INTERNET POLICY REVIEW
Journal on internet regulation

Volume 9 | Issue 3

Regulatory arbitrage and transnational surveillance: Australia's extraterritorial assistance to access encrypted communications

Monique Mann
Department of Criminology, Deakin University, Geelong , Australia, monique.mann@deakin.edu.au

Angela Daly
Law School, University of Strathclyde, Glasgow, United Kingdom, a.daly@strath.ac.uk

Adam Molnar
Sociology and Legal Studies, University of Waterloo, Canada, adam.molnar@uwaterloo.ca

Published on 16 Sep 2020 | DOI: 10.14763/2020.3.1499

Abstract: This article examines developments regarding encryption law and policy within 'Five Eyes' (FVEY) countries by focussing on the recently enacted Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Cth) in Australia. The legislation is significant both domestically and internationally because of its extraterritorial reach, allowing the development of new ways for Australian law enforcement and security agencies to access encrypted telecommunications via transnational designated communications providers, and allowing for Australian authorities to assist foreign counterparts in both enforcing and potentially circumventing their domestic laws. We argue that Australia is the 'weak link' in the FVEY alliance as - unlike other FVEY members - has no comprehensive enforceable human rights protections. Given this, there is a possibility for regulatory arbitrage in exploiting these new surveillance powers to undermine encryption via Australia.

Keywords: Encryption, Five eyes, Surveillance, Extraterritoriality

Article information

Received: 26 Sep 2019 **Reviewed:** 09 Jan 2020 **Published:** 16 Sep 2020

Funding: As part of Dr Mann's Vice-Chancellor's Research Fellowship, Queensland University of Technology provided funds for Dr Murphy's research assistance, and travel to present this research.
Competing interests: The author has declared that no competing interests exist that have influenced the text.

URL:
http://policyreview.info/articles/analysis/regulatory-arbitrage-and-transnational-surveillance-australias-extraterritorial

Citation: Mann, M. & Daly, A. & Molnar, A. (2020). Regulatory arbitrage and transnational surveillance: Australia's extraterritorial assistance to access encrypted communications. *Internet Policy Review*, *9*(3). DOI: 10.14763/2020.3.1499

This paper is part of Geopolitics, jurisdiction and surveillance, a special issue of Internet Policy Review *guest-edited by Monique Mann and Angela Daly.*

INTRODUCTION

Since the Snowden revelations in 2013 (see e.g., Lyon, 2014; Lyon, 2015) an ongoing policy issue has been the legitimate scope of surveillance, and the extent to which individuals and groups can assert their fundamental rights, including privacy. There has been a renewed focus on policies regarding access to encrypted communications, which are part of a longer history of the 'cryptowars' of the 1990s (see e.g., Koops, 1999). We examine these provisions in the Anglophone 'Five Eyes' (FVEY) [1] countries - Australia, Canada, New Zealand, the United Kingdom and the United States (US) - with a focus on those that attempt to regulate communications providers. The paper culminates with the first comparative analysis of recent developments in Australia. The Australian developments are novel in the breadth of entities to which they may apply and their extraterritorial reach: they attempt to regulate transnational actors, and may implicate Australian agencies in the enforcement - and potential circumvention - of foreign laws on behalf of foreign law enforcement agencies. This latter aspect represents a significant and troubling development in the context of FVEY encryption-related assistance provisions.

We explore this expansion of extraterritorial powers that extend the reach of all FVEY nations via Australia, by requesting or coercing assistance from transnational technology companies as "designated communications providers", and allowing foreign law enforcement agencies to request their Australian counterparts to make such requests. Australia has unique domestic legal arrangements, which includes an aggressive stance on mass surveillance (Molnar, 2017), an absence of comprehensive constitutional or legislated fundamental rights at the federal level (Daly & Thomas, 2017; Mann et al., 2018), and has recently enacted the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) [2], the focus of this article. We demonstrate that Australia's status as the 'weak link' in the FVEY alliance enables the introduction of laws less likely to be constitutionally or otherwise legally permissible elsewhere. We draw attention to the extraterritorial reach of the Australian provisions which affords the possibility for other FVEY members to engage in regulatory arbitrage to exploit the weaker human rights protections and oversight measures in Australia.

HUMAN RIGHTS AND NATIONAL SECURITY IN AUSTRALIA

Australia has a well-documented track record of 'hyper legislation' of national security measures (Roach, 2011), having passed over 64 anti-terrorism specific laws since 9/11 that have been recognised as having serious potential to encroach democratic rights and freedoms (Williams & Reynolds, 2017). Some of these laws have involved digital and information communications infrastructures and their operators, such as those facilitating Australian security and law enforcement agencies' use of Computer Network Operations (Molnar, Parsons, & Zouave, 2017) and the introduction of mandatory data retention obligations on internet service providers (Suzor, Pappalardo, & McIntosh, 2017). Australia's role as a leading proponent in advocating for stronger powers against encrypted communications is consistent with this history.

Yet, unlike any of the other FVEY members, Australia has no comprehensive enforceable human rights protection at the federal level (Daly & Thomas, 2017; Mann et al., 2018). [3] Australia does not have comprehensive constitutional rights (like the US and Canada), a legislated bill of rights (like NZ and the UK) nor recourse to regional human rights bodies (like the UK and its relationship with the European Convention on Human Rights) (Refer to Table 1).

Given this situation, we argue Australia is a 'weak link' among FVEY partners because its legal framework allows for a more vigorous approach to legislating for national security at the expense of human rights protections, including but not limited to, privacy (Williams & Reynolds, 2017; Mann et al., 2018). Australia's status as a human rights 'weak link' affords the 'legal possibility' for measures which may be 'legally impossible' in other jurisdictions, including those of the other FVEY countries, given peculiar domestic and regional rights protections.

ENCRYPTION LAWS IN THE FIVE EYES

FVEY governments have made frequent statements regarding their surveillance capabilities 'going dark' due to encryption, with consequences for their ability to prevent, detect and investigate serious crimes such as terrorism and the dissemination of child exploitation material (Comey, 2014). This is despite evidence that the extensive surveillance powers that these agencies maintain are mostly used for the investigation of drug offences (Wilson & Mann, 2017; Parsons & Molnar, 2017). Further, there is an absence of evidence that undermining encryption will improve law enforcement responses (Gill, Israel, & Parsons, 2018), coupled with disregard for the many legitimate uses of encryption (see e.g., Abelson et al., 2015), including the protection of fundamental rights (see e.g., Froomkin, 2015).

It is important to note, as per Koops and Kosta (2018), that communications may be encrypted by different actors at different points in the telecommunications process. Where, and who applies encryption, will affect which actors have the ability to decrypt communications, and accordingly where legal obligations to decrypt may lie, or be actioned. For example, in some scenarios the service provider maintains the means of decrypting the communications, but this would not be the case where the software provider or end user has the means to decrypt (i.e., 'at the ends'). More recently, the focus has shifted to communications providers offering encrypted services or facilitating a third party offering such services over their networks. These actors can be forced to decrypt communications either via 'backdoors' (i.e., deliberate weaknesses or vulnerabilities) built into the service, or via legal obligations to provide assistance. The latter scenario is not a technical backdoor *per se*, but could be conceptualised as a 'legal' means to acquire a 'backdoor' as the government agency will obtain covert access to the service and communications therein, thus having a similar outcome to a technical backdoor. It is these measures which are the focus of our analysis. We provide a brief overview of the legal situation in each FVEY country (Table 1), before turning to Australia as our main focus.

