as being a matter of significant concern.

These concerns are not restricted to Australia. A coalition of 31 international civil society organizations, companies, and trade associations have written to the Australian Government to raise concerns that, if enacted, a draft surveillance bill would threaten digital security and privacy by undermining encryption.[33] They stressed that "strong encryption is the cornerstone of the modern information economy's security", pointing out a former working group of the United States' National Security Council strongly warned against technical "proofs of concept," including one for "provider enabled remote access to encrypted devices through current update procedures".[34]

---

[33] New America, *Coalition Raises Serious Concerns About Australian Draft Bill and Encryption Backdoors,* Press Release, 9 September 2018. https://www.newamerica.org/oti/press-releases/coalition-raises-serious-concerns-about-australian-draft-bill-and-encryption-backdoors/

[34] Coalition comments in response to the Exposure Draft of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (the Assistance and Access Bill), 9 September 2018, p3. https://newamericadotorg.s3.amazonaws.com/documents/Coalition_comments_on_Australia_bill.pdf

6. The Case for the Bill

In support of the Bill, the Department of Home Affairs has stated that:

- Encryption impacts at least nine out of every ten of ASIO's priority cases.
- Over 90 per cent of data being lawfully intercepted by the AFP now use some form of encryption.
- Effectively all communications among terrorists and organised crime groups are expected to be encrypted by 2020.[35]

But these statistics do not comprise either evidence or argument. While encryption may affect 90% of ASIO's priority cases, it needs to be asked whether the necessary information or evidence was obtained through other means, and whether the information actually was material to the matter at hand? The Department of Home Affairs and ASIO can already access encrypted data with specialist decryption techniques or at start or end points where data are not encrypted.

Future predictions of prevalence of use is insufficient unaccompanied by an analysis of the "encryption impacts", for example, by showing the number by priority of cases that have not been able to be satisfactorily or fully progressed because of encryption. Similarly, it is necessary to methodically consider what other factors may play a part in adverse outcomes and how these may be addressed other than through legislative provisions equivalent to using 'a sledgehammer to crack a walnut'.

Research involving law enforcement, security and intelligence personnel in the United States indicates that the inability to effectively *identify* which service providers have access to relevant data and difficulties in *obtaining* sought-after data were the biggest problems that law enforcement currently face in leveraging digital evidence. These challenges ranked significantly higher than any other challenges, including challenges associated with accessing data from devices or interpreting the data that has been obtained.[36] The basic conclusion from this study was that "Law enforcement access to encrypted data is an issue, but the magnitude of the challenge is not yet significant enough to justify decryption mandates."[37]

Further, the Australian National Security College, which is supportive of legislated powers that determine thresholds for when particularly sophisticated decryption and access tools may be applied against domestic intelligence targets, says "backdoors reduce the security and integrity of our information collectively and over the long term,

---

35 Australian Department of Home Affairs, Consultation: The Assistance and Access Bill 2018, viewed 10 September 2018 at https://www.homeaffairs.gov.au/about/consultations/assistance-and-access-bill-2018

36 Carter, W.A, Daskal, J. C. *Low-Hanging Fruit - Evidence-Based Solutions to the Digital Evidence Challenge,* Center for Strategic and International Studies, 2018. https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180725_Carter_DigitalEvidence.pdf?tAGR_DvxRdp0RspiGYNGcGKTUjrGY3rN

37 Lewis,J.A., Zheng, D.E. and Carter, W.A. *The Effect of Encryption on Lawful Access to Communications and Data,* Center for Strategic and International Studies, 2017. https://csis-prod.s3.amazonaws.com/s3fs-public/publication/170221_Lewis_EncryptionsEffect_Web.pdf?HQT76OwM4itFrLEIok6kZajkd5a.r.rE

as it is not possible to ensure they are used only by those agencies. The security of our society relies upon the security of our information. We do not become more secure by increasing its vulnerability."[38]

As Australian Police already have existing broad powers, such as their ability to covertly hack devices at the endpoints when information is not encrypted, the absence of a well-argued case as to why more powers are needed, severely undermines the case for the Bill.

7. Alternate Means

While there are challenges posed by technology to law enforcement and intelligence services, and countering online child sexual abuse and negating terrorism threats is important, protecting the human rights of citizens is also legitimate and necessary in a democratic society.

