An Analysis of New Zealand Intelligence and Security Agency Powers to Intercept Private Communications: Necessary and Proportionate?

SIMONE COOPER*

The intersection of rapid technological change and global terrorism has created a problem for intelligence and security agencies that protect their home states. In response, Western legislatures have widened interception powers. This has privacy and security consequences for all users of communications technologies. This article analyses recent changes to the law governing communications interception in New Zealand and places these changes in a global and local context. It measures the Telecommunications (Interception Capability and Security) Act 2013 and the Intelligence and Security Act 2017 against the International Principles on the Application of Human Rights to Communications Surveillance*. Ultimately, this article argues that the New Zealand legislative framework fails to comply with this international best practice.*

I INTRODUCTION

The intersection of rapid technological change and global terrorism has created a problem for intelligence and security agencies that protect their respective nations. People who commit crimes and acts of terrorism employ ubiquitous communications technologies used by billions of innocent citizens. In response, Western legislatures have widened interception powers. This has privacy and security consequences for all users. In New Zealand, this change is embodied in the Telecommunications (Interception Capability and Security) Act 2013 (TICSA) and the Intelligence and Security Act 2017 (ISA).

This article looks at the global and local context of surveillance powers and analyses whether New Zealand law complies with international best practice contained in the *International Principles on the Application of Human Rights to Communications Surveillance* (*Necessary & Proportionate Principles*).[1] It is limited in scope to the powers of New Zealand's intelligence and security agencies: the Government Communications Security Bureau (GCSB) and the New Zealand Security Intelligence Service (NZSIS).

* BA/LLB(Hons). Thank you to retired Judge Dr David Harvey, Sam Arcand, and Noel and Linda Cooper.

1 Necessary & Proportionate *International Principles on the Application of Human Rights to Communications Surveillance* (May 2014) [*Necessary & Proportionate Principles*].

Part II details the global and local context of state surveillance powers. It frames international developments from the 21st century in the context of the 'going dark' debate. One side of this debate calls for an expansion of interception powers in response to increasingly encrypted, 'dark' communications channels. The alternative argument is that we are living in a golden age of surveillance. Governments have more access to intelligence now than ever before due to the pervasive use of digital technologies by the public. Accordingly, greater surveillance powers, in conflict with human rights, are uncalled for. Part II then explores the influence of these ideas on the New Zealand legislative context.

Part III briefly sets out the relevant New Zealand legislation: the ISA and the TICSA. This article does not consider the Privacy Bill 2018 because it does not substantively alter the obligations of the GCSB and NZSIS as discussed in this article.[2] This is largely due to a number of general[3] and specific[4] exceptions applicable to those agencies.

Part IV analyses the law against a number of the *Necessary & Proportionate Principles*. It concludes that the New Zealand legislation does not meet international best practice for communications interception law.

II CONTEXT

The TICSA and the ISA are best understood when situated within their global and local context. Law is a reflection of the values and concerns of legislators and, theoretically, the constituency they represent. Concerns about terrorism and the appropriate limits of state surveillance powers are at the forefront of the public, legislative and academic imaginations of communications interception. The first Section of this Part provides a global view of these issues, both geographically and conceptually. It explains key converging factors that shape surveillance discourses and law reform, and introduces critiques of the 'going dark' narrative that drives expansive surveillance powers. The second section provides a local narrative. It explains the origins of the TICSA and the ISA and their rationale, and indicates key areas of concern, which will be developed in Part IV.

Global Context

On 22 March 2017, Khalid Masood mounted the footpath along Westminster Bridge, killing three pedestrians before stabbing a Police officer outside the Houses of Parliament.[5] He used encrypted messaging service WhatsApp a few

2 Privacy Bill 2018 (34-1).
3 Clauses 52(1)(a)(i), 60(4)(b) and 61(4)(b). See also IPP 10(1)(f) and IPP 11(1)(f) in cl 19.
4 Clauses 25, 54(a) and 100(1). See also IPP 10(2) and IPP 11(1)(g) in cl 19.
5 Esther Addley, Luke Harding and Robert Booth "'All hell was let loose': witnesses on the Westminster attack" *The Guardian* (online ed, London, 22 March 2017).