UNITED STATES

The legal situation in the US to compel decryption depends, at least in part, on the actor targeted. The US has no specific legislation dealing with encryption although other laws on government investigatory and surveillance powers may be applicable (Gonzalez, 2019). Forcing an individual to decrypt data or communications has generally been considered incompatible with the Fifth Amendment to the US Constitution (i.e. the right against self-incrimination), although there is no authoritative Supreme Court decision on the issue (Gill, 2018). Furthermore, the US government may be impeded by arguments that encryption software

constitutes 'speech' protected by the First Amendment and Fourth Amendment (Cook Barr, 2016; Gonzalez, 2019; see also Daly, 2017).

For communications providers, the US has a provision in the Communications Assistance for Law Enforcement Act (CALEA) §1002 on Capability Requirements for telecommunications providers, which states that providers will *not* be required to decrypt or ensure that the government can decrypt communications encrypted by customers, unless the provider has provided the encryption used (see e.g., Koops & Kosta, 2018). [4]

In an attempt to avoid the difficulty of forcing individuals to decrypt, and the CALEA requirements' application only to telecommunications companies, attention has been turned to technology companies, including equipment providers. Litigation has been initiated against companies that refuse to provide assistance; the most notable being the FBI-Apple dispute concerning the locked iPhone of one of the San Bernardino shooters (Gonzalez, 2019). Ultimately the FBI were able to unlock the iPhone without Apple's assistance, by relying on a technical solution from Cellebrite (Brewster, 2018), thereby engaging in a form of 'lawful hacking' (Gonzalez, 2019). Absent a superior court's ruling, or legislative intervention, the legal position regarding compelled assistance remains uncertain (Abraha, 2019).

CANADA

Canada does not have specific legislation that provides authorities the power to compel decryption. Canadian authorities have imposed requirements on wireless communications providers through spectrum licensing conditions in the form of the Solicitor General Enforcement Standards for Lawful Interception of Telecommunications (SGES) Standard 12 which obliges providers to decrypt any communications they have encrypted on receiving a lawful request, but excludes end-to-end encryption "that can be employed without the service provider's knowledge" (Gill, Israel, & Parsons, 2018, p. 59; West & Forcese, 2020). It appears the requirements only apply to encryption applied by the operator itself, can involve a bulk rather than case-by-case decryption requirement, do not require the operator to develop "new capabilities to decrypt communications they do not otherwise have the ability to decrypt", and do not prevent operators employing end-to-end encryption (Gill, Israel, & Parsons, 2018, p. 60; West & Forcese, 2020).

There are provisions of the Canadian Criminal Code which give operators immunity from civil and criminal liability if they cooperate with law enforcement 'voluntarily' by preserving or disclosing data to law enforcement, even without a warrant (Gill, Israel, & Parsons, 2018, p. 57). There are also production orders and assistance orders that can be issued under the Criminal Code to oblige third parties to assist law enforcement, and disclose documents and records which could, in theory, be used to target encrypted communications (Gill, Israel, & Parsons, 2018, pp. 62-63), but West and Forcese (2020, p. 13) cast doubt on this possibility. There are also practical limitations, including the fact that many digital platforms and service providers do not have a physical presence in Canada, and thus are effectively beyond the jurisdiction of Canadian authorities (West & Forcese, 2020). Here, Mutual Legal Assistance Treaty (MLATs) could be used, although their use is notoriously beset with delay, and may only be effective if the other jurisdiction has its own laws to oblige third parties to decrypt data or communications (West & Forcese, 2020).

The Canadian Charter of Rights and Freedoms has a number of sections relevant to how undermining encryption can interfere with democratic freedoms, namely sections 2 (freedom of expression), 7 (security of the person), 8 (right against unreasonable search and seizure), and

the right to silence and protection from self-incrimination contained in sections 7, 11 and 14 (West & Forcese, 2020). Case law from Canadian courts suggests that individuals cannot be compelled to decrypt their own data (Gill, 2018, p. 451). The Charter implications of BlackBerry's assistance to the Canadian police in the *R v Mirarchi* [5] case was never ruled on as the case was dropped (Gill, Israel, & Parsons, 2018, p. 58).

In absence of a legislative proposal before the Canadian Parliament, it is difficult to surmise how, and whether, anti-encryption powers would run up against human rights protections. Yet any concrete proposal would likely face scrutiny in the courts given the impacts on Canadians' Charter-protected rights.

NEW ZEALAND

In New Zealand, provisions in the Telecommunications (Interception Capability and Security) Act 2013 (TISCA) require network operators to ensure that their networks can be technically subjected to lawful interception (Cooper, 2018). [6] Section 10(3) requires that public telecommunications network operators, on receipt of a lawful request, must decrypt encrypted communications carried by its network, if that operator has provided the means of encryption. Subsection 10(4) states that an operator is not required to decrypt communications that have been encrypted using a publicly available product supplied by another entity, and the operator is not under any obligation to ensure that a surveillance agency has the ability to decrypt communications.

It appears these provisions may entail that an operator cannot provide end-to-end encryption on its services so that their networks can be subject to lawful interception - that is, they must maintain the cryptographic key where encryption is managed centrally by the service provider (Global Partners Digital, n.d.) and engineer a 'back door' into the service (Cooper, 2018). However, NGO NZ Council for Civil Liberties considered the impact of this provision is theoretical as most services are offshore, and this provision does not apply extraterritorially (Beagle, 2017). Yet, section 38 of TICSA allows the responsible minister to make "service providers" (discussed below) subject to provisions such as this on the same basis as "network operators", which may involve section 10 having an extraterritorial reach (Keith, 2020).

There is a further provision in section 24 of TISCA that places both network operators and service providers (defined as anyone, whether in New Zealand or not, who provides a communications service to an end user in New Zealand) under obligations to provide 'reasonable' assistance to surveillance agencies with interception warrants or lawful interception authorities, including the decryption of communications, when they were the source of the encryption. Such companies do not have to decrypt encryption they have not provided nor "ensure that a surveillance agency has the ability to decrypt any telecommunication" (TICSA s 24(4)(b)). It is unclear what "reasonable assistance" entails, and how that would apply to third party app providers such as WhatsApp (to which section 24 would *prima facie* apply but not section 10 in the absence of a section 38 decision). It is also unclear how this provision would be enforced against offshore companies (Dizon et al., 2019, pp. 74-75).