The same technologies that empower criminals and terrorists to evade detection or launch malicious attacks can also provide enormous benefits with respect to security, privacy, and the economy.[39] Unfortunately the debate about how to successfully meet these challenges has become polarised. Any response to the complications caused for law enforcement investigations and intelligence collection by encryption, needs a holistic approach that avoids weakening encryption.

There are other avenues the Government can pursue. These involve collaboration between law enforcement and the tech sector on alternative sources of information to assist organised crime and terrorism investigations. The Lowy Institute considers that one useful framework is the Global Internet Forum to Counter Terrorism which was established as a partnership between Facebook, Microsoft, YouTube, and Twitter. It fosters cooperation among tech companies, civil society groups and academics, governments and supranational bodies such as the EU and the United Nations. Through artificial intelligence and human moderation, the partnership has developed content detection and classification techniques to identify and remove extremist content and terrorist clusters from its platforms. It is suggested that similar cooperation could be extended to the platforms' encrypted products.[40]

A convincing case for these extra new powers needs to be made given the draconian nature of the powers, the secrecy provisions and the penalty regime. It needs to be established if the issues identified in the US research play a role in Australia, and if they are, addressing them and ascertaining if they have been effective in mitigating the extent of the problem before seeking to enact the Assistance and Access Bill.

---

38 Mosey, M. and Henschke, A. *Defining thresholds in law – sophisticated decryption and law enforcement* Policy Options Paper No 8, National Security College, Australian National University, April 2018.

39 Lewis, J.A., Zheng, D.E. and Carter, W.A. *The Effect of Encryption on Lawful Access to Communications and Data,* Center for Strategic and International Studies, 2017. https://csis-prod.s3.amazonaws.com/s3fs-public/publication/170221_Lewis_EncryptionsEffect_Web.pdf?HQT76OwM4itFrLEIok6kZajkd5a.r.rE

40 van Graver, D., *Exceptional access: Australia's encryption laws,* The Lowy Institute, 26 June 2018, Sydney https://www.lowyinstitute.org/the-interpreter/exceptional-access-australia-encryption-laws

The effect upon ordinary Australians as consumers also needs to be considered. While it appears that costs incurred by providers in meeting the changes required by agencies, can be negotiated, the question arises just who is really paying for the development of new capabilities. Ultimately these costs can be expected to be passed to services users and product purchasers, and/or taxpayers. Similarly, in terms of individuals, such as sole traders and the like, receiving Requests and Notices, they are unlikely to be able to defend themselves through legal means. The imbalance between an individual without avenues of consultation or appeal and the ability of interception agencies to compel the performance of certain actions under secrecy, requires far better standards of oversight and accountability. The Government cannot expect the public to trust agencies when these counterbalancing mechanisms are absent.

The Assistance and Access Bill can be seen as an evolution from preceding legislation and, potentially, a harbinger of what is to follow. My concerns are compounded by the Australian Government's failure to provide remedy for serious invasions of privacy. Further, currently Australia has limited human rights and privacy protections – it has no constitutional protection for privacy; it has no Bill of Rights that enshrines privacy, there is no tort of privacy, and unlike its neighbour, New Zealand, it has failed European adequacy assessments.

The Assistance and Access Bill is unlikely to be workable in some respects and is an unnecessary infringement of basic liberties in others. The broad drafting provides a high level of discretion on the use of these exceptional powers not to the Parliament but to agencies and the Attorney General. Its aims do not justify a lack of judicial oversight, or independent monitoring, or the extremely troubling lack of transparency.

For all of the reasons set out above, this Bill needs to be put aside. It is fatally flawed. A new approach to addressing the challenges posed by encryption for law enforcement and national security is required. The legislative framework established in Australia is important not just for Australia but internationally and will illustrate for international scrutiny, Australia's capacity for leadership in the protection of the fundamental and inalienable right of privacy.

I would be happy to be of any assistance in this process and I am at your disposal for any other consultation or information.

Finally, I would like to inform you that this communication, as a comment on pending or recently adopted legislation, regulations or policies, will be made available to the public and posted on the website page for the mandate of the Special Rapporteur on the right to privacy: https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx

Please accept, Excellency, the assurances of my highest consideration.

Joseph Cannataci
Special Rapporteur on the right to privacy

Annex:

Correspondence of Mr. David Kaye, Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, dated 11 September 2018.