*Brendan Walker-Munro**

A SHOT IN THE DARK: AUSTRALIA'S PROPOSED ENCRYPTION LAWS AND THE 'DISRUPTION CALCULUS'

Abstract

In December 2018, in response to several foiled terrorist attacks, Australia passed some of the most intrusive telecommunications interception legislation in Australian legal history. Yet the response of the Australian Government is not a cohesive strategy designed to deal with the disruption caused by the emergence and abundance of encrypted messaging. This article deals with the legislative amendments encapsulated in the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) ('the Bill'), and addresses the issues of scope and scale which remain unresolved in spite of these changes. It then reflects upon a new concept — the 'disruption calculus' — to illustrate that the new amendments are unlikely to achieve the regulatory aims sought by intelligence and police forces in Australia. Finally, the article uses Israel's model of encryption regulation to illustrate that a more varied and holistic approach in line with the disruption calculus can provide an effective alternative for regulatory authorities in Australia

I Introduction

On the subject of individuals evading detection by law enforcement, much has been written about the promises of end-to-end encryption programs.[1] A number of freely available applications, such as Signal, WhatsApp, Wickr and Telegram, have grown in prominence in response (at least partly) to market

* JD (Southern Queensland), PhD Candidate (Swinburne); Investigations Manager, ATO.

1 Harold Abelson et al, 'Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications' (2015) 1(1) *Journal of Cybersecurity* 69; Reema Shah, 'Law Enforcement and Data Privacy: A Forward-Looking Approach' (2015) 125(2) *Yale Law Journal* 543; David E Sanger and Nicole Perlroth, 'Encrypted Messaging Apps Face New Scrutiny Over Possible Role in Paris Attacks', *The New York Times* (online, 16 November 2015) <https://www.nytimes.com/2015/11/17/world/europe/encrypted-messaging-apps-face-new-scrutiny-over-possible-role-in-paris-attacks.html>; Kristin Finklea, Congressional Research Service, *Encryption and Evolving Technology: Implications for US Law Enforcement Investigations* (Report, 18 February 2016) <https://fas.org/sgp/crs/misc/R44187.pdf>.

demand for greater communications security.[2] The benefits of encrypted messaging are the creation of a space where free-minded citizens might purchase or sell goods or engage freely in political or emotive discourse without the overarching threat of surveillance from the state.[3] But it also offers a dark side: a hidden marketplace where both buyer and seller are protected from identification, reprisal or arrest.[4] The criminal law response to encryption is difficult and involves a balancing act, as 'the power of ciphers protects citizens when they read, bank and shop online — and the power of ciphers protects foreign spies, terrorists and criminals when they pry, plot and steal'.[5]

This article intends to deal with the amendments encapsulated in the Bill. It identifies and codifies the issues, individual and systemic, which remain unanswered even on the passing of the legislation by the Australian Parliament. It then reflects upon a new concept — the 'disruption calculus' — to demonstrate that the proposed laws are likely to miss their target because of the nature of the disruption they are seeking to address, and the narrow method of regulatory intervention the government has chosen to implement. Like the Australian Government's approach to interception of metadata, the encryption laws are not future-proof.[6] The article closes with a comparison of Australia's approach to regulating encryption with that of Israel, a country not only considered a world leader in market and social methodologies of regulation, but also a 'living lab' for counterterrorism policy where 'entrepreneurism flourishes amidst perpetual internal and external national security threats and the extensive associated surveillance needs'.[7]

II Contextual Information

Communication platforms which employ end-to-end encryption permit users to exchange short messages in a similar fashion to text or SMS messages, without

---

2 Ksenia Ermoshina, Francesca Musiani and Harry Halpin, 'End-To-End Encrypted Messaging Protocols: An Overview' in Franco Bagnoli et al (eds), *Internet Science: Third International Conference, INSCI 2016, Florence, Italy, September 12–14, 2016, Proceedings* (Springer International Publishing, 2016) 244.

3 Daniel Moore and Thomas Rid, 'Cryptopolitik and the Darknet' (2016) 58(1) *Global Politics and Strategy* 7.

4 Judith Aldridge and David Décary-Hétu, 'Not an "Ebay for Drugs": The Cryptomarket "Silk Road" as a Paradigm Shifting Criminal Innovation' [2014] *Social Science Research Network* 1 <http://dx.doi.org/10.2139/ssrn.2436643>.

5 Moore and Rid (n 3) 9.

6 Rick Sarre, 'Revisiting Metadata Retention in Light of the Government's Push for New Powers', *The Conversation* (online, 8 June 2018) <https://theconversation.com/revisiting-metadata-retention-in-light-of-the-governments-push-for-new-powers-97931>.

7 Matthew Waxman and Doron Hindin, 'How Does Israel Regulate Encryption', *Lawfare* (Blog Post, 30 November 2015) <https://www.lawfareblog.com/how-does-israel-regulate-encryption>.

incurring the costs associated with an SMS exchange. Yet the development of such applications has been far more disruptive to law enforcement; in many cases, not even the company is able to decrypt its own messages. In response to a subpoena received in late 2014 as part of a drug trafficking investigation, WhatsApp allegedly replied: 'WhatsApp cannot provide information we do not have'.[8]

Australia also has some of its own experience on this front. Phantom Secure, a Canada-based developer of smartphone software, marketed its products in 2015 and 2016 as specifically designed to protect against interception by both government and corporate agents. Studies of the devices quickly determined that the encryption methodologies were of significant attraction to organised crime groups.[9] The Australian Federal Police ('AFP') were subsequently involved in a major international investigation which saw Phantom Secure's CEO Vincent Ramos indicted on racketeering and conspiracy charges, immediately before the United States' Federal Bureau of Investigation ('FBI'), AFP and Royal Canadian Mounted Police officers seized thousands of phones during raids across the three countries.[10]

Much of the Australian jurisprudential experience has come by way of dealing with terrorism offences.[11] In *R v Besim*, an 18-year-old was convicted of planning a terrorist act.[12] The accused had allegedly planned to crash into a police officer with a car and then behead him — plans which he shared via Telegram with a 14-year-old known by the pseudonym 'S'. These discussions were only discovered when police in the United Kingdom arrested S on unrelated matters and identified the information on his phone. In one of the judgments in *R v Khaja*, the use of an encrypted messaging service to communicate the accused's plans was held to be a circumstance increasing the seriousness of the offence.[13] Lastly in *R v MHK*, the Commonwealth Director of Public Prosecutions appealed a sentence of seven years imposed on an offender who, at the age of 17, pleaded guilty to planning a terrorist act. The Court of Appeal increased the sentence from seven to 11 years, noting that the offender used

8 Matt Apuzzo, 'WhatsApp Encryption Said to Stymie Wiretap Order', *The New York Times* (online, 12 March 2016) <https://www.nytimes.com/2016/03/13/us/politics/whatsapp-encryption-said-to-stymie-wiretap-order.html>. See Shah (n 1).

9 Matteo Vergani and Sean Collins, 'Radical Criminals in the Grey Area: A Comparative Study of Mexican Religious Drug Cartels and Australian Outlaw Motorcycle Gangs' (2015) 38(6) *Studies in Conflict & Terrorism* 414; Rick Sarre, 'Metadata Retention as a Means of Combatting Terrorism and Organised Crime: A Perspective from Australia' (2017) 12(3) *Asian Journal of Criminology* 167. See also *Re McNally* [2018] VSC 522.

10 Lucy McNally and John Stewart, 'Australian Federal Police Seize Phantom Secure Phones as Part of Global Crackdown', *ABC News* (online, 16 March 2018) <https://www.abc.net.au/news/2018-03-16/afp-seize-phones-as-part-of-phantom-secure-crackdown/9555652>.

11 See, eg, *R v Elomar* (2010) 264 ALR 759; *Benbrika v The Queen* (2010) 29 VR 593; *R v Khalid* [2017] NSWSC 1365.

12 *R v Besim* [2016] VSC 537.

13 *R v Khaja [No 5]* [2018] NSWSC 238.

encrypted messaging software as one of 'a variety of deceptions' designed to keep his preparations secret from close members of his family.[14]

In Australia, end-to-end encryption transcripts have only been used as evidence in the last five years,[15] but it is important to note that, in all these cases, transcripts were provided either by a party to the conversations or from police who had forensically extracted the data from a mobile phone. No Australian case has yet dealt with the possibility of intercepted end-to-end data or forensically decrypted messages.[16]

III The Australian Encryption Laws

The concept of everyday access to encrypted methodologies being used to hide widespread criminality and illegality (otherwise known as 'going dark') is considered one of the greatest threats facing law enforcement and national security agencies in the 21st century.[17]

Telecommunications interception and access has been a feature of Australia's legal landscape since at least the 1970s, when the *Telecommunications (Interception and Access) Act 1979* (Cth) ('*Telecommunications Act 1979*') first came into being. The *Telecommunications Act 1979* permits certain agencies various degrees of access to telecommunications data, with increasing levels of scrutiny over such access. Generally speaking, three levels of access are permitted:

a) Access to existing information or documents: this includes details about what inbound and outbound telephone calls or SMSes a particular service makes during a given period, but more recently has also included access to metadata. These require an authorisation under pt 4-1 of the *Telecommunications Act 1979*, signed by an 'authorised officer', with a limited list of law enforcement agencies also permitted access.[18]

---

14 *DPP (Cth) v MHK (a Pseudonym)* (2017) 52 VR 272, 291 [63].