There are further provisions in the Search and Surveillance Act 2012 which affect encryption. Section 130 includes a requirement that "the user, owner, or provider of a computer system [...] offer reasonable assistance to law enforcement officers conducting a search and seizure including providing access information" which could be used to force an individual or business to decrypt data and communications (Dizon et al., 2019, p. 61). There is a lack of clarity as to how the privilege against self-incrimination operates (Dizon et al., 2019, pp. 62-63). There is

also a lack of clarity about what "reasonable assistance" from companies, which will likely be third parties, and not able to avail themselves of the protection against self-incrimination, may entail (Dizon et al., 2019, pp. 65-66).

New Zealand has human rights protections enshrined in its Bill of Rights Act 1990, and section 21 contains the right to be secure against unreasonable searches and seizures. However, it "does not have higher law status and so can be overridden by contrary legislation…but there is at least some effort to avoid inconsistencies" (Keith, 2020). There is also the privilege against self-incrimination, "the strongest safeguard available in relation to encryption as it works to prevent a person from being punished for refusing to provide information that could lead to criminal liability" (Dizon et al., 2019, p. 7). There is no freestanding right to privacy in the New Zealand Bill of Rights, and so aspects of privacy must be found via other recognised rights (Butler, 2013), or may be protected via data protection legislation and New Zealand courts' "relatively strong approach to unincorporated treaties, including human rights obligations" (Keith, 2020).

Despite being part of the FVEY communiques on encryption mentioned below, Keith (2020) views New Zealand's domestic approach as more "cautious or ambivalent", with "no proposal to follow legislation enacted by other Five Eyes countries".

UNITED KINGDOM

The most significant law is the UK's Investigatory Powers Act 2016 (henceforth IPA). [7] Section 253 allows a government minister, subject to approval by a 'Judicial Commissioner', to issue a 'Technical Capability Notice' (TCN) to any communications operator (which includes telecommunications companies, internet service providers, email providers, social media platforms, cloud providers and other 'over-the-top' services), whether UK-based or anywhere else in the world, imposing obligations on that provider. Such an obligation can include the operator having to remove "electronic protection applied by or on behalf of that operator to any communications or data". The government minister must also consider technical practicalities such as whether it is 'practicable' to impose requirements on operators, and for the operators to comply. Section 254 provides that Judicial Commissioners conduct a necessity and proportionality test before approving a TCN. This means that a provider receiving a TCN would not be able to provide end-to-end encryption for its customers, and must ensure there is a method of decrypting communications. In other words, the provider must centrally manage encryption and maintain the decryption key (Smith, 2017a).

In November 2017, the UK Home Office released a Draft Communications Data Code of Practice for consultation, which clarified that a TCN would *not* require a telecommunications operator to remove encryption *per se*, but "it requires that operator to maintain the capability to remove encryption when subsequently served with a warrant, notice or authorisation" (UK Home Office, 2017, p. 75). Furthermore, it was reiterated that an obligation to remove encryption can only be imposed where "reasonably practicable" for the communications provider to comply with, and the obligation can only pertain to encryption that the communications provider has itself applied, or in circumstances when this has been done, for example, by a contractor on the provider's behalf.

Later, in early 2018, after analysing responses to the Draft Code, the UK Home Office introduced draft administrative regulations to the UK Parliament, which were passed in March 2018. These regulations affirm the Home Office's previous statements that TCNs require that operators "maintain the capacity" to disclose communications data on receipt of an authorisation or warrant, and such notices can only impose obligations on telecommunications

providers to remove "electronic protection" applied by, or on behalf of, the provider "where reasonably practicable" (Ni Loideain, 2019, p. 186). This would seem to entail that encryption methods applied by the user are not covered by this provision (Smith, 2017b). However, Keenan (2019) argues that the regulations may "compel [...] operators to facilitate the 'disclosure' of content by targeting authentication functions" which may have the effect of secretly delivering messages to law enforcement.

While some of the issues identified above with the UK's TCNs may be clarified by these regulations, other issues remain. For example, the situation remains unclear for a provider wanting to offer end-to-end encryption to its customers without holding the means to decrypt them. Practical questions remain about how the provisions can be enforced against providers which may not be geographically based in the UK, such as technology companies and platforms which may or may not maintain offices in the UK. To date, there is also no public knowledge of whether any TCNs have been made, approved by Judicial Commissioners, and complied with by operators (Keenan, 2019).

In addition to TCNs, section 49 of the Regulation of Investigatory Powers Act (2000) (RIPA) allows law enforcement agencies in possession of a device to issue a notice to the device user or device manufacturer to compel them to unlock encrypted devices or networks (Keenan, 2019). The law enforcement officer must obtain permission from a judge on the grounds that it is "necessary in the interests of national security, for the purpose of preventing or detecting crime, or where it is in the interest of the economic well-being of the United Kingdom" (Keenan, 2019). Case law on section 49 notices in criminal matters has generally not found the provision's use to force decryption to violate the privilege against self-incrimination, in sharp distinction to the US experience (Keenan, 2019).

It is unclear whether these provisions would withstand such a challenge before the European Court of Human Rights on the basis of incompatibility with ECHR rights, especially Article 6 (right to a fair trial) and Article 8 (right to privacy).

AUSTRALIA

In Australia the encryption debate commenced in June 2017 when then-Australian Prime Minister Turnbull (in)famously stated that "the laws of mathematics are very commendable, but the only law that applies in Australia is the law of Australia" (Pearce, 2017, para. 8). This remark, interpreted colloquially as a 'war on maths' (Pearce, 2017), gestured at an impending legislative proposal that would introduce provisions to weaken end-to-end encryption.

In August 2018, the Five Eyes Alliance met in a 'Five Country Ministerial' (FCM) and issued a communique that stated: " *We agreed to the urgent need for law enforcement to gain targeted access to data, subject to strict safeguards, legal limitations, and respective domestic consultations"* (Australian Government Department of Home Affairs, 2018, para. 18). The communique was accompanied by a Statement of Principles on Access to Evidence and Encryption, assented to by all FVEY governments (Australian Government Department of Home Affairs, 2018). The statement affirmed the important but *non-absolute* nature of privacy, and signalled a "pressing international concern" posed by law enforcement inability to access encrypted content. FVEY partners also agreed to abide by three principles in the statement: mutual responsibility; the paramount status of rule of law and due process; and freedom of choice for lawful access solutions. "Mutual responsibility" relates to industry stakeholders being responsible for providing access to communications data. The "freedom of choice" principle relates to FVEY members encouraging service providers to "voluntarily establish lawful access

solutions to their products and services that they create or operate in our countries", with the possibility of governments "pursu[ing] technological, enforcement, legislative or other measures to achieve lawful access solutions" if they "continue to encounter impediments to lawful access to information" (Australian Government Department of Home Affairs, 2018, paras. 34-35).