minutes before the attack.[6] The British Home Secretary responded by declaring WhatsApp's end-to-end encryption (E2EE) "completely unacceptable" and a hiding place for terrorists.[7] This is a familiar narrative. Former United Kingdom Prime Minister David Cameron had previously called for a ban on E2EE following the *Charlie Hebdo* attacks in 2015.[8]

This is part of the 'going dark' debate, the latest in a series of discourses concerning technology, terrorism and surveillance. The problem as framed by lawmakers is that terrorists, like the rest of the population, are increasingly using encrypted mobile messaging applications to recruit, organise and execute attacks in the West. The law has failed to keep pace with this technology. Even where intelligence and security agencies have the lawful authority to intercept communications, they do not have the technical ability or legislative framework to compel the likes of Apple, Google and Facebook to decrypt them.[9]

Encryption is not a new technology. However, for the average computer user, using early forms of encryption[10] requires a degree of dedication and knowledge that "is simply too much for most users to bother".[11] Apple, Google and Facebook's decisions to build E2EE into their messaging applications,[12] and encrypt their devices and operating systems[13] resulted in a large number of everyday communications and user content moving 'into the dark'.[14] However, Peter Swire and Kenesa Ahmad argue that despite the wider use of encryption, we are currently living in a "Golden Age of Surveillance".[15]

Following the September 11 terror attacks, the United States, followed by other Western democracies, massively expanded the technological capabilities and surveillance powers of their law enforcement

---

6 Andrew Sparrow "WhatsApp must be accessible to authorities, says Amber Rudd" *The Guardian* (online ed, London, 26 March 2017).

7 For a brief and digestible outline of end-to-end encryption and the issues discussed in this article, see Computerphile "End to End Encryption (E2EE) - Computerphile" (30 March 2017) YouTube <www.youtube.com>.

8 Rowena Mason "UK spy agencies need more powers, says Cameron" *The Guardian* (online ed, London, 12 January 2015); and see Alex Hern "How has David Cameron caused a storm over encryption?" *The Guardian* (online ed, London, 15 January 2015).

9 See James Comey, former Director of the Federal Bureau of Investigation "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?" (speech to the Brookings Institution, Washington DC, 16 October 2016).

10 For example, Pretty Good Privacy [PGP], which works by Person A encrypting a message with a public key and Person B decrypting it with a private key that only Person B knows. Note that this is a simplified explanation; for a brief and digestible overview of PGP, see Bernard John Poole "PGP Tutorial for Beginners to PGP" (7 December 2017) University of Pittsburgh <www.pitt.edu>.

11 Jonathan Zittrain and others "Don't Panic: Making Progress on the 'Going Dark' Debate" (Berkman Center for Internet & Society Research Paper 2016-1, Harvard University, 2016) at 4–5.

12 Andy Greenberg "WhatsApp Just Switched on End-to-End Encryption for Hundreds of Millions of Users" (18 November 2014) Wired <www.wired.com>.

13 David Sanger "Signaling Post-Snowden Era, New iPhone Locks Out NSA" *The New York Times* (online ed, New York, 26 September 2014); and Craig Timberg "Newest Androids will join iPhones in offering default encryption, blocking police" *The Washington Post* (online ed, Washington DC, 18 September 2014).

14 Zittrain, above n 11, at 5.

15 Peter Swire and Kenesa Ahmad "'Going Dark' Versus a Golden Age of Surveillance" (28 November 2011) Center for Democracy & Technology <www.cdt.org>.

and intelligence agencies.[16] In doing so, states "have sought to limit the advance of terrorism but, in the process, also created enormous challenges for (transnational) constitutionalism".[17]

There have also been massive advances in digital communications technologies, and their democratisation through smartphones. As of January 2017, over half of the world's population uses a smartphone and half of all Internet traffic was through mobile devices.[18] Mobile users are increasingly transitioning from traditional voice calls and text messages to Voice over Internet Protocol services such as Skype and FaceTime, as well as online messaging applications.[19] The latter are called Over The Top (OTT) services. This is because they operate over Internet networks, but independently of and outside the network provider's control and distribution.[20]