15 *R v Al-Kutobi* [2016] NSWSC 1760; *DPP (Cth) v Satharupan* [2016] VCC 1783. See also the Fair Work Commission's treatment on appeal in *Wong v Taitung Australia Pty Ltd* (2017) 268 IR 145.

16 The closest so far appears to be *DPP v Tran* [2016] VCC 77, which appears to involve a mixture of surveillance, telecommunications interception warrants and forensic analysis.

17 James A Lewis, Denise E Zheng and William A Carter, Center for Strategic and International Studies, *The Effect of Encryption on Lawful Access to Communications and Data* (Report, February 2017) 12–17; Hoaithi YT Nguyen, *Lawful Hacking: Towards a Middle-Ground Solution to the Going Dark Problem* (MA Thesis, Naval Postgraduate School, 2017).

18 Including delegates of a law enforcement agency as defined by the *Telecommunications (Interception and Access) Act 1979* (Cth) s 5AB(1).

b) Access to stored communications: this might include stored emails, SMSes or actual content of communications passing over or through a particular communications service during a given period. Stored communications require the issue of a stored communications warrant under pt 3-3 of the *Telecommunications Act 1979,* which can only be issued by an issuing authority.[19]

c) Access to install and monitor interception technology: generally these cover various telephone, internet and email interception technologies (also known as 'wiretaps'), where the communication between two parties is listened to or observed by a law enforcement agency. Again, a warrant must be issued under Pts 2-2 and 2-5 of the *Telecommunications Act 1979*, and again are limited to police, select law enforcement agencies and the Australian Security Intelligence Organisation ('ASIO').

All of these various authorisations and warrants are monitored by the Commonwealth Ombudsman as an oversight mechanism, with additional layers of protection for journalists. Division 4C of pt 4-1 requires the ASIO or a 'law enforcement agency' to apply to the Attorney-General for a warrant if they seek records related to a person the agency reasonably believes is a journalist. A 'Public Interest Advocate' is also involved in this process to make submissions to the Attorney-General about the scope of the proposed journalist information warrant.[20]

The Australian Government has thus moved relatively swiftly to address the disconnect between its law enforcement agencies and encryption technology. In July 2017, it signalled its intention to address the issue with the passing of legislation that would target the corporate sector to cooperate with law enforcement, by coercion if necessary.[21] In August 2018, Australia met with the other Five Eyes nations[22] where a joint position was reached on the importance of the primacy of the rule of law and due process protections, as a balance between a citizen's right to privacy and the legitimate public interest in enforcement of the criminal law.[23] On 20 September 2018, proposed amendments were introduced into the House of Representatives. These amendments contained a number of changes to Australian surveillance law:

---

19 Usually a judicial or tribunal officer: ibid s 6DB.

20 Ibid s 180X.

21 Malcom Turnbull, 'Press Conference with Attorney-General and Acting Commissioner of the AFP — Sydney — 14 July 2017' (Press Conference, 14 July 2017) <https://www.malcolmturnbull.com.au/media/press-conference-with-attorney-general-and-acting-commissioner-of-the-afp-s>.

22 The Five Eyes Alliance is an intelligence-sharing alliance established under the UKUSA Agreement between Canada, New Zealand, the United Kingdom, the United States of America and Australia. The alliance is designed to facilitate the timely and free sharing of intelligence and national security information.

23 Attorney-General's Department, 'Statement of Principles on Access to Evidence and Encryption' (Media Release, 30 August 2018) <https://www.attorneygeneral.gov.au/Media/Documents/joint-statement-principles-access-evidence.pdf>.

a) Schedule 1 amends the *Telecommunications Act 1997* (Cth) to insert a new 'Part 15 — Industry assistance', which contains certain requirements for industry to assist law enforcement and national security agencies to decrypt communications.

b) Schedule 2 amends the *Australian Security Intelligence Organisation Act 1979* (Cth) ('*ASIO Act*') to expand powers already present with respect to computer access warrants and authorisations executed by ASIO under the *Surveillance Devices Act 2004* ('*SD Act'*).

c) Schedule 3 amends the *Crimes Act 1914* (Cth) to expand police powers under search warrant provisions to compel the production of passwords and assistance to access a device which may hold evidentiary material, subject to an assistance order, and to access data remotely during the valid period of the warrant.

d) Schedule 4 broadens the search warrants powers under the *Customs Act 1901* (Cth) to permit the Australian Border Force to seek assistance orders similar to those in the *Crimes Act 1914* (Cth).

e) Schedule 5 amends the *ASIO Act* to introduce provisions for the ability of ASIO officers to require certain assistance in relation to its execution of a warrant authorised under existing provisions.

It is important to note that the amendments offer the new pt 15 powers only to defined 'interception agencies', being the Police Forces of the states and territories, the AFP and Australian Crime Commission, ASIO, the Australian Secret Intelligence Service, and the Australian Signals Directorate.[24] This is hardly surprising, given that these are also the agencies that already have a specific ability to apply for existing telecommunications interception and data access warrants under the *Telecommunications Act 1997* (Cth).

Pt 15 introduces a tiered approach to assistance requirements, with non-compliance forming the basis for civil liability and penalties of up to $10 million:

a) A 'technical assistance request' ('TAR') under div 2, which is a voluntary request to provide assistance that might facilitate the agency undertaking its investigative work, such as removing electronic protection, providing technical information, installing software, putting information in a given format and facilitating access to devices or services.[25]

---

24 *Telecommunications Act 1997* (Cth) s 317B. State and Territory interception forces must notify and seek the approval of the AFP Commissioner before issuing any Notice under pt 15: at s 317LA.

25 Ibid s 317E. Electronic protection includes both authentication and encryption measures: at s 317B.

b) A 'technical assistance notice' ('TAN') under div 3, which compels a service provider to assist the agency in a way that is both practicable and technically feasible.[26]

c) A 'technical capability notice' ('TCN') under div 4 issued by the Attorney-General (with the approval of the Home Affairs Minister), which requires that a service provider build an inherent capability into their systems or infrastructure that would enable ASIO or an interception agency to undertake their functions.

Yet Australia's proposal is still considered unique amongst the Five Eyes nations, as it goes a step further than the existing 'industry assistance' provisions in the United Kingdom and New Zealand law. The New Zealand legislation imposes general duties on network operators to provide 'access points' and 'delivery ports' (as well as housings and staff to support interception equipment) to enable interception agencies to lawfully intercept communications passing over the networks those operators provide.[27]

The United Kingdom legislation permits a wide variety of interception warrants to be issued for equipment interference (covering conduct that would be analogous to 'wiretaps' or pt 2-2 or pt 2-5 warrants) but places the oversight of interception warrants and notices under the aegis of the Investigatory Powers Commissioner, Judicial Commissioners and/or the Secretary of State. TCNs under the *Investigatory Powers Act 2016* (UK) require consultation by the Secretary of State with the person who will be affected by its issue about, inter alia, the technical feasibility and cost of complying with the TCN.[28]

Australia's language around TCNs is considered a world first, even amongst other Five Eyes nations. Whilst New Zealand law imposes duties on telecommunications providers, it does so in general terms about developing the capability to intercept (as opposed to decrypt) communications which pass over their networks. Even the United Kingdom (which already includes TCNs in their legal framework) these provisions stop short of requiring that a given technology provider actively provide a potential 'back door' into their systems that would assist interception agencies — which is what the Australian TCN contemplates. The following is a brief comparison of some of the relevant provisions in Australian and UK law:

26 Ibid s 317P.

27 Without specifically proscribing a decryption capability: *Telecommunications (Interception Capability and Security) Act 2013* (NZ) ss 9–11.

28 *Investigatory Powers Act 2016* (UK) ss 15, 61, 99, 136, 158, 176, 252–7.

Table 1: Brief comparison of Australian and United Kingdom legislation on TCNs

***Telecommunications Act 1997* (Cth)**	***Investigatory Powers Act 2016* (UK)**
A TCN is a notice that requires the provider to perform one or more specified acts 'directed towards ensuring that the designated communications provider is capable of giving listed help to ASIO, or an interception agency, in relation to the performance of a function, or the exercise of a power, conferred by or under a law of the Commonwealth, a State or a Territory, *so far as the function or power relates to a relevant objective'* (s 317T(2)(a)(i)).	A TCN is a notice imposing on the relevant operator any applicable obligations relating to 'the removal by a relevant operator of *electronic protection applied by or on behalf of that operator* to any communications or data … obligations relating to the security of any postal or telecommunications services provided by a relevant operator' (s 253(5)).