In the month following this meeting, the Australian government introduced what became the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) (or '*AA Act*'), which was subsequently passed by the Australian Parliament in December 2018. The Act amends pre-existing surveillance legislation in Australia, including the *Telecommunications Act 1997* (Cth) and the *Telecommunications (Interception and Access) Act 1979* (Cth). It includes a series of problematic reforms that have extraterritorial reach beyond the Australian jurisdiction. [8]

Specifically, three new mechanisms which seem (at least at face value) to be inspired by the UK's IPA are introduced into the Telecommunications Act: Technical Assistance Requests (TARs), [9] Technical Assistance Notices (TANs) [10] and Technical Capability Notices (TCNs). [11] TARs can be issued by Australian security agencies [12] that may "ask the provider to do acts or things on a voluntary basis that are directed towards ensuring that the provider is capable of giving certain types of help." [13] TARs escalate to TANs compelling assistance and impose penalties for non-compliance. The Australian Attorney-General can also issue TCNs which "may require the provider to do acts or things directed towards ensuring that the provider is *capable* of giving certain types of help" or to actually do such acts and things.

While the language of TCN is similar to the UK IPA, there is a much longer and more broadly worded list of "acts or things" that a provider can be asked to do on receipt of a TCN. [14] Although, as per section 317ZG, "systemic weaknesses" cannot be introduced, [15] there is still a significant potential impact on the security and privacy of encrypted communications. An important distinction between Australian and the UK TCNs is that the Australian notices are issued by the executive and are not subject to judicial oversight (Table 1).

The *AA Act* has extraterritorial reach beyond Australia in two main ways. The first is via obligations imposed on "designated communications providers" located outside Australia. "Designated communications providers" is defined extremely broadly to include, *inter alia,* carriers, carriage service providers, intermediaries and ancillary service providers, and any provider of an "electronic service" with any end-users in Australia, or of software likely to be used in connection with such a service, that has any end-users in Australia. It includes any "constitutional corporation" [16] that manufactures, installs, maintains or supplies devices for use, or likely to be used, in Australia, or develops, supplies or updates software that is capable of being installed on a computer or device that is likely to be connected to a telecommunications network in Australia (Ford & Mann, 2019). Thus a very wide range of providers from Australia and overseas will fall within these definitions (McGarrity & Hardy, 2020). Failure to comply with notices may result in financial penalties for companies, yet it is not clear how such penalties may be enforced *vis-à-vis* companies which are not incorporated or located in Australia. In any case in which a TAR is issued, it provides designated communications providers with civil immunity [9] from damages that may arise from the request (for example, rendering phones or devices useless), which may incentivise compliance prior to escalation to an enforceable TAN or TCN (Ford & Mann, 2019).

The second aspect of the *AA Act*'s extraterritorial reach is the provision of assistance by Australian law enforcement to their counterparts via the enforcement of foreign laws. The TARs, TANs, and TCNs all involve "assisting the enforcement of the criminal laws of a foreign country,

so far as those laws relate to serious foreign offences". [17] This is also reinforced by further amendments to the *Mutual Assistance in Criminal Matters Act 1987* (Cth) that bypass MLAT processes, and provide a conduit to the extraterritorial application of Australia's surveillance laws. That is, Australian law enforcement agencies are able to assist foreign governments through their requests for Australian assistance, including in the form of accessing encrypted communications and/or designing new ways to access encrypted communications (as per TCNs), for the enforcement of their own criminal laws. [18] This may operate as a loophole through which foreign law enforcement agencies circumvent their own legal system's safeguards and capitalise on Australia's lack of a federal human rights framework (Ford & Mann, 2019).

Table 1: Overview of anti-encryption measures in each FVEY country

	United States	**Canada**	**New Zealand**	**United Kingdom**	**Australia**
Relevant law/s	Communications Assistance for Law Enforcement Act §□1002.	No specific legislation that provides authorities the power to compel decryption. Narrow obligation in Solicitor General Enforcement Standards for Lawful Interception of Telecommunications (SGES) Standard 12.	Telecommunications (Interception Capability and Security) Act 2013 sections 10 and 24.	Investigatory Powers Act 2016 section 253.	*Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) section 317A.
Entities targeted	Application only to "telecommunications companies."	Application only to "wireless communication providers."	Section 10 applies to "network operators" and section 24 applies to "network operators" and "service providers".	Any "communications operator" (which includes telecoms companies, internet service providers, email providers, social media platforms, cloud providers and other 'over-the-top' services).	The definition of "designated communications provider" is set out in section 317C. It includes but is not limited to "a carrier or carriage service provider", "person provides an electronic service that has one or more end-users in Australia", or "the person manufactures or supplies customer equipment for use, or likely to be used, in Australia".

	United States	Canada	New Zealand	United Kingdom	Australia
Statutory obligations imposed on target	Companies will *not* be required to decrypt or ensure that the government can decrypt communications encrypted by customers, unless the provider itself has provided the encryption used.	Providers must decrypt any communications they have encrypted themselves on receiving a lawful request. Seems not to apply to end-to-end encryption not applied by the provider.	Operators, on the receipt of a lawful request to provide interception, must decrypt encrypted communications carried by its network, if that operator has provided the means of encryption (s 10). Operators and providers must provide "reasonable" assistance to surveillance agencies with interception warrants or lawful interception authorities, including the decryption of communications when they have provided the encryption (s 24).	Operators obliged to do certain things which can include the removal of "electronic protection applied by or on behalf of that operator to any communications or data". It is unclear whether a provider receiving a TCN would be able provide end-to-end encryption for its customers.	Providers may be issued with Technical Assistance Requests (TARs), Technical Assistance Notices (TANs) and/or Technical Capability Notices (TCNs). TARs can be issued by Australian security agencies that may "ask the provider to do acts or things on a voluntary basis that are directed towards ensuring that the provider is capable of giving certain types of help." TARs escalate to TANs compelling assistance and impose penalties for non-compliance. The Australian Attorney-General can also issue TCNs which "may require the provider to do acts or things directed towards ensuring that the provider is *capable* of giving certain types of help" or to actually do such acts and things.
Human rights protections	US Constitution, notably the Fourth and Fifth Amendment. Also, First Amendment in terms of cryptographic code as a possible form of protected free speech.	Canadian Charter of Rights and Freedoms: Section 2 (freedom of expression), Section 7 (security of the person), Section 8 (right against unreasonable search and seizure), and the right to silence and protection from self-incrimination contained in sections 7, 11 and 14.	Human Rights Act 1993.	Human Rights Act 1998, European Convention on Human Rights.	No comprehensive protection at the federal level; no right to privacy in Australian Constitution.
Approval mechanisms for encryption powers' exercise	N/A	Minister of Public Safety (executive branch).	Powers subject to interception warrants or other lawful interception authority. "Indirect" judicial supervision (Keith, 2020).	Approval by Judicial Commissioner.	Approval by administrative or executive officer (TCNs are approved by the Attorney-General). If a warrant or authorisation was previously required for the activity, it is still required after these reforms.
Extraterritorial application	Does not apply extraterritorially	Does not apply extraterritorially.	Section 10 does not apply extraterritorially unless section 38 decision made. Section 24 applies to both NZ providers and foreign providers providing a service to any end-user in NZ.	Applies to both UK-based and foreign-based communications operators.	Applies to both Australian and foreign-based providers. Providers can receive notices to assist with the enforcement of foreign criminal laws.
Relevant court cases	Apple-FBI	*R v Mirarchi*	None known.	None known.	Not applicable.