The ubiquity of these smart technologies has greatly enhanced governments' capacity to monitor users and collect data about their behaviours. As a result, the practical barriers to global and mass surveillance have broken down. The United Nations High Commissioner for Human Rights concludes: "the technological platforms upon which global political, economic and social life are increasingly reliant are not only vulnerable to mass surveillance, they may actually facilitate it".[21] The ramifications of this were revealed in 2013 when former National Security Agency contractor Edward Snowden exposed mass surveillance by the United States and its Five Eyes partners to *The Guardian*.[22] The revelations uncovered governmental mass surveillance as "a dangerous habit rather than an exceptional measure".[23] They worked to show the vulnerability of digital communications technologies to electronic surveillance, as well as how permissive laws and secret operations allowed mass surveillance to occur without adequate scrutiny. This "sparked a global conversation about the balance between liberty and security in the digital era".[24]

Numerous scholars have lamented that government surveillance, often in the name of counter-terrorism, has justified severe breaches of human

16 Federico Fabbrini "Privacy and National Security in the Digital Age: European and Comparative Constitutional Perspectives" (2015) 20 TLR 5 at 6. See, for example, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 Pub L No 107-56, § 215, 115 Stat 272 at 287 (2001); Directive 2006/24/EC on Data Retention [2006] OJ L105/54; and Telecommunications (Interception and Access) Act 1979 (Cth).

17 Konrad Lachmayer and Normann Witzleb "The Challenge to Privacy From Ever Increasing State Surveillance: A Comparative Perspective" (2014) 37 UNSWLJ 748 at 748.

18 Simon Kemp "Digital in 2017: Global Overview" (24 January 2017) We Are Social <www.wearesocial.com>.

19 Kemp, above n 18.

20 See Commerce Commission *Annual Telecommunications Monitoring Report 2017* (December 2017) at 30.

21 *The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights* A/HRC/27/37 (30 June 2014) at [2].

22 See, for example, Glenn Greenwald "NSA collecting phone records of millions of Verizon customers daily" *The Guardian* (online ed, London, 6 June 2013).

23 *The Right to Privacy in the Digital Age*, above n 21, at [3].

24 Fabbrini, above n 16, at 9.

rights.[25] Most poetically, James Colraine has argued that "[w]hile encryption can empower terrorists in a way that threatens the physical safety of the body politic in a democratic society, unfettered government surveillance can threaten its soul."[26]

Privacy is the primary right that is infringed by surveillance. This fundamental human right is enshrined in international covenants,[27] as well as domestic constitutional[28] and case law.[29] However, other rights, such as freedom of expression and association and the right to family life are also invoked when governments intercept communications.[30] Each of these rights arguably forms the basis for a free and democratic society.[31] They ensure that people have the liberty to hold, express and act on their identity and opinions, even when they diverge from social norms or the will of the state. Commentators are concerned that mass surveillance in particular creates a "chilling effect" on free expression and association, as well as invading privacy.[32] However, the state also has a duty to protect its citizens from criminal and terrorist threats.[33] Persons have a right to life, liberty and security.[34] Therefore individual rights, such as privacy, can be limited by law to ensure competing rights (such as security) are upheld. Governments contemplated the proverbial balance striking between privacy and security following the Snowden revelations.

Since 2013, reviews into state surveillance have taken place in Australia,[35] the United States[36] and the United Kingdom.[37] These have resulted in decisions to both restrict and expand state surveillance powers. For example, in the United States, legislation was passed purporting to end drag-net collection of communications metadata by the National Security Agency.[38] However, in the United Kingdom, the Investigatory Powers Act 2016 (UK), nicknamed the "snooper's charter", expanded surveillance powers to such a

25 At 8; *The Right to Privacy in the Digital Age,* above n 21, at [3]; and Lachmayer and Witzleb, above n 17, at 773.

26 James Colraine "Encrypted Messaging Apps in the Age of Terrorism and Snowden: Savior or Safe Haven" (MA Thesis, Georgetown University, 2016) at 10.

27 *Universal Declaration of Human Rights* GA Res 217A, A/Res/3/217A (1948), art 12; and International Covenant on Civil and Political Rights 999 UNTS 171 (opened for signature 16 December 1966, entered into force 23 March 1976) [ICCPR], art 17.

28 Basic Law for the Federal Republic of Germany 1949, arts 10 and 13.

29 *Hosking v Runting* [2005] 1 NZLR 1 (CA); and *Katz v United States* 389 US 347 (1967).

30 *The Right to Privacy in the Digital Age*, above n 21, at [14].

31 *Necessary & Proportionate Principles*, above n 1, at 2.