The draft Bill introduced into the House of Representatives on 20 September 2018 was referred to the Parliamentary Joint Committee on Intelligence and Security ('PJCIS') for inquiry, with a report published in early December 2018. The Bill passed both Houses on 6 December 2018. The Bill was also reviewed by the Parliamentary Standing Committee for the Scrutiny of Bills.[29] Whilst a full analysis of the Standing Committee's findings is beyond the scope of this article, that Committee raised additional concerns regarding the potential unconstitutional nature of excluding ADJR review of notices,[30] the blurring of the separation of powers doctrine,[31] as well as incompatibility with the Attorney-General's own policy guidance.[32]

IV Response to the Bill's Proposals

The exposure draft of the legislation was released on 14 August 2018. Over 340 submissions were received by the Department of Home Affairs during this initial exposure draft, which the Department claimed 'was productive and led to significant amendments to the Bill to address key concerns raised and reinforce the policy intent of the Bill'.[33] The Bill was referred to the PJCIS on 20 September 2018, who

29 Parliamentary Standing Committee for the Scrutiny of Bills, Parliament of Australia, *Scrutiny Digest* (Digest No 14 of 2018, 28 November 2018) 23–82 ('*Scrutiny Digest'*).

30 Under the provisions of the *Administrative Decisions (Judicial Review) Act 1977* (Cth) ('ADJR').

31 Where officers of the administrative branch of government could offer civil immunity to designated communication providers to comply with pt 15 notices.

32 Attorney-General's Department, *A Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers* (Guide, September 2011) 50–2; cf *Telecommunications Act 1997* (Cth) s 317ZF(1).

33 Department of Home Affairs, Submission No 18 to PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (2018) 42.

held public hearings from 19 October to 30 November 2018, and also invited further submissions. In total (including confidential and withheld submissions) 105 submissions were received:

Table 2: Broad classes of persons making submissions to the PJCIS

Party	Number of Submissions
Telecommunication providers	8
Members of Parliament	3
Non-Governmental Organisations	26
Police or Crime Commissions	5
Members of the public	39
Name Withheld	11
Confidential	6
United Nations Special Rapporteur	1
Government agencies (Office of the Australian Information Commissioner, Commonwealth Ombudsman, Inspector-General of Intelligence and Security)	6

The responses to the proposals were unsurprisingly partisan. The submission of the Department of Home Affairs reflected on the 'extensive two-stage consultation' engaged in by the drafters of the legislation as well as between the responsible Ministers.[34] The Independent Commission Against Corruption (NSW), Law Enforcement Conduct Commission, Queensland Police Service, and Police Federation of Australia all supported the Bill without amendment (Victoria Police who, while supporting the Bill, lamented that they would not have access to the Bill's powers for their own investigations).[35] The Minister himself also provided a submission seeking 'accelerated' consideration of the legislation.[36] The Commonwealth Ombudsman was cautiously neutral, accepting that their oversight role under the proposed

34 Ibid 42.

35 Police Federation of Australia, Submission No 36 to PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (12 October 2018); Law Enforcement Conduct Commission, Submission No 57 to PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (2018); Independent Commission Against Corruption, Submission No 75 to PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (17 October 2018); Queensland Police, Submission No 97 to PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (2018); Victoria Police, Submission No 98 to PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (30 November 2018).

36 Peter Dutton, Submission No 89 to PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (22 November 2018).

framework was likely to lead to an expansion of the Ombudsman's role and would require additional resourcing.[37]

Unfortunately, there was far more opposition (at least in numbers of submissions) from representatives of Australia's information technology, computer security and telecommunication providers. Key criticisms were the lack of consultation, lack of specific definitions, extraterritorial nature of the Bill and erosion of trust likely to occur between telecommunications providers and their consumers.[38] Other specific examples of opposition included:

a) Optus strongly suggested a mandated consultation step to identify costs and capability concerns as well as permitting options for voluntary compliance (other than by TAR) to minimise the costs of introducing new capabilities.[39]

b) Telstra went a step further, suggesting TANs should not 'require development or implementation of a technical capability the relevant [provider] does not have'.[40]

a) Mozilla described their concerns around the increased international tensions inherent in the sale of 'compromised software' in jurisdictions other than Australia.[41]

b) Cisco specifically cited their disclosure obligations and security policy to the public on 'bugs' and how this interacted with TANs and TCNs.[42]

---

37 Commonwealth Ombudsman, Submission No 64 to PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (15 October 2018).

38 Australian Computer Society, Submission No 1 to PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill* 2018 (25 September 2018) 2; Kaspersky Lab, Submission No 13 to PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (2018); Coalition of Civil Society Organisations & Technology Companies and Trade Associations, Submission No 29 to PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (21 November 2018).

39 Optus, Submission No 41 to PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (October 2018) 2–3.

40 Telstra, Submission No 44 to PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (12 October 2018) 5 [2.2].

41 Mozilla, Submission No 46 to PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (12 October 2018) 3–4.

42 Cisco, Submission No 42 to PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (12 October 2018) 5–7, 9.

c) Senetas suggested Australia's international reputation in cyber security R&D would be damaged (with flow-on effects on exports). In addition, poor testing of vulnerabilities could result in unforeseen consequences such as mass outages.[43]

Dr Riana Pfefferkorn, Cryptography Fellow for the Stanford Center for Internet and Society, was far less restrained in her view of the legislation:

> Simply put, the Bill would create a freight train without any brakes … It will do nothing to prevent the Australian Government from undermining the security — and privacy, economic interests, even personal safety — not only of millions of Australians, but of covered entities' other users around the world.
>
> I urge the Committee not to let this dangerous and misguided Bill proceed.[44]

There were even voices of caution amongst Members of Parliament and other government agencies, who expressed their concerns that the Bill impermissibly infringed the human rights of all Australians.[45] Even the Inspector-General of Intelligence and Security expressed her reservations about having a proposed oversight role and the technical challenges of modern encryption.[46]

Perhaps the most compelling submission came from Joseph Cannataci, the United Nations Special Rapporteur on the Right to Privacy in the Digital Age. The mandate of Cannataci's appointment includes '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'.[47] His submission to the PJCIS was a direct letter to both the Minister for Foreign Affairs and Minister for Home Affairs:

> [The 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

---

43 Senetas, Submission No 85 to PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (2018) 1.

44 Riana Pfefferkorn, Submission No 35 to PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (11 October 2018) 3.

45 Australian Human Rights Commission, Submission No 47 to PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (12 October 2018); Office of the Australian Information Commissioner, Submission No 65 to PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (15 October 2018).

46 Inspector-General of Intelligence and Security, Submission No 52 to PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (12 October 2018).

47 Human Rights Council, *The Right to Privacy in the Digital Age*, 28th sess, Agenda Item 3, UN Doc A/HRC/RES/28/16 (1 April 2015) 3.

> 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.[48]

A theme emerges from Cannataci's submission that despite the threat of encrypted messaging to law enforcement, it 'is not yet significant enough to justify decryption mandates'.[49] He also cited the lack of judicial oversight of pt 15 notices,[50] definitional issues, and the lack of consultation with industry as fatal points in the legislation. Given that Australia lacks superior legal protections for privacy such as a Bill of Rights or constitutional right to privacy, he also expressed concerns that Australia's proposal was out of lockstep even with other Five Eyes nations, and would inevitably follow the experiences of the United Kingdom and European governments in this area.[51]

Yet despite the many submissions and committee reports relating to the proposed amendments, the PJCIS made only modest recommendations. The Bill was amended to clarify certain definitions and inserted provisions for a service provider to be consulted and obtain advice about compliance with a TCN.[52] Provisions relating to TANs and TARs were also amended to ensure they could not be used to circumvent existing processes for which a warrant was already required.[53] Despite Labor members of the PJCIS having considered the Bill, a number of concerns remained.[54] The Bill received Royal Assent on 8 December 2018 and is now part of Australian law.[55] A further inquiry by the PJCIS is now underway and a separate statutory review by the Independent National Security Legislation Monitor is due within 12 months of the legislation coming into effect. Yet there remain some substantial problems with the proposed regulatory framework the Commonwealth has imposed.

---

48 Joseph Cannataci, Submission No 81 to PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (12 October 2018) 4.

49 Lewis, Zheng and Carter (n 17).

50 Cf *Investigatory Powers Act 2016* (UK) ss 252–8.

51 Such as the findings of the European Court of Human Rights: *Big Brother Watch v the United Kingdom* (European Court of Human Rights, Grand Chamber, Applications Nos 58170/13, 62322/14 and 24960/15, 13 September 2018) ('*Big Brother Watch*').

52 PJCIS, Parliament of Australia, *Advisory Report on the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (Report, December 2018) 5–7 ('PJCIS report').

53 *Telecommunications Act 1997* (Cth) s 317ZH.

54 Such as in the definitions for systemic vulnerability and weakness, target technology, imposition of relevant objectives for the issue of pt 15 notices as well as a process for State and Territory interception agencies to apply to the AFP Commissioner for such notices.

55 For this reason, from hereon any references to the *Telecommunications Act 1997* (Cth) are references to that Act, as amended.