DISCUSSION

The recent legislative developments in Australia position it as a leading actor in the ongoing calls for a broader set of measures to weaken or undermine encryption. The *AA Act* introduces wide powers for Australian law enforcement and security agencies to request, or mandate assistance in, communications interception from a wide category of communications providers, internet and equipment companies, both in Australia and overseas, *and* permits foreign agencies to make requests to Australian agencies to use these powers in the enforcement of foreign laws. Compared to the other FVEY jurisdictions' laws in Table 1, the *AA A*ct's provisions cover the broadest category of providers and companies, to do the broadest category of assistance acts, with the weakest oversight mechanisms and no protections for human rights.

Australia's *AA Act* also gives these provisions the most broad and significant extraterritorial reach of the FVEY equivalent. While New Zealand and the UK also extend their assistance obligations to foreign entities, Australia's *AA Act* surpasses this to provide assistance to foreign law enforcement agencies. This is a highly worrying development since the *AA Act* facilitates the paradoxical enforcement (of criminal laws) and circumvention of (human rights) foreign laws on behalf of foreign law enforcement agencies, through *inter alia* the coercion of transnational technology companies into designing new ways of undermining encryption at a global scale via Australian law in the form of TCNs.

The idea of jurisdiction shopping by FVEY law enforcement agencies may be applicable, whereby Australia has enacted powers that have extraterritorial consequence, and that could operate to serve the wider FVEY alliance, especially given the lack of judicial oversight of TCNs, and Australia's weak human rights protections. Jurisdiction shopping concerns the strategic pursuance of legislative, policy and operational objectives in specific venues to achieve outcomes that may not be possible in other venues due to the local context. [19]

The *AA Act* provisions expand legally permissible extraterritorial measures to obtain encrypted communications, and in theory, this enables FVEY partners to 'jurisdiction shop' to exploit the lack of human rights protections in Australia. This is not the first time Australia has been an attractive jurisdiction shopping destination. One previous example relates to Operation Artemis run by the Queensland Police where a website used for the dissemination of child exploitation material was relocated to Australian servers so that police could engage in a controlled operation and commit criminal offences (including the dissemination of child exploitation material) without criminal penalty (Høydal, Stangvik, & Hansen, 2017; McInnes, 2017). [20]

Australia emerges as a strategic forum for FVEY partners to implement new laws and powers with extraterritorial reach, as unlike other FVEY members, Australia has no meaningful human rights protections that would prevent gross invasions arising from measures that undermine encryption, coupled with weak oversight mechanisms (McGarrity & Hardy, 2020). These considerations also relate to the pre-existing use of 'regulatory arbitrage' by FVEY members, which involves information being legally accessed and intercepted in one of the FVEY countries with weaker human rights protection, then being transferred and used in other FVEY countries with more restrictive legal frameworks (Citron & Pasquale, 2010). This situation may allow for authorisation for extraterritorial data gathering to, in effect, be funnelled through the 'weak link' of Australia. Thus, the *AA Act* presents an opportunity for FVEY partners to engage in further regulatory arbitrage by jurisdiction shopping their requests to access encrypted communications *and* to mandate designated communications providers (i.e. transnational technology

companies) design and develop new ways to access encrypted communications via Australia.

However, it is difficult to ascertain the extent to which the FVEY partners are indeed exploiting the Australian 'weak link', for two reasons. One, the FVEY alliance operates in a highly secretive manner. Second, the *AA Act* severely restricts transparency, via the introduction of secrecy provisions and enhanced penalties for unauthorised disclosure, and an absence of judicial authorisation of the exercise of the powers (Table 1). There is very limited ex-post aggregated public reporting of the exercise of the powers. One of these few mechanisms is the Australian Department of Home Affairs annual report on the operation of the *Telecommunications (Interception and Access) Act 1979* (Cth). The 2018-2019 report stated that seven TARs were issued, five to the Australian Federal Police and two to the New South Wales Police. Cybercrime and telecommunications offences were the two most common categories of crimes for which the TARs were issued, with the notable absence of any terrorism offences - the main rationale supporting the introduction of the powers. In the Australian Senate Estimates process in late 2019, it was revealed that the TAR powers had been used on a total of 25 occasions up to November 2019 (Sadler, 2020a). [21] The fact that only TARs have been issued may indicate that designated communications providers are complying with requests in the first instance, and thus there is no need to escalate to enforceable notices.

One possible, and as yet unresolved, countervailing development to the *AA Act* in the FVEY countries concerns the US introduction of the Clarifying Lawful Overseas Use of Data (CLOUD) Act, which aims to facilitate US and foreign law enforcement access to data held by US-based communications providers in criminal investigations, bypassing MLAT procedures (Abraha, 2019; see also Gstrein, 2020, this issue; Vazquez Maymir, 2020, this issue). Bilateral negotiations regarding mechanisms for accessing (via US technology companies) and sharing e-evidence under the CLOUD Act between the US and Australia are underway, and there have been some early questions and debates (Bogle, 2019; Hendry, 2020) as to whether Australia will comply with CLOUD requirements. Specifically, the CLOUD Act allows "foreign partners that have robust protections for privacy and civil liberties to enter into executive agreements with the United States to use their own legal authorities to access electronic evidence" (Department of Justice, n.d) (PDF). CLOUD agreements between the US and foreign governments should not include any obligations forcing communications providers to maintain data decryption capabilities nor should they include any obligation preventing providers from decrypting data. [22] It is uncertain whether Australia would comply with CLOUD requirements given its aforementioned weak human rights framework, and the absence of judicial oversight for the authorisation of the anti-encryption powers.

These concerns seem to have motivated the current Australian opposition party, Labor, to introduce a private member's bill into the Australian Parliament in late 2019 to 'fix' some aspects of the *AA Act*, despite their bipartisan support in passage of the law at the end of 2018. Notable fixes sought include the introduction of enhanced safeguards, including judicial oversight and clarification that TARs, TANs, and TCNs cannot be used to force providers to build systemic weaknesses and vulnerabilities in their systems, including implementing or building a new decryption capability. At the time of writing, the Australian Parliament is considering the bill, although it is unlikely it will be passed given the government has indicated it will vote down Labor's proposed amendments (Stadler, 2020b).

CONCLUSION

Laws to restrict encryption occur in the context of regulatory arbitrage (Citron & Pasquale, 2010). This paper has analysed new powers that allow for Australian law enforcement and security agencies to request or mandate assistance in accessing encrypted communications, *and* permits foreign agencies to make requests to Australian agencies to use these powers in the enforcement of foreign laws, taking advantage of a situation where there is less oversight and fewer human rights or constitutional protections. The *AA Act* presents new opportunities for FVEY partners to leverage access to (encrypted) communications via Australia's 'legal backdoors', which may undermine protections that might otherwise exist within local legal frameworks. This represents a troubling international development for privacy and information security.