32 Paul Anderson "Fighting 'Terrorism', Repressing Democracy: Surveillance and Resistance in the UK" (Legal Studies Research Paper No 2016/1, University of Warwick, May 2016) at 6–7.

33 *General Comment No 35 on Article 9 (Liberty and security of person)* CCPR/C/GC/35 (16 December 2014) at [7].

34 ICCPR, art 9.

35 See Parliamentary Joint Committee on Intelligence and Security *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation* (May 2013).

36 See Richard Clarke and others *Liberty and Security in a Changing World* (The President's Review Group on Intelligence and Communications Technologies, 12 December 2013).

37 See Intelligence and Security Committee of Parliament (UK) *Privacy and Security: A modern and transparent legal framework* (March 2015); and David Anderson *A Question of Trust: Report of the Investigatory Powers Review* (Independent Reviewer of Terrorism Legislation, June 2015).

38 Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 Pub L No 114-23, §§ 103, 201 and 501, 129 Stat 268 at 272, 277 and 282.

degree that privacy advocates warn it will "provide an international standard to authoritarian regimes around the world".[39]

Here, we return to the 'going dark' issue. Four years on from the first Snowden leaks, increasingly native encryption and E2EE — itself a reaction to those leaks[40] — has reinvigorated state calls to strengthen surveillance powers. The issue is whether these calls are justified.

Along with Swire and Ahmad, several others also reject the 'going dark' narrative.[41] They argue that the huge advances in technology, and the scale and rate of their uptake, outweigh any loss of access to information due to encryption. Most security and law enforcement agencies can already compel a substantial range of useful information, including location data, call-associated data and digital dossiers: personal information held by private and government institutions.[42] This metadata can disclose as much, if not more, "detail than would be discernible from the content of communications".[43] The "digital exhaust" we emit as we move with our devices in the world is only growing.[44] Scholars also cite the unlikelihood of encryption becoming ubiquitously adopted when most communications businesses "rely on access to user data for revenue streams and product functionality".[45] The growth of the unencrypted "Internet of Things",[46] and the impracticality, inconvenience and fallibility of implementing encryption for some communication channels are reasons we are unlikely to 'go dark' at all.[47]

In light of this arguable Golden Age, we must challenge government calls for wider surveillance powers on the grounds that current channels are 'going dark'. This is particularly pertinent when the Executive increasingly dominates decision-making. The state holds the power to define, determine and review a threat and an appropriate response when it frames issues in terms of *privacy versus security* and *national security*.[48] In an atmosphere of fear and urgency, governments can monopolise decision-making and cash in on the "semantic fog" that surrounds the concepts of 'national security' and 'threat'.[49] They can both define those concepts and justify a dramatic expansion of executive power.[50]

This is not to say that there is no legitimate threat to public safety. Numerous terror attacks in the West have harmed innocent people, and future attacks no doubt loom in the minds of the public and lawmakers. Interrogation

---

39 Alan Travis "'Snooper's charter' bill becomes law, extending UK state surveillance" *The Guardian* (online ed, London, 29 November 2016).
40 See, for example, Sanger, above n 13.
41 Matthias Schulze "Clipper Meets Apple vs FBI—A Comparison of the Cryptography Discourses from 1993 and 2016" (2017) 5 Media and Communication 54 at 59; and Zittrain, above n 11, at 2–3.
42 Swire and Ahmad, above n 15.
43 *Necessary & Proportionate Principles*, above n 1, at 3.
44 Schulze, above n 41, at 59.
45 Zittrain, above n 11, at 3.
46 At 3.
47 Schulze, above n 41, at 59.
48 Anderson, above n 32, at 3–4.
49 At 3.
50 At 3–4.

is required about whether governments are acting democratically when defining unspecified threats, and what forms necessary and proportionate responses.[51] At present, it is being done without sufficient engagement with the public to define what the public good is and how to secure it.[52]

New Zealand Context

Within this global context, New Zealand reviewed and reformed its own intelligence and security regime for communications interception with the Government Communications Security Bureau Act 2003 and the Telecommunications (Interception Capability) Act 2004. This section is concerned with the 2013 changes to both Acts and the 2016 review of New Zealand's intelligence and security laws that resulted in the ISA.