V Problems of Scope and Scale

One of the most valid criticisms raised by the opponents to the Bill was its inconsistency with Australia's international law obligations. The provisions in the *Investigatory Powers Act 2016* (UK), on which the Bill was modelled, were struck down by the European Court of Human Rights[56] for violating arts 8 and 10 of the *European Convention on Human Rights*,[57] as were similar data retention provisions in EU member states.[58] Although Australia is not bound by the European Convention, the Convention shares several similarities with the *Universal Declaration of Human Rights*[59] and Australia's Human Rights Framework.[60] It is strongly arguable that the Bill could likewise offend provisions around 'security of person' (art 3), right to legal review (art 10) and arbitrary interferences with privacy (art 12). This hypothesis is buttressed by the findings of the Parliamentary Joint Committee on Human Rights who made similar comments in their report.[61] In effect, they found that the Bill imposed significant restrictions on Australia's human rights obligations because most of the considerations for pt 15 are conducted in camera and ex parte, and are not subject to applications for judicial review.

Moving to matters of domestic law, the Bill was vague on specifying the offences to which it would apply. The initial draft of the Bill sought to permit the intrusion of the interception and national security agencies for *any* matter falling under their purview. Following the hearing of evidence at both public hearings and written submission stages, the PJCIS recommended that the criminal law enforcement provisions of the *Telecommunications Act 1997* amendments be restricted to the investigation of offences with a maximum penalty of at least three years imprisonment.[62] A similar distinction was suggested by the Parliamentary Standing Committee for the Scrutiny of Bills.[63] Whilst this might seem like an appropriate distinction to remove the majority of simple or summary offences, the time period looks arbitrary when considering that investigation of the following offences would be sufficient

56 *Big Brother Watch* (n 51).

57 *Convention for the Protection of Human Rights and Fundamental Freedoms*, opened for signature 4 November 1950, 213 UNTS 222 (entered into force 3 September 1953), as amended by *Protocol No 14 to the Convention for the Protection of Human Rights and Fundamental Freedoms, Amending the Control System of the Convention*, opened for signature 13 May 2004, CETS No 194 (entered into force 1 June 2010) ('European Convention').

58 Thomas Wahl and Cornelia Riehle, 'Focus: Anti-Money Laundering' [2016] (4) *European Criminal Law Associations Forum* 153, 164.

59 *Universal Declaration of Human Rights*, GA Res 217 A (10 December 1948).

60 Attorney-General's Department, *Australia's Human Rights Framework* (Framework, April 2010).

61 Parliamentary Joint Committee on Human Rights, *Human Rights Scrutiny Report: Report 11 of 2018* (Report, 16 October 2018) 24–71; *Telecommunications Act 1997* (Cth) sch 1 pt 1.

62 PJCIS report (n 52) 3 [2.3].

63 *Scrutiny Digest* (n 29) 36–8.

ground for the issuing of a request or notice to vitiate encryption privacy under the proposed pt 15:

a) Possessing, making, exhibiting or selling infringements of copyright;[64]

b) Fishing in a Commonwealth marine area;[65] and

c) Mail tampering, dishonestly dealing in personal financial information, and (ironically) possessing an interception device.[66]

Both TANs (issued by the head of an interception agency) and TCNs (issued by the Attorney-General) must also require assistance from a service provider that is 'reasonable and proportionate' as well as in terms that are 'practicable and technically feasible'.[67] Whilst Recommendation 11 in the PJCIS report[68] may have resulted in the inclusion of new sections to define (respectively) what is 'reasonable and proportionate' for the issue of TARs, TANs and TCNs, the legislation remains near-silent on the definition of 'practicable and technically feasible'.[69] There is some manoeuvrability for TCNs, as a TCN cannot be issued until a consultation notice has been issued and a provider has provided the Attorney-General with a submission on the grounds of that TCN. This submission may include expert assessment and reports on whether a systemic weakness or systemic vulnerability has been or could be introduced by two assessors.[70] TANs have no such provision. Deployment of any assistance or capability under a TAN or TCN which creates a systemic weakness or systemic vulnerability under s 317ZG also obviates liability for the provider.

But in the absence of a s 317W report for consultation with the Attorney-General, which entity determines what is 'practicable' and 'technically feasible'? Is it the service provider, the requesting agency, the courts, or the standards of society at large? Whilst there is some scope for a senior officer of the interception agency[71] to provide 'advice' on the scope of the service provider's obligations, there is no real extrinsic or independent assessment on the balance of the notice. To demonstrate the difficulty of answering these questions, let us consider a hypothetical scenario: ASIO wants to conduct a targeted installation of malware on several iPhones operated by

64 *Copyright Act 1968* (Cth) ss 132AD–132AM.

65 *Environment Protection and Biodiversity Conservation Act 1999* (Cth) s 390SB.

66 *Criminal Code* (Cth) ss 471.7, 480.4 and 474.4 respectively.

67 *Telecommunications Act 1997* (Cth) ss 317P, 317V.

68 PJCIS report (n 52) 6.

69 *Telecommunications Act 1997* (Cth) ss 317PA, 317RA, 317ZAA; these terms do provide some flexibility in their application, as what is practicable and technically feasible will always depend upon the circumstances.

70 One of whom must be a former judge: ibid ss 317W, 317WA.

71 Either the Director-General of Security or the chief officer of an interception agency, as appropriate: ibid ss 317MAA(1)–(2).

a suspected terrorist, whose details are known to the agency. ASIO might consider that the installation is both practicable and technically feasible, but Apple might disagree for reasons ASIO have nott considered. Assisting law enforcement in this way might expose Apple to a heightened risk of terrorist attack themselves, lower their share price, cause them to lose opportunities with foreign investors or other nations' governments, or suffer reduced sales from consumers who do not want their privacy compromised. These considerations may not sway ASIO in issuing a TAN, but would certainly be part of Apple's consideration around compliance. Apple could risk incurring the civil penalty of Australia rather than breaching the European *General Data Protection Regulation*.[72]

Likewise, there are issues with the definition of systemic weaknesses and vulnerabilities. At what point is a weakness or vulnerability considered 'systemic'? The Bill failed to include the recommendations of the Director-General of the Australian Signals Directorate, who considered a 'systemic' weakness or vulnerability to be 'a weakness that 'might actually jeopardise the information of other people as a result of that action being taken'.[73] The Communications Alliance submission makes the problems with ambiguity in the Bill abundantly clear:

> It is unclear at what point a requested weakness would become systemic, ie would a weakness be systemic when a certain system is involved or does the concept of systemic revolve around the number of users (potential or actual?) affected by the weakness and, if so, what would a relevant user number threshold be? It is also not clear how vendors of telecommunications network equipment could be required to do a SAT [specified act or thing] without introducing a systemic weakness or vulnerability given that their products are at the core of most digital communications. Similarly, it is not clear what a weakness or vulnerability would be in the eyes of the requesting agency.[74]

The overlap of the provisions and lack of clarity around important terms also raises a number of serious questions about the scope and scale of TANs and TCNs. The lack of requirement for ministerial involvement for the issue of a TAN seems like an appropriate scaling of compulsory power reposing in an investigative agency. However, the fact that a TAN is not subject to consultation and also lacks clarity around what constitutes 'practicable and technically feasible' assistance opens the door to potential for misuse or abuse, either by the interception agency or third parties. Consider our earlier scenario with an interception agency installing malware on several iPhones.

---

72 In which case it stands to be fined up to 4% of its annual turnover: Apple, Submission No 53 to the PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (2018) 5–7.

73 PJCIS report (n 52) xi.

74 Communications Alliance, Australian Information Industry Association and Australian Mobile Telecommunications, Submission to the Department of Home Affairs, *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* [Exposure Draft] (7 September 2018) 12–13 ('Communications Alliance report').

Assuming the investigation relates to a sufficiently serious criminal offence, this approach does not involve the introduction of a 'systemic' weakness and also does not require a specific 'capability' to be built into a service provider's system, so could be grounds for the issue of a TAN. In fact, this specific example is cited in the Explanatory Memorandum:

> The mere fact that a capability to selectively assist agencies with access to a target device exists will not necessarily mean that a systemic weakness has been built. The nature and scope of any weakness and vulnerability will turn on the circumstances in question and the degree to which malicious actors are able to exploit the changes required.[75]

There is the possibility that malware could be targeted by another interception agency without the need for a TAN (as they are exploiting a vulnerability already present in the software). There is no oversight of this activity, and in fact the sharing of information relating to TARs, TANs and TCNs is permitted between interception agencies,[76] meaning the AFP could learn of ASIO's installation of the malware and seek to exploit it themselves without being subject to the scrutiny of their Agency Head, the Inspector-General of Intelligence and Security or the Commonwealth Ombudsman.[77] The malware could also be exploited by another investigative agency not even covered by the protections and requirements of the Bill. In the most extreme case, ASIO, the body that has statutory responsibility for Australia's domestic security, could have facilitated access to that phone by a hacker, working alone or for the government of another nation.

VI Australian Regulators and Telecommunications Interception

The history of telecommunications interception in Australia is littered with such examples of law enforcement use gone wrong. At the end of each financial year the Attorney-General's Department publishes a report detailing the occasions when law enforcement agencies accessed telecommunications data under the *Telecommunications Act 1997*. Previous revisions of the *Telecommunications Act 1997* permitted access to any state, territory or federal agency with a role connected to the enforcement of the criminal law, or a law administering a pecuniary penalty — which rather elastically covered everything from murder and drug offences, to on-street parking and unregistered pets. In fact, the Department's 2014–15 Annual Report[78] listed that a host of various agencies had successfully accessed telecommunications data

75 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 67–8.