ACKNOWLEDGEMENTS

The authors would like to acknowledge Dr Kayleigh Murphy for her excellent research assistance and the Computer Security and Industrial Cryptography (COSIC) Research Group at KU Leuven, the Law Science Technology Society (LSTS) Research Group at Vrije Universiteit Brussel, and the Department of Journalism in Maria Curie-Skłodowska University (Lublin, Poland) for the opportunity to present and receive feedback on this research. Finally, we thank Tamir Israel, Martin Kretschmer, Balázs Bodó, and Frédéric Dubois for their comprehensive peer-review comments and editorial review.

REFERENCES

Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W., Gilmore, J., Green, M., Landau, S., Neumann, P. G., Rivest, R. L., Schiller, J. I., Schneier, B., Specter, M. A., & Weitzner, D. J. (2015). Keys under doormats: Mandating insecurity by requiring government access to all data and communications. *Journal of Cybersecurity*, *1*(1), 69–79. https://doi.org/10.1093/cybsec/tyv009

Abraha, H. H. (2019). How Compatible is the US 'CLOUD' Act' with Cloud Computing? A Brief Analysis. *International Data Privacy Law*, *9*(3), 207–215. https://doi.org/10.1093/idpl/ipz009

Australian Constitution. https://www.aph.gov.au/about_parliament/senate/powers_practice_n_procedures/constitution

Australian Government Department of Home Affairs. (2018). *Five country ministerial 2018*. Australian Government Department of Home Affairs. https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-coordination/five-country-ministerial-2018

Australian Government, Department of Home Affairs. (2019). *Telecommunications (Interception and Access) Act 1979: Annual Report 2018-19* [Report]. Australian Government, Department of Home Affairs. https://parlinfo.aph.gov.au/parlInfo/download/publications/tabledpapers/c424e8ec-ce9a-4dc1-a53e-4047e8dc4797/upload_pdf/TIA%20Act%20Annual%20Report%202018-19%20%7BTabled%7D.pdf;fileType=application%2Fpdf#search=%22publications/tabledpapers/c424e8ec-ce9a-4dc1-a53e-4047e8dc4797%22

Beagle, T. (2017, July 2). Why we support effective encryption [Blog post]. *NZ Council for Civil Liberties*. https://nzccl.org.nz/content/why-we-support-effective-encryption

Bell, S. (2013, November 25). Court rebukes CSIS for secretly asking international allies to spy on Canadian suspects travelling abroad. *The National Post*. https://nationalpost.com/news/canada/court-rebukes-csis-for-secretly-asking-international-allies-to-spy-on-canadian-terror-suspects

Bogle, A. (2019, October 31). Police want Faster Data from the US, but Australia's Encryption Laws Could Scuttle the Deal. *ABC News*. https://www.abc.net.au/news/science/2019-10-31/australias-encryption-laws-could-scuttle-cloud-act-us-data-swap/11652618

Brewster, T. (2018, February 26). *The Feds Can Now (Probably) Unlock Every iPhone Model in Existence*. https://www.forbes.com/sites/thomasbrewster/2018/02/26/government-can-access-any-apple-iphone-cellebrite/#76a735e8667a

Butler, P. (2013). The Case for a Right to Privacy in the New Zealand Bill of Rights Act. *New Zealand Journal of Public & International Law*, *11*(1), 213–255.

Citron, D. K., & Pasquale, F. (2010). Network Accountability for the Domestic Intelligence Apparatus. *Hastings*, *62*, 1441–1494. https://digitalcommons.law.umaryland.edu/fac_pubs/991/

Comey, J. B. (2014). *Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?* Federal Bureau of Investigation. https://www.fbi.gov/news/speeches/going-dark-are-

technology-privacy-and-public-safety-on-a-collision-course

Constitution Act, (1982). https://laws-lois.justice.gc.ca/eng/const/page-15.html

Cook Barr, A. (2016). Guardians of Your Galaxy S7: Encryption Backdoors and the First Amendment. *Minnesota Law Review*, *101*(1), 301–339. https://minnesotalawreview.org/article/note-guardians-of-your-galaxy-s7-encryption-backdoors-and-the-first-amendment/

Cooper, S. (2018). An Analysis of New Zealand Intelligence and Security Agency Powers to Intercept Private Communications: Necessary and Proportionate? *Te Mata Koi: Auckland University Law Review*, *24*, 92–120.

Daly, A. (2017). Covering up: American and European legal approaches to public facial anonymity after SAS v. France. In T. Timan, B. C. Newell, & B.-J. Koops (Eds.), *Privacy in Public Space: Conceptual and Regulatory Challenges*(pp. 164–183). Edward Elgar.

Daly, A., & Thomas, J. (2017). Australian internet policy. *Internet Policy Review*, *6*(1). https://doi.org/10.14763/2017.1.457

Department of Justice. (n.d.). *Frequently Asked Questions*. https://www.justice.gov/dag/page/file/1153466/download

Dizon, M., Ko, R., Rumbles, W., Gonzalez, P., McHugh, P., & Meehan, A. (2019). *A Matter of Security, Privacy and Trust: A study of the principles and values of encryption in New Zealand (Report*. New Zealand Law Foundation and University of Waikato.

Ford, D., & Mann, M. (2019). International Implications of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018. *Australian Privacy Foundation*. https://privacy.org.au/wp-content/uploads/2019/06/APF_AAAct_FINAL_040619.pdf

Froomkin, D. (2015). U.N. Report Asserts Encryption as a Human Right in the Digital Age. *The Intercept*. https://theintercept.com/2015/05/28/u-n-report-asserts-encryption-human-right-digital-age/

Gill, L. (2018). Law, Metaphor and the Encrypted Machine. *Osgoode Hall Law Journal*, *55*(2), 440–477. https://doi.org/10.2139/ssrn.2933269

Gill, L., Israel, T., & Parsons, C. (2018). *Shining a Light on the Encryption Debate: A Canadian Fieldguide* [Report]. Citizen Lab; The Canadian Internet Policy & Public Interest Clinic. https://citizenlab.ca/2018/05/shining-light-on-encryption-debate-canadian-field-guide/

Global Partners Digital. (n.d.). *World Map of Encryption Law and Policies*. https://www.gp-digital.org/world-map-of-encryption/

Gonzalez, O. (2019). Cracks in the Armor: Legal Approaches to Encryption. *Journal of Law, Technology & Policy*, *2019*(1), 1–46. http://illinoisjltp.com/journal/wp-content/uploads/2019/05/Gonzalez.pdf

Gstrein, O. (2020). Mapping power and jurisdiction on the internet through the lens of government-led surveillance. *Internet Policy Review*, *9*(3). https://doi.org/10.14763/2020.3.1497

Hendry, J. (2020, January 14). Home Affairs Rejects Claims Anti-Encryption Laws Conflict with US CLOUD Act. *IT News*. https://www.itnews.com.au/news/home-affairs-rejects-claims-anti-encryption-laws-conflict-with-us-cloud-act-536339