While the Snowden revelations did have an influence on reform,[53] the catalyst was the report by Rebecca Kitteridge (Kitteridge Report),[54] an earlier review of the GCSB's compliance mechanisms.[55] Prior to becoming NZSIS Director,[56] Cabinet Secretary Kitteridge was seconded to the GCSB in October 2012 to review the GCSB's compliance with the Government Communications Security Bureau Act. This followed an admission by the Government that the GCSB had unlawfully intercepted Kim Dotcom's communications.[57] Under s 14(1) of the Government Communications Security Bureau Act, the GSCB was not permitted to take any action "for the purpose of intercepting the private communications of a person who is a New Zealand citizen or a permanent resident". Mr Dotcom, a permanent resident, had been charged with money laundering and piracy in the United States in association with his Megaupload business. He was subject to extradition. The GCSB had intercepted his communications on behalf of the NZSIS in its investigation of Mr Dotcom. This spying was widely reported in the New Zealand media and prompted the Kitteridge Report.[58]

Ms Kitteridge found that the GCSB had assisted the NZSIS and New Zealand Police in intercepting the communications of 88 individuals between 1 April 2003 and 26 September 2012.[59] The GCSB was barred from intercepting domestic communications. However, the GCSB's justification was that it was acting on behalf of the NZSIS and New Zealand Police, who

51 At 3.
52 At 3.
53 Michael Cullen and Patsy Reddy *Intelligence and Security in a Free Society: Report of the First Independent Review of Intelligence and Security in New Zealand* (G24a, 29 February 2016) at [1.40].
54 Rebecca Kitteridge *Review of Compliance at the Government Communications Security Bureau* (March 2013).
55 Human Rights Commission *Protection of Fundamental Freedoms in the Digital Age* (paper presented to the United Nations Human Rights Committee, 20 June 2014) at [1].
56 "Director-General's biography" New Zealand Security Intelligence Service <www.nzsis.govt.nz>.
57 "Dotcom: Illegal spying revealed" *The New Zealand Herald* (online ed, Auckland, 24 September 2012).
58 See, for example, Andrea Vance "GCSB acted illegally on Kim Dotcom" *Stuff* (online ed, New Zealand, 29 August 2013); and "Key & Dotcom - the story so far" *Radio New Zealand* (New Zealand, 16 September 2014).
59 Kitteridge, above n 54, at [5].

were authorised to intercept communications. The GCSB acted in this "grey area" on internal legal advice that their actions were lawful.[60]

In response to the Kitteridge Report, the Government passed the Government Communications Security Bureau Amendment Act 2013 under urgency. The new s 8C authorised the GCSB to intercept New Zealanders' communications when assisting the NZSIS, New Zealand Police or New Zealand Defence Force.[61] This prospectively made legal the kind of spying that was unlawful in the Dotcom case. In addition, s 8A authorised the GCSB to spy on New Zealanders when performing its cyber security function. Section 14 was amended to prohibit domestic spying only in relation to intelligence gathering and analysis.

The Bill faced considerable opposition from the New Zealand Law Society and the Human Rights Commission,[62] as well as media criticism.[63] The New Zealand Law Society raised concerns about the Bill's intrusive powers in relation to New Zealanders.[64] It argued they were inconsistent with the rights to freedom of expression, freedom from unreasonable search and seizure, and the right to privacy.[65] The Law Society also criticised the failure to define threats faced to justify expansion of powers beyond generalisations such as "a changing security environment";[66] using Parliamentary urgency;[67] and the consequent lack of public debate.[68] These concerns were exacerbated by New Zealand's membership in the Five Eyes network and the potential for sharing domestic intelligence with the National Security Agency.[69]

At the same time, the government passed the TICSA to replace the earlier Telecommunications (Interception Capability) Act 2004. The TICSA imposes obligations on network operators, such as Vodafone and Spark, to ensure that their networks are "interception capable" and to assist intelligence agencies with executing interception warrants.[70] One of the Act's key motivations was to clarify that the duty to assist extends to overseas service providers,[71] and it includes the obligation to decrypt content.[72] Another