76 *Telecommunications Act 1997* (Cth) ss 317ZF(6)–(12).

77 Ibid s 317TAB.

78 Attorney-General's Department, *Telecommunications (Interception and Access) Act 1979 Annual Report 2014–15* (Report, 2011).

1,116 times in the enforcement of a criminal law,[79] and 2,197 times in the enforcement of a law administering a pecuniary penalty or protecting public revenue.[80]

These agencies included various local councils, liquor regulators, racing and wagering bodies, and the RSPCA. The highest number of authorisations was from the New South Wales Office of Fair Trading, who with 675 authorisations for 2014–15 exceeded the requests of several of the dedicated anti-corruption commissions including NSW's Independent Commission Against Corruption and Victoria's Independent Broad-Based Anti-Corruption Commission.

One recommendation from the 2012 inquiry was the reduction in agencies able to access telecommunications data by using a 'gravity of conduct' test, where serious crime and threats to security were of higher importance than non-criminal matters.[81] A subsequent inquiry was commenced following the introduction of the proposed Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014. Recommendations 17 to 28 of that Inquiry related to tightening the safeguards around access to telecommunications data, limiting it only to 'enforcement agencies' declared by primary legislation or regulation.[82] When these provisions came into effect on 13 October 2015, it reduced the number of agencies permitted to make telecommunications data requests from 63 to only 20.[83] In a case of circumstances going full circle, the recent PJCIS enquiry into the Bill has heard that s 313 of the *Telecommunications Act 1997* is now being used by a whole variety of agencies including fisheries, workplace health and safety, local councils, and the racing and taxi integrity bodies to circumvent the metadata restrictions imposed in 2014 and obtain information that the 2014 amendments intended to make subject to a warrant.[84]

Another example which resulted in embarrassment throughout the government was the approach to content blocking (also called 'blacklisting'). The approach seems relatively straightforward — block specific IP address ranges from connecting to domestic browsers, or blocking webpages based on specific keywords. But the devil is in the detail. Many Australian regulators rely on s 313(3) of the *Telecommunications Act 1997* to block access to offensive material, by relying on the provision for providers to render law enforcement with 'reasonably necessary' assistance. Subsection 313(3) permits (although with vague and imprecise language) Australian law enforcement to block illicit websites and thereby 'prevent and disrupt activity

79 Ibid 44.

80 Ibid 47.

81 PJCIS, Parliament of Australia, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation* (Report, May 2013) 25–6.

82 PJCIS, Parliament of Australia, *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (Report, February 2015) xvii–xxii.

83 Attorney-General's Department, *Telecommunications (Interception and Access) Act 1979 Annual Report 2015–16* (Report, 2015) vii.

84 Evidence to PJCIS, Parliament of Australia, Canberra, 19 October 2018, 41 (John Stanton).

which may cause serious harm to the Australian community'.[85] But in April 2013, ASIC inadvertently blocked several webpages of the Melbourne Free University when trying to target a serial fraudster.[86] The result (perhaps unsurprisingly) was a Senate inquiry which produced a report scathing in its criticism of the 'inability of the agency to correctly target the offending websites without causing collateral damage, and the time delay in identifying the problem'.[87]

Both definitional and targeting problems abound throughout the Bill. The breadth of 'designated service provider' in the Bill is particularly problematic. Whilst clearly meant to capture large corporate actors such as Facebook, Telstra and Google and make them subject to the issue of pt 15 notices, the definition is equally capable of capturing the assistance rendered by a single individual, such as a line technician or retailer. Whilst the Explanatory Memorandum couches the definition as being in 'technologically neutral language to allow for new types of entities and technologies to fall within its scope as the communications industry evolves', it also permits a degree of legislative creep over the powers available to interception agencies. In their submission to the PJCIS, the Communications Alliance raised concerns that TARs and TANs could be issued 'anywhere in the supply chain'.[88] The Australian Industry Group, Internet Architecture Board and Massachusetts Institute of Technology's Internet Policy Research Initiative collectively expressed grave concerns with the seemingly limitless number of entities that could be compelled to comply with pt 15 notices.[89]

Other hypothetical scenarios demonstrate the potential problems with the legislation. What happens if the introduction of a vulnerability, not in itself a 'systemic weakness' or 'systemic vulnerability', permits some incidental knowledge of a corporation's software to be divulged that could be exploited by a third party? Suppose that we take our previous scenario and assume that several iPhones contain a specific

---

85 Australian Federal Police, Submission No 20 to Standing Committee on Infrastructure and Communications, *Inquiry into the Use of Subsection 313(3) of the Telecommunications Act 1997 by Government Agencies to Disrupt the Operation of Illegal Online Services* (18 March 2015) 1.

86 House of Representatives Standing Committee on Infrastructure and Communications, Parliament of Australia, *Balancing Freedom and Protection: Inquiry into the Use of Subsection 313(3) of the Telecommunications Act 1997 by Government Agencies to Disrupt the Operation of Illegal Online Services* (Report, June 2015) 10–13.

87 Ibid 21 [2.55].

88 Communications Alliance report (n 74) 11 [2.4].

89 Australian Industry Group, Submission No 3 to PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (10 September 2018); Internet Architecture Board, Submission No 23 to PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (10 October 2018); Massachusetts Institute of Technology Internet Policy Research Initiative, Submission No 32 to PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (11 October 2018).

vulnerability implanted under a legitimate and lawful TAN. The vulnerability itself is not systemic, either by reference to the Explanatory Memorandum, the evidence heard by the PJCIS or the terms of the Bill itself. But the imposition of the capability compelled by ASIO or the interception agency might permit a third party to identify a weakness in Apple's security or other software, or use the introduced weakness as leverage to insert their own malware or other program. The amended disclosure provisions make this potential problem worse.[90] Although the Digital Industry Group Inc ('DIGI') requested these changes on the basis of consumer concern around government intrusions into privacy,[91] they might also signal to unethical hackers that a given security flaw is present in the provider's software — all they have to do is find it.

Finally, the laws appear to ignore the transnational nature of the connected economy, where the idea of compelling a multinational such as Google or Facebook to modify its own proprietary software to the detriment of customers in only one of its operating territories is extremely controversial for three reasons. Firstly, such large companies are usually not headquartered in Australia and so may only be bound to comply to the extent that they carry on their operations within the sovereign power or jurisdictional authority of Australia.[92] Should the cost or risk of complying with the jurisdictional requirements become too much, there is a very real risk of such companies restricting or withdrawing their services in Australia. It is worth noting that the Bill also deals with the expansion of ASIO's powers under computer access warrants. In particular, the proposed s 43A of the *SD Act* requires that a computer access warrant only be granted for a computer in a foreign jurisdiction if consent has been obtained from the authority of that country competent to give consent for surveillance devices[93] — there is no such provision for TANs or TCNs.

These companies could also argue that it is not 'practicable' under the *Telecommunications Act 1997* to comply with a TAN or TCN on the grounds that the proposed action would jeopardise customers in other jurisdictions, most notably those covered by the European Union's *General Data Protection Regulation.*[94] As the DIGI put in their submission:

---

90 *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) ss 317ZF(14)–(17).

91 DIGI, Supplementary Submission No 78 to the PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (27 November 2018) 6 ('DIGI submission').

92 *Telecommunications Act 1997* (Cth) ss 9–11.

93 *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) sch 2 s 1.

94 *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)* [2016] OJ L 119/1.

> A Notice may compel businesses with operations or customers outside Australia to take actions in Australia that violate the laws of other countries in which they operate … The Bill does include a defense to noncompliance with a Notice if it requires an action in a foreign country that would contravene the laws of that country, but there is no defense if a Notice requires a recipient to do an act or thing in Australia that might violate the laws of another country in which it operates or has customers.[95]

In addition, compliance with Australian laws may render the multinational liable to sanctions under the laws of other companies in which it operates, something that Apple makes clear:

> Even though this bill grants immunity for compliance with a TAN or TCN, it does not and cannot extend that immunity to cover liability in foreign jurisdictions. For instance, most user content is stored in the United States and US law controls access to that data by law enforcement. Failure on the part of any US entity to follow those requirements gives rise to criminal and civil liability. Most relevant, Title III of the US Omnibus Crime Control and Safe Streets Act would subject Apple to criminal sanctions for any unauthorised interception of content in transit, which this bill could permit. If Australian authorities were to issue a TAN or TCN that required access to data of European Union citizens, Apple could face stiff penalties of up to 4% of its annual turnover under the General Data Protection Regulation, were it to comply.[96]

An introduced weakness or vulnerability might not be considered systemic under s 317B of the Bill, in that it is not a vulnerability or weakness that 'affects a whole class of technology'. However, the definition specifically excises a weakness or vulnerability 'selectively introduced to one or more target technologies that are connected to a particular person'. This 'target technology' may be the particular carriage service, electronic service, software, computer, data processing device or item of equipment directly or indirectly connected to the person. By applying that weakness or vulnerability to that person it nonetheless affects other persons or classes of persons (both domestically and internationally) who use the service, computer or item of sufficient similarity to that individual, such as being on the same network, using the same encryption key, email server, phone or internet service provider — the list is endless. As Greens MP Adam Bandt said:

> [I]magine that there's basically a group of people—people under 18 or people in Victoria—all of a sudden now under this proposal. Does that now not count as a systemic weakness, if you say: 'I'm just introducing a backdoor into your app for a particular group of particular people. It's only them that we're going to spy on'? Who knows? Probably.[97]

---

95 DIGI submission (n 91) 12.

96 Apple (n 72) 7.

97 Commonwealth, *Parliamentary Debates*, House of Representatives, 6 December 2018, 12781 (Adam Bandt).

So much like ASIC's ill-fated blocking of Melbourne Free University, an unknown and potentially limitless class of persons' privacy located anywhere in the world can be threatened by the issue of a single careless TAN or TCN in Australia.