Holyoke, T., Brown, H., & Henig, J. (2012). Shopping in the Political Arena: Strategic State and Local Venue Selection by Advocates. *State and Local Government Review*, *44*(1), 9–20. https://doi.org/10.1177/0160323X11428620

Høydal, H. F., Stangvik, E. O., & Hansen, N. R. (2017, October 7). Breaking the Dark Net: Why the Police Share Abuse Pics to Save Children. *VG*. https://www.vg.no/spesial/2017/undercover-darkweb/?lang=en

Human Rights, E. C. (2010). *European Convention on Human Rights*. https://www.echr.coe.int/Documents/Convention_ENG.pdf

Investigatory Powers Act 2016 (UK), Pub. L. No. 2016 c. 25 (2016). http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted

Investigatory Powers (Technical Capability) Regulations 2018 (UK. (n.d.). http://www.legislation.gov.uk/ukdsi/2018/9780111163610/contents

Keenan, B. (2019). State access to encrypted data in the United Kingdom: The 'transparent' approach. *Common Law World Review*. https://doi.org/10.1177/1473779519892641

Keith, B. (2020). Official access to encrypted communications in New Zealand: Not more powers but more principle? *Common Law World Review*. https://doi.org/10.1177/1473779520908293

Telecommunications Amendment (Repairing Assistance and Access) Bill 2019, (2019) (testimony of Kristina Keneally). https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/s1247_first-senate/toc_pdf/19S1920.pdf;fileType=application%2Fpdf

Koops, B.-J. (1999). *The Crypto Controversy: A Key Conflict in the Information Society*. Kluwer Law International.

Koops, B.-J., & Kosta, E. (2018). Looking for some light through the lens of "cryptowar" history: Policy options for law enforcement authorities against "going dark". *Computer Law & Security Review*, *34*(4), 890–900. https://doi.org/10.1016/j.clsr.2018.06.003

Ley, A. (2016). Vested Interests, Venue Shopping and Policy Stability: The Long Road to Improving Air Quality in Oregon's Willamette Valley. *Review of Policy Research*, *33*(5), 506–525. https://doi.org/10.1111/ropr.12190

Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique. *Big Data & Society*, *1*(2). https://doi.org/10.1177/2053951714541861

Lyon, D. (2015). *Surveillance After Snowden*. Polity Press.

Mann, M., & Daly, A. (2019). (Big) data and the north-in-south: Australia's informational imperialism and digital colonialism. *Television and New Media*, *20*(4), 379–395. https://doi.org/10.1177/1527476418806091

Mann, M., Daly, A., Wilson, M., & Suzor, N. (2018). The Limits of (Digital) Constitutionalism: Exploring the Privacy-Security (Im)Balance in Australia. *International Communication Gazette*, *80*(4), 369–384. https://doi.org/10.1177/1748048518757141

McGarrity, N., & Hardy, K. (2020). Digital surveillance and access to encrypted communications in Australia. *Common Law World Review*. https://doi.org/10.117/1473779520902478.

McInnes, W. (2017, October 8). Queensland Police Take Over World's Largest Child Porn Forum in Sting Operation. *Brisbane Times*. https://www.brisbanetimes.com.au/national/queensland/queensland-police-behind-worlds-largest-child-porn-forum-20171007-gywcps.html

Molnar, A. (2017). Technology, Law, and the Formation of (il)Liberal Democracy? *Surveillance & Society*, *15*(3/4), 381–388. https://doi.org/10.24908/ss.v15i3/4.6645

Molnar, A., Parsons, C., & Zouave, E. (2017). Computer network operations and 'rule-with-law' in Australia. *Internet Policy Review*, *6*(1). https://doi.org/10.14763/2017.1.453

Murphy, H., & Kellow, A. (2013). Forum Shopping in Global Governance: Understanding States, Business and NGOs in Multiple Arenas. *Global Policy*, *4*(2), 139–149. https://doi.org/10.1111/j.1758-5899.2012.00195.x

Mutual Assistance in Criminal Matters Act 1987 Compilation No. 35, (2016). https://www.legislation.gov.au/Details/C2016C00952

Nagel, P. (2006). Policy Games and Venue-Shopping: Working the Stakeholder Interface to Broker Policy Change in Rehabilitation Services. *Australian Journal of Public Administration*, *65*(4), 3–16. https://doi.org/10.1111/j.1467-8500.2006.00500a.x

New Zealand Bill of Rights Act 1990. http://www.legislation.govt.nz/act/public/1990/0109/latest/DLM224792.html

Ni Loideain, N. (2019). A Bridge Too Far? The Investigatory Powers Act 2016 and Human Rights Law. In L. Edwards (Ed.), *Law, Policy and the Internet* (2nd ed., pp. 165–192). Hart.

Parsons, C. A., & Molnar, A. (2017). *Horizontal Accountability and Signals Intelligence: Lesson Drawing from Annual Electronic Surveillance Reports*. SSRN. http://dx.doi.org/10.2139/ssrn.3047272

Pearce, R. (2017, July 27). Australia's War on Maths Blessed with Gong at Pwnie Awards. *ComputerWorld*. https://www.computerworld.com.au/article/625351/australia-war-maths-blessed-gong-pwnie-awards/

Pfefferkorn, R. (2020, January 30). The EARN IT Act: How to Ban End-to-End Encryption Without Actually Banning It [Blog post]. *The Center for Internet Society*. https://cyberlaw.stanford.edu/blog/2020/01/earn-it-act-how-ban-end-end-encryption-without-actually-banning-it

Pralle, S. (2003). Venue Shopping, Political Strategy, and Policy Change: The Internationalization of Canadian Forest Advocacy. *Journal of Public Policy*, *23*(3), 233–260. https://doi.org/10.1017/S0143814X03003118

Regulation of Investigatory Powers Act 2000, Pub. L. No. 2000 c. 23 (2000).

http://www.legislation.gov.uk/ukpga/2000/23/contents

Roach, K. (2011). *The 9/11 Effect: Comparative Counter-Terrorism*. Cambridge University Press.

Sadler, D. (2020a, February 3). Encryption laws not used to fight terrorism [Blog post]. *InnovationAus*. https://www.innovationaus.com/encryption-laws-not-used-to-fight-terrorism/?fbclid=IwAR2fdjBwK827idNXHY4X5-5Xk3d8LZJBjSVJrLMutxBn6XeWXTvzyNhsVtg

Sadler, D. (2020b, February 14). No encryption fix until at least October [Blog post]. *InnovationAus*. https://www.innovationaus.com/no-encryption-fix-until-at-least-october/?fbclid=IwAR0HdUHyy2ArihJC6lEze0H_rxvJnB4ryNknGMAlsWf4PeibIpJXJYD--dI

Search and Surveillance Act, (2012). http://www.legislation.govt.nz/act/public/2012/0024/latest/DLM2136536.html

Smith, G. (2017, May 8). Back doors, black boxes and #IPAct technical capability regulations [Blog post]. *Graham Smith's Blog on Law, IT, the Internet and Online Media*. http://www.cyberleagle.com/2017/05/back-doors-black-boxes-and-ipact.html

Smith, Graham. (2017, May 29). Squaring the circle of end to end encryption [Blog post]. *Graham Smith's Blog on Law, IT, the Internet and Online Media*. https://www.cyberleagle.com/2017/05/squaring-circle-of-end-to-end-encryption.html

Solicitor General. (2008). *Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications*. https://perma.cc/NQB9-ZHPY

Suzor, N., Pappalardo, K., & McIntosh, N. (2017). The Passage of Australia's Data Retention Regime: National Security, Human Rights, and Media Scrutiny. *Internet Policy Review*, *6*(1). https://doi.org/10.14763/2017.1.454

Telecommunications Act, (1997). https://www.legislation.gov.au/Details/C2017C00179

Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018, Pub. L. No. 148 (2018). https://www.legislation.gov.au/Details/C2018A00148

Telecommunications (Interception Capability and Security) Act 2013 (NZ), (2013). http://www.legislation.govt.nz/act/public/2013/0091/22.0/DLM5177923.html

United Kingdom Home Office. (2017). *Communications Data Draft Code of Practice*. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/663675/November_2017_IPA_Consultation_-_Draft_Communications_Data_Code_of_Pract....pdf

US Telecommunications: Assistance Capability Requirements, USC § 1002, 47 Telecommunications § 1002 (1994). https://www.law.cornell.edu/rio/citation/108_Stat._4280

Vazquez Maymir, S. (2020). Anchoring the Need to Revise Cross-Border Access to E-Evidence. *Internet Policy Review*, *9*(3). https://doi.org/10.14763/2020.3.1495

West, L., & Forcese, C. (2020). Twisted into knots: Canada's challenges in lawful access to encrypted communications. *Common Law World Review*. https://doi.org/10.1177/1473779519891597

Williams, G., & Reynolds, D. (2017). *A charter of rights for Australia* (4th ed.). NewSouth Press.

Wilson, M., & Mann, M. (2017, September 7). Police Want to Read Encrypted Messages, but They Already Have Significant Power to Access our Data. *The Conversation*. https://theconversation.com/police-want-to-read-encrypted-messages-but-they-already-have-significant-power-to-access-our-data-82891

Zuan, N., Roos, C., & Gulzau, F. (2016). Circumventing Deadlock Through Venue-shopping: Why there is more than just talk in US immigration politics in times of economic crisis. *Journal of Ethnic and Migration Studies*, *42*(10), 1590–1609. https://doi.org/10.1080/1369183X.2016.1162356

FOOTNOTES

1. The FVEY partnership is a comprehensive intelligence alliance formed after the Second World War, formalised under the UKUSA Agreement (see e.g., Mann & Daly, 2019).

2. Cth stands for Commonwealth, which means "federal" legislation, as distinct from state-level legislation.

3. At the state and territory level: Victoria, Queensland and the Australian Capital Territory have human rights laws, however the surveillance powers examined in this article are subject to Commonwealth jurisidiction rendering so these state and territory based protections are inapplicable. See: *Charter of Human Rights and Responsibilities Act 2006* (Vic); *Human Rights Act 2019 (QLD); Human Rights Act 2004* (ACT).

4. However, the draft EARN IT bill currently before the US Congress, if enacted, may impact negatively upon providers' ability to offer end-to-end encrypted messaging. See Pfefferkorn (2020).

5. *R v Mirarchi* involved BlackBerry providing the Canadian police with a key which allowed them to decrypt one million BlackBerry messages (Gill, Israel & Parsons, 2018, p. 57-58). The legal basis and extent of BlackBerry's assistance to the Canadian police was unclear from the 'heavily redacted' court records (West & Forcese, 2020).

6. For a full picture of New Zealand legal provisions which may affect encryption see Dizon et al. (2019).

7. For additional provisions in UK law which may be relevant to encryption see Keenan (2019).

8. The analysis presented here focuses on Schedule 1 of the AA Act. Schedule 2 of the AA Act introduces computer access warrants that allow law enforcement to covertly access and search devices, and to conceal the fact that devices have been accessed.

9. a. b. S 317G.

10. S 317L.

11. S 317T.

12. Namely 'the Director□General of Security, the Director□General of the Australian Secret Intelligence Service, the Director□General of the Australian Signals Directorate or the chief officer of an interception agency'.

13. Namely 'ASIO, the Australian Secret Intelligence Service, the Australian Signals Directorate or an interception agency'.

14. For example, "removing one or more forms of electronic protection that are or were applied by, or on behalf of, the provider", "installing, maintaining, testing or using software or equipment" and "facilitating or assisting access to… a facility, customer equipment, electronic services and software" are included in the list of 'acts or things' that a provider may be asked to do via these provisions. The complete list of 'acts or things' are listed in section 317E

15. According to AA Act s 317B a systematic vulnerability means "a vulnerability that affects a whole class of technology, but does not include a vulnerability that is selectively introduced to one or more target technologies that are connected with a particular person" and a systematic weakness means "a weakness that affects a whole class of technology, but does not include a weakness that is selectively introduced to one or more target technologies that are connected with a particular person."

16. A category which, according to paragraph 51(xx) of the Australian Constitution, comprises "foreign corporations, and trading or financial corporations formed within the limits of the Commonwealth".

17. S 317A; Table 1.

18. AA Act s 15CC(1); Surveillance Devices Act 2004 (Cth) ss 27A(4) and (4)(a).

19. Analyses of policy venue shopping have been conducted in relation to a range of policy areas, inter alia, immigration, environmental, labour, intellectual property, and rehabilitation policies (see e.g., Ley, 2016; Holyoke, Brown, & Henig, 2012; Pralle, 2003; Zuan, Roos, & Gulzau, 2016; Nagel, 2006; Murphy & Kellow, 2013). According to Pralle (2003, p. 233) a central "component of any political strategy is finding a decision setting that offers the best prospects for reaching one's policy goals, an activity referred to as venue shopping". Further, Murphy and Kellow (2013, p. 139) argue that policy venue shopping may be a political strategy deployed at global levels where "entrepreneurial actors take advantage of 'strategic inconsistencies' in the characteristics of international policy arenas".

20. A further example that demonstrates regulatory arbitrage between FVEY members from the perspective of Canada, brought to light in 2013, involved Canada's domestic security intelligence service (CSIS) being found by the Federal Court to have 'breached duty of candour' by secretly refusing to disclose their leveraging of FVEY networks when it applied for warrants during an international terrorism investigation involving two Canadian suspects (Bell 2013).

21. It should be noted that due to the overlapping time frames and aggregated nature of reporting, the 25 occasions the powers were used may also include some of the 7 occasions reported in the most recent Home Affairs annual-report.

22. CLOUD Act s 105 (b) (3). Note: The US Department of Justice claims the CLOUD Act is "encryption neutral" in that "neither does it prevent service providers from assisting in such decryption, *or* prevent countries from addressing decryption requirements in their own domestic laws." (Department of Justice, n.d)