VII Overlaying the Disruption Calculus

I posit that all of these concerns with the legislation arise from a single root cause that a single law-based solution cannot treat. This root cause is one of regulatory disruption — the substantive disconnection of criminal law enforcement from the target of its investigative activities. Encryption, and its employment in peer-to-peer messaging applications such as WhatsApp, disrupt those enforcement agencies by reducing their capability to detect offending facilitated by the use of those programs. They can, of course, continue to legally intercept communications between two parties (subject to compliance with existing restrictions around telecommunications interception) but without the keys to the encryption being used, are powerless to get to the actual content of the communication which might evidence the offence or identify the perpetrators. Encryption also permits entry to illicit markets more readily by criminal entrepreneurs who have access to cheap, effective mechanisms for communication which are not subject to regulatory oversight, and reduces the likelihood that any evidence obtained against a person might, depending on all of the circumstances, be admissible to prove the circumstances of the offence.

The problem arises because the presence of a disruptor (encrypted communications) facilitates criminal entrepreneurship by:

a) lowering barriers to entry to the various unlawful markets (sale of drugs, distribution of radical propaganda, planning or conspiring to commit various offences); and

b) offering new fora for unlawful conduct for incumbent market entrants (for example, being able to plan a fraud in a large company by several employees in a confidential and secure way).

This is not to say that everyday citizens have, with the passage of the Bill into law, taken up opportunities to engage in widespread lawlessness. Instead it reflects the observation that regulators are no longer capable of pursuing their regulatory objectives because of disruption by a new practice, device or system. One could argue that what these amendments seek to do is to restore surveillance capabilities to detect unlawful behaviour. The amendments also look to raise the barriers to entry for offending behaviour by 'forecasting' or 'telegraphing' that encryption methodologies can be compromised at point-of-offer. There is no point using an encrypted service if the service provider can be compelled to hand over your conversations to the police.

I argue that this argument is a hollow one. The proscriptive nature of the definitions of the Act, despite Parliament's best efforts to 'use neutral language', are unlikely to be agile enough to keep pace with the developments of the communications industry.

In addition, law-based command-and-control style regulation is only one possible tool in the armoury of the contemporary regulator.[98] Lastly it ignores the latest research in regulation and governance, which requires that a proper regulatory response

> involves recognition that complexity excludes simple governance solutions and that effective governance often requires a combination of mechanisms oriented to different scales, different temporal horizons, etc., that are appropriate to the object to be governed. In this way strategies and tactics can be combined and rebalanced to reduce the likelihood of governance failure in the face of turbulence in the policy environment and changing policy risks.[99]

So I consider that the proper regulatory response requires a concept borrowed from the field of cybernetics[100] — the law of requisite variety where 'only variety can destroy variety'.[101] Single-use methodologies are doomed to failure, and the deployment of the widest possible set of regulatory responses against a disruptor (such as encryption) is crucial. The tools that can be used fall into four categories by reference to Lessig's work,[102] more recently extended by Murray and Scott.[103] These four regulatory methodologies are:

a) Hierarchy (law, ordinances and the physical instruments of compliance).

b) Community (typified by 'naming and shaming', or the use of other mechanisms of social feedback to limit or mitigate unlawful behaviour).

c) Competition (permitting the economic forces of supply and demand in the market promote and encourage compliant behaviour, whilst punishing deviance with financial disincentive).

d) Design (creating and maintaining architectural solutions to channel and shape regulatees into compliant behaviour, and blocking opportunities for deviance).

---

98 Lawrence Lessig, 'The Law of the Horse: What Cyberlaw Might Teach' (1999) 113(2) *Harvard Law Review* 501, 508.

99 Bob Jessop, 'Metagovernance' in Mark Bevir (ed), *The SAGE Handbook of Governance* (Sage Publications Ltd, 2011) 1, 16.

100 W Ross Ashby, *Introduction to Cybernetics* (Chapman and Hall, 1956); W Ross Ashby, 'Requisite Variety and its Implications for the Control of Complex Systems' in George J Klir (ed), *Facets of Systems Science* (Springer, 1991) 405.

101 Stafford Beer, *Decision and Control: The Meaning of Operational Research and Management Cybernetics* (John Wiley & Sons, 1994) 279.

102 Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books, 1999) 93–4.

103 Andrew Murray and Colin Scott, 'Controlling the New Media: Hybrid Responses to New Forms of Power' (2002) 65(4) *Modern Law Review* 491.

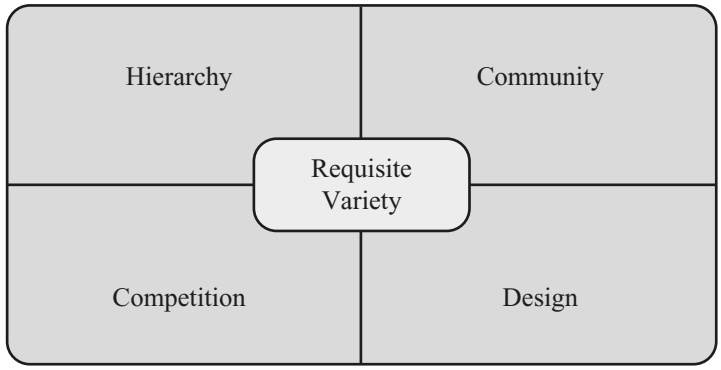

Figure 1: The four regulatory methodologies providing requisite variety

All of these methodologies, brought together in a synergistic whole, give rise to the creation of regulatory solutions with sufficient 'requisite variety' to combat regulatory disruption. There are several theoretical examples that show the amendments to the Act do not embrace this concept. Criminals may, for example, migrate from 'reputable' messaging apps such as WhatsApp and Signal to other service providers specifically located in overseas jurisdictions. There, safe beyond the territorial reach of Australian law, such providers could legitimately ignore pt 15 notices given to them by the interception agencies and continue to market and offer their products to the less salubrious of society. Our law enforcement and national security agencies remain effectively powerless to stop such conduct, as enforcement options are limited in international jurisdictions that may not recognise the offending conduct as illegal under their sovereign laws.[104]

These laws also promote 'cockroaching phenomenon', a term broadly defined as the proliferation of criminal actors in response to increased regulatory scrutiny.[105] Illicit actors who, until now, have communicated using existing commercial off-the-shelf technologies which are happy to cooperate with law enforcement might themselves take the opportunity to branch out into their own telecommunication offerings. There is effectively nothing stopping an enterprising criminal from developing their own 'Phantom Secure' platform to protect themselves from government intervention.[106] The host of such a platform is highly unlikely to give the formal nature of a pt 15 Notice due credit or attention. Whilst this might expose them to a civil penalty, it effectively negates the government's entire encrypted telecommunications policy (not to mention that dismantling such an operation would be incredibly resource-intensive and require potential international cooperation).

104 For examples of the difficulties: see *Humane Society International Inc v Kyodo Senpaku Kaisha Ltd* [2015] FCA 1275.

105 Ian Hosein, Prodromos Tsiavos and Edgar A Whitley, 'Regulating Architecture and Architectures of Regulation: Contributions from Information Systems' (2003) 17(1) *International Review of the Law of Computers & Technology* 85, 90.

106 McNally and Stewart (n 10).

Of course, it is simple to suggest that law is not the only tool to solve complex social problems. This is because we are dealing with the concept of crime, which is not always a non-compliance caused by mistake or negligence. Instead it is 'an object of struggle, power, and social forces'[107] and so we need to have some potential examples of how these methodologies might appear when brought to fruition. In other work I have suggested a number of options by which the savvy regulator might use non-law solutions:[108]

a) Delegating some of their power to the marketplace, by permitting firms to succeed or fail according to compliance with both law and consumer expectation.[109]

b) Implementing hard-coded or physically engineered technological counter-measures in addition to law reform and market incentives, such as those deployed to protect copyright designs.[110]

c) Imposition of social stigma with certain kinds of unwanted conduct. For example, whilst committing an act of bankruptcy is not an offence, it garners a high degree of social stigma that discourages or disincentives certain conduct.[111]

d) Licensing or taxing products or services such as dangerous occupations or substances, rather than outright banning them;[112]

---

107 Steve Tombs, 'Crisis, What Crisis? Regulation and the Academic Orthodoxy' (2015) 54(1) *Howard Journal of Criminal Justice* 57, 69.

108 Brendan Walker-Munro, 'Disruption, Regulatory Theory and China: What Surveillance and Profiling Can Teach the Modern Regulator' (2019) 8(2) *Journal of Governance and Regulation* 23.

109 Daniel Spulber, 'Unlocking Technology: Antitrust and Innovation' (2008) 4(4) *Journal of Competition Law & Economics* 915; Timothy Sandefur, *The Permission Society: How the Ruling Class Turns Our Freedoms into Privileges and What We Can Do About It* (Encounter Books, 2016).

110 Benoît Macq, Patrice Rondao Alface and Mireia Montanola, 'Applicability of Watermarking for Intellectual Property Rights Protection in a 3D Printing Scenario' (Conference Paper, International Conference on 3D Web Technology, 18–21 June 2015).

111 Paul Ali, Lucinda O'Brien and Ian Ramsay, '"Short a Few Quid": Bankruptcy Stigma in Contemporary Australia' (2015) 38(4) *University of New South Wales Law Journal* 1575.

112 Mark T Law and Sukkoo Kim, 'Specialization and Regulation: The Rise of Professionals and the Emergence of Occupational Licensing Regulation' (2005) 65(3) *The Journal of Economic History* 723; Kari Lancaster, Kate Seear and Alison Ritter, 'Making Medicine; Producing Pleasure: A Critical Examination of Medicinal Cannabis Policy and Law in Victoria, Australia' (2017) 49 *International Journal of Drug Policy* 117.

e) Certification as a mark of honour or distinction amongst consumers, who then tend to prefer that product over a competitor.[113] The coffee industry in particular strives for marks or brands of quality as a way of increasing prices or winning customers.[114]

f) Physical or hard coded barriers to non-compliance, such as chicanes to stop trucks carrying drugs from ramming through Customs road blocks at ports of entry.[115]

g) Utilising the surveillance or information gathering capabilities of third party agencies to support knowledge gaps in the regulator's awareness of its target population.[116]

By using an approach that is 'more than law', we therefore develop an approach at Figure 2 which I have dubbed the 'disruption calculus'. It offers a glimpse at ways that a modern regulator might choose to use multiple levers to exert the behavioural change it seeks. In the words of Brownsword, regulators can

> achieve the desired regulatory effect by relying vicariously on non-governmental pressure … or by relying on market mechanisms; in addition, they know that careful consideration needs to be given to selecting the optimal mix of various regulatory instruments.[117]

Applying the conceptual model outlined in Figure 2 suggests that the Australian Government would benefit from considering the combined use of the law with other regulatory methodologies and should 'seek contextual, integrated, joined-up strategies that will work in synergy'.[118] The current approach of lawmaking via amendment does not socially stigmatise the unlawful use of encrypted messaging applications. Nor should it, given the attraction of the everyday Australian to the usage of these programs, but there are arguably ways in which it could do so in a non-exclusive fashion. The amendments do not encourage the market to generate or supply applications which would support law enforcement to pursue their objectives in protecting Australians from terrorism, paedophilia or organised crime. And

---

113 Tim Bartley, 'Certification as a Mode of Social Regulation' in David Levi-Faur (ed), *Handbook on the Politics of Regulation* (Edward Elgar Publishing, 2011) 441.

114 Atika Wijaya and Pieter Glasbergen, 'Toward a New Scenario in Agricultural Sustainability Certification? The Response of the Indonesian National Government to Private Certification' (2016) 25(2) *The Journal of Environment & Development* 219.

115 Malcolm K Sparrow, *The Character of Harms: Operational Challenges in Control* (Cambridge University Press, 2008) ch 2.

116 Nicholas Gane, 'The Governmentalities of Neoliberalism: Panopticism, Post-Panopticism and Beyond' (2012) 60(4) *The Sociological Review* 611.

117 Roger Brownsword, 'Code, Control, and Choice: Why East is East and West is West' (2005) 25(1) *Legal Studies* 1, 1–2.

118 John Braithwaite, 'The Essence of Responsive Regulation' (2011) 44(3) *University of British Columbia Law Review* 475, 490.

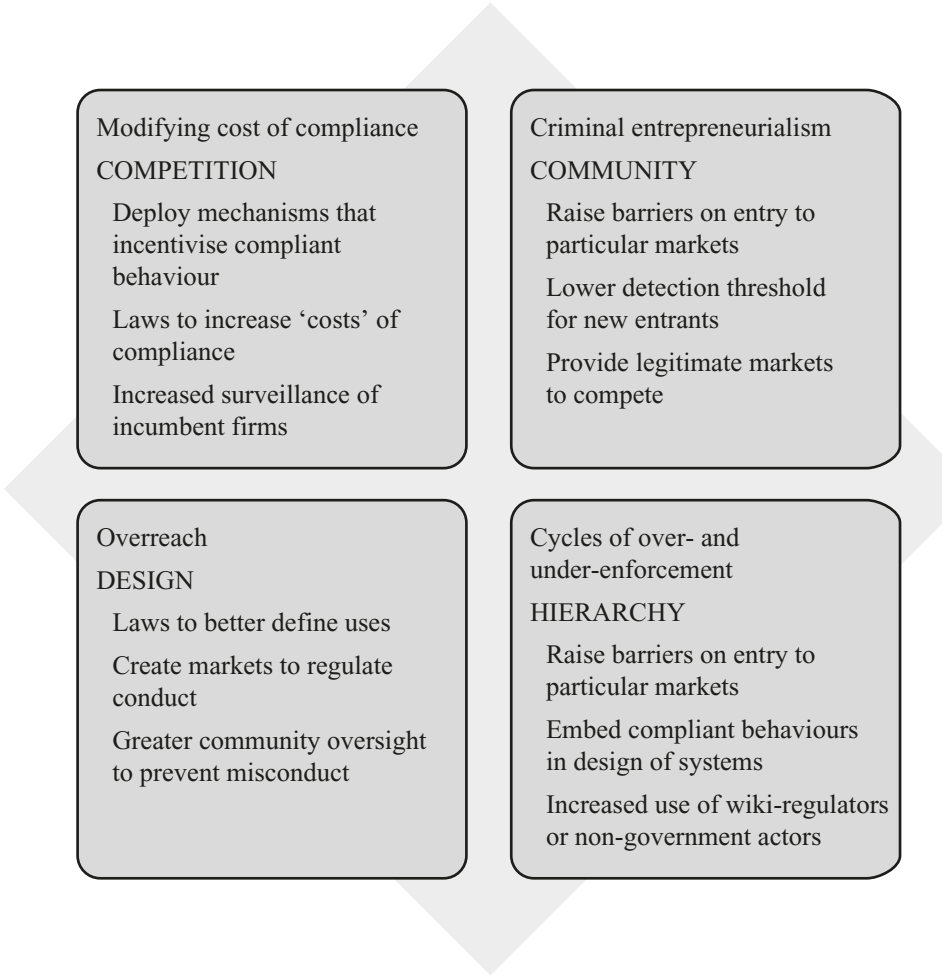

Figure 2: The Disruption Calculus

although the Bill attempts to make some rudimentary modification of the architecture of either short messaging services and its overlaid encryption framework to create a space where non-compliance cannot go, it does so without apparent consideration of the broader impacts of introducing such weaknesses. Instead, the law simply creates an additional set of tools for law enforcement and national security agencies that possibly trade off broader or collective electronic security to potentially identify individual instances of wrongdoing.

VIII Other Approaches to Regulation Promoted by the Disruption Calculus

What might a multi-modal regulatory response proposed by the disruption calculus look like in practice? Surprisingly, few of the submissions to the PJCIS suggested any

alternatives to Australia's proposed regime. Kaspersky Lab did suggest that Australia instead follow the United States' example of *increasing* encryption to better secure the nation, its citizens and interests.[119] AccessNow recommended utilising existing Mutual Legal Assistance Treaties as well as more collaborative approaches between industry and law enforcement (such as technical experts educating investigators on ways to access data already available).[120] Of relevance to this article is Cannataci's pragmatic approach that offers a non-law solution to this problem. He suggested that there were

> 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 … It is suggested that similar cooperation could be extended to the platforms encrypted products.[121]

This collaborative approach speaks of the kinds of regulatory methodologies contained in the 'market' segment of Figure 2. Looking internationally, we can identify that Israel is a significant world player in the export of computer encryption, surveillance and intrusion technologies.[122] With further analysis, we can identify that Israel adopts a multi-modal regulatory methodology around encryption, where Israeli law and government policy focuses instead on licensing entrants to the market as well as extremely close collaboration between government, universities and private sector.[123] Of course, Israel might seem a confusing choice as they are not part of the Five Eyes alliance — but they have a number of useful benefits on the implementation of market and social regulatory methodologies to deal with a disruptor problem like encryption.

What makes Israel's approaches to regulation of encryption so enticing is their use of competition together with law as a regulatory tool in two respects:

a) Promoting, encouraging and fostering cooperation between government and tech companies by incentivising compliant and cooperative conduct (such as with access to a large market and favourable tax treatments) rather than relying on legal compulsion and threat of pecuniary enforcement; and

b) Creating and maintaining a niche market for third party corporations to develop and sell new products that might break or intercept encrypted communications under the imprimatur of existing access regimes.

---

119 For example, Secure Data Act, HR Res 5823, 115th Congress (2018).

120 AccessNow, Submission No 33 to the PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (12 October 2018) 12–13.

121 Cannataci (n 48) 15.

122 Daniel Benoliel, 'Towards a Cybersecurity Policy Model: Israel National Cyber Bureau Case Study' [2015] (16) *North Carolina Journal of Law & Technology* 435.

123 Waxman and Hindin (n 7); ibid 476.

Part of Israel's approach to the regulation of encryption is via law at first instance. This authority derives from its *Control of Commodities and Services Law* 5717–1957, which delegates authority to Ministers to utilise subordinate legislation to control particular goods and services being developed or offered by Israeli companies or companies operating in Israel. The subsequent order issued in 1974 prohibits engagement in encryption activities without a licence, where engagement includes purchase, sale, import/export, development and distribution.[124] Since 1999, actual regulatory responsibility for Israeli encryption regulation has been the ambit of the Encryption Control Department of the Ministry of Defense ('MOD').[125]

It is important to note that whilst these laws might seem draconian and exert a significant degree of control around the regulation of encryption technology, in reality the MOD exercises a light regulatory touch that is more focused on market development and incentivising compliant behaviours, even by major players such as IBM, Huawei, Apple and Microsoft. At the time of writing, no investigation or prosecution has been undertaken since 1998. There is also a category of licence known as a 'free means' which, if granted, exempts the technological development from regulation altogether. The Israeli Ministry of Defence website lists at least 1,000 encryption items that have been granted a free means licence since 12 June 2016.[126]

More broadly, the Israeli MOD also takes steps to incentivise high-tech markets.[127] Israeli tax law is already particularly advantageous to R&D companies seeking to establish themselves, and individual taxpayer incomes derived from R&D receive reduced tax rates.[128] Other advantages, such as grants and export incentives, are also available.[129] More recent studies have shown Israeli law promoting the 'Silicon Valley effect' has been so successful that '[t]he lessons on the role of Israeli government in promoting high-tech clusters via VC [venture capital] financing programs would be useful for other countries to learn from the Israeli experience'.[130] The Israeli MOD also funds challenges (such as the Combating Terrorism Technology Startup

---

124 *Order Governing the Control of Commodities and Services (Engagement in Encryption Items)* 5735–1974.

125 Ministry of Defense, 'Policy of Control and Licensing of Commercial Encryption Items' (Media Release, 24 September 2000) <http://www.mod.gov.il/English/Encryption_Controls/Pages/Encryption_Policy.aspx>.

126 'Free Means', *Ministry of Defense* (Web Page) <https://www.mod.gov.il/English/Encryption_Controls/Pages/FreeMeans.aspx>.

127 Dan Senor and Saul Singer, *Start-Up Nation: The Story of Israel's Economic Miracle* (Twelve Publishing, 2011).

128 *The Law for Encouragement of Research and Development in Industry* (1984) § 1 (Israel).

129 Yitzhak Hadari, 'The Role of Tax Incentives in Attracting Foreign Investments in Selected Developing Countries and the Desirable Policy' (1990) 24(1) *The International Lawyer* 121; Saul Lach, 'Do R&D Subsidies Stimulate or Displace Private R&D? Evidence from Israel' (2002) 50(4) *The Journal of Industrial Economics* 369.

130 Jarunee Wonglimpiyarat, 'Exploring Strategic Venture Capital Financing with Silicon Valley Style' (2016) 102 *Technological Forecasting and Social Change* 80.

Challenge)[131] and 'hackathons', community events designed to share ideas, create innovations and promote social engagement with computer security problems.[132] It is trite to observe that when a need is well-defined, the market responds positively — when the FBI sought a court order to compel Apple to break the encryption on terrorist Syed Farook's iPhone, an unknown third party came forward and assisted the FBI with breaking the encryption without Apple's assistance.[133] As Waxman and Hindin opine:

> Israel has created a system that appears to assert tough controls on a broad range of software and technology providers but, in reality, offers a variety of licensing exemptions, eschews direct enforcement, and adopts an overall approach that seeks to encourage compliance and facilitate private sector and government collaboration.[134]

By using the regulatory methodology of competition, Israel's policy and legal approach to encryption has encouraged major investment from some of the largest tech companies in the world[135] and provides a substantial proportion of the cyber-security and encryption products for sale in the global market.[136] Israel leads the world in its development and implementation of computer security, led in large part by its seamless integration between the private tech sector, the military, law enforcement and Government officials.[137]

The overall effect of Israel's approach to encryption regulation is staggeringly synchronised:

> The country of Israel relies on its centralized law enforcement and cybercrime unit with assistance from private partners like Cellebrite, along with ties to the military and academia ... No concerns or controversies are voiced about exceptional access by the prime minister, members of the Knesset, or other political leaders in the country. The population, a significant number of whom are involved in burgeoning high technology fields, remains silent on the methods used by the Israel Police and the subject of exceptional access at large.

---

131 See generally Israel Defense, 'Fighting Terrorism with Technology' (Web Page, 10 February 2016) <https://www.israeldefense.co.il/en/content/fighting-terrorism-technology>.

132 Judy Gray and Taylor Kiland, *Cyber Technology: Using Computers to Fight Terrorism* (Enslow Publishing, 2016).

133 Office of the Inspector-General, United States Department of Justice, *A Special Inquiry Regarding the Accuracy of FBI Statements Concerning its Capabilities to Exploit an iPhone Seized During the San Bernardino Terror Attack Investigation* (Report, March 2018) 1.

134 Waxman and Hindin (n 7).

135 James Donahue, *A Comparative Analysis of International Encryption Policies En Route to a Domestic Solution* (MA Thesis, Naval Postgraduate School, 2018) 43.

136 Waxman and Hindin (n 7).

137 Benoliel (n 122) 474–6.

> No indication can be seen that technology companies like Apple have any obligations placed on them to assist with exceptional access; nor have companies publicly articulated complaints if such demands were made of them … Scholars have indicated that Israel's streamlined regulatory framework may be a factor in the assistance it receives from the private sector. No evidence has been found to support such a claim, but it is not an unreasonable assumption.[138]

There are several cogent criticisms of Israel's regulatory framework. Without the benefit of litigation, either in challenge to licence decisions or by way of prosecution for non-compliance, there is no judicial consideration of the way Israel's Encryption Control Department assesses encryption items and exercises their administrative powers. There are also no guidelines or other reporting around the balancing of public interest considerations in licensing decisions made by the MOD.[139] Yet these criticisms seem miniscule when compared to the overwhelming benefits of a regulatory scheme encouraging such close collaboration and partnership between researchers, tech companies and the government. Rather than taking the Australian approach of compelling a tech company to violate its brand and erode the trust of its consumers, the Israeli regulatory approach is one of 'encourag[ing] compliance by minimizing reasons not to comply'.[140]

I do not intend to propose that Australia should adopt Israel's method of regulation, though such an analysis might form a fascinating basis for future research. Instead I consider that the Israel example serves as an illustration that using non-law solutions under the disruption calculus can be as effective as using the compulsion of law. If we remember the four methodologies, Israel's approach to encryption embraces the 'market' methodology to support law enforcement rather than relying on 'law' through compulsion and threats of legal action. Israel also promotes third parties via the 'community' methodology to solve the problems of national security by offering a niche market for the development of products that would assist law enforcement. Such an approach ought to engender more trust from the public whilst also fostering a more cooperative information-sharing arrangement between industry and government.

IX Conclusion

The Commonwealth has sought to forge ahead in its attempts to control a known source of regulatory disruption: encrypted communications. Yet in its haste to bring the conduct of certain classes of criminal actors back into compliance by the passing of the Bill, it fails to substantively deal with the reasons why criminal law regulators

138 Donahue (n 135) 55–6 (citations omitted).

139 Barak Jolish, 'The Encryption Debate in Plaintext: National Security and Encryption in the United States and Israel' in Yair Frankel (ed), *Financial Cryptography: 4th International Conference, FC 2000 Anguilla, British West Indies, February 20–24, 2000 Proceedings* (Springer International Publishing, 2001) 202.

140 Waxman and Hindin (n 7).

became disconnected in the first place. In the words of the United Nations Special Rapporteur,

> 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.[141]

By reflecting upon the 'disruption calculus' as well as by benchmarking against the regulatory methodologies of Israel, we have seen that the amendments to Australia's telecommunications laws are very likely to have the same issues as the incumbent legislation because they do not adequately address the source of regulatory disconnection. Whilst the proposed amendments might make some headway against the threshold of detection of unlawful activity, they do not address barriers for entry to criminal markets nor the other elements of behavioural adaptation that may be adopted by criminal agents in the market. The framers have also not followed the 'law of requisite variety', by failing to embrace multiple domains of control across community, competition or design-based regulatory modalities. In effect, the Commonwealth has taken a shot in the dark, hoping to hit a target. Time will tell whether that shot was accurate or not.

141 Cannataci (n 48) 16.