60 At [23]–[26]; and Andrea Vance and Tracy Watkins "Illegal spying: 85 Kiwis watched" *Stuff* (online ed, New Zealand, 9 April 2013).
61 Government Communications Security Bureau Act 2003, s 8C.
62 New Zealand Law Society "Submission to the Intelligence and Security Committee on the Government Communications Security Bureau and Related Legislation Amendment Bill" (14 June 2013); and Human Rights Commission *Report to the Prime Minister: Government Communications Security Bureau and Related Legislation Amendment Bill; Telecommunications (Interception Capability and Security) Bill, and Associated Wider Issues Relating to Surveillance and the Human Rights of People in New Zealand* (9 July 2013).
63 Andrea Vance "Demystifying the GCSB bill: Spies and lies" *Stuff* (online ed, New Zealand, 20 August 2013).
64 New Zealand Law Society, above n 62, at [9].
65 At [9].
66 At [13]–[15].
67 At [4].
68 At [5].
69 Vance, above n 63.
70 Telecommunications (Interception Capability and Security) Act 2013 [TICSA], ss 9–14 and 24.
71 Telecommunications (Interception Capability and Security) Bill 2013 (108-1) (explanatory note) [TICS Bill explanatory note] at 2.
72 Ministry of Business, Innovation & Employment [MBIE] *Technical Paper: Telecommunications Interception Capability and Network Security* (December 2012) at [89]–[99].

motivation was to ensure that obligations were sufficiently flexible to meet current operational needs and technological developments.[73] In practice, that means the TICSA extends a higher level of duties to service providers and smaller operators through Ministerial "deem-in" powers.[74] These powers were highly criticised during the legislative process. One commentator argued that they provide "sweeping new powers to widen the net" of interception capable services "at the stroke of a pen and without due oversight".[75] However, the government framed the Act as a clarification rather than an extension of interception powers.[76]

Three years after these changes, former Deputy Prime Minister the Hon Sir Michael Cullen and soon-to-be Governor-General Dame Patsy Reddy released the first Independent Review of Intelligence and Security in New Zealand.[77] In proposing comprehensive legislative reform, Cullen and Reddy were concerned with the "need to maintain both security and the rights and liberties of New Zealanders".[78] In practice, Cullen and Reddy prioritised surveillance. They considered violent extremism and radicalisation a real threat that required domestic surveillance for intelligence purposes.[79]

Cullen and Reddy recommended that the New Zealand Security and Intelligence Act 1969 and Government Communications Security Bureau Act be consolidated into one intelligence and security Act.[80] The New Zealand Intelligence and Security Bill 2016 adopted the majority of Cullen and Reddy's recommendations and echoed their reasoning.[81] It aimed to improve transparency and oversight of the agencies, and to reflect a long-standing commitment to human rights, democracy and accountability. It also tried to ensure that the law was adaptable to changing circumstances and technology,[82] and that intelligence agencies could operate in "an increasingly complex security environment, where [they] are confronted by growing numbers of cyber threats and the rise of terrorist groups".[83]

One key change in the ISA is a new authorisation scheme that extends intelligence surveillance to New Zealand citizens. Agencies may obtain a Type 1 warrant to intercept the communications of a New Zealander to protect "national security" or contribute to New Zealand's "well-being".[84] This further widens the grounds for domestic surveillance allowed by the 2013 amendment[85] and removes the previous s 14 prohibition on domestic

73 TICS Bill explanatory note, above n 71, at 1; and MBIE *Technical Paper*, above n 72, at [31(b)–(e)], [34] and [29(c)].
74 MBIE *Regulatory Impact Statement: Telecommunications industry — Updating interception capability obligations* (12 March 2013) at [52], [57] and [63]; and TICSA, ss 19 and 38.
75 Adam Bennett "Spying on NZ: Law widens net for snooping" *The New Zealand Herald* (online ed, Auckland, 25 June 2013).
76 MBIE *Regulatory Impact Statement*, above n 74, at [68].
77 Cullen and Reddy, above n 53.
78 At [4].
79 At [1.19], [1.33], and [1.57].
80 At [25] and [4.13]–[4.18].
81 New Zealand Intelligence and Security Bill 2016 (158-1) (explanatory note) at 1.
82 At 1–3.
83 John Key "Intelligence and Security legislation introduced" (press release, 16 August 2016).
84 Intelligence and Security Act 2017 [ISA], ss 53 and 58–59.
85 Government Communications Security Bureau Amendment Act 2013.

intelligence surveillance.[86] However, while the ISA provides clarity about the extent of domestic spying, it does not justify why these powers are necessary or quell concerns about broad powers ordering surveillance on arguably vague grounds. It purports to strike the appropriate balance between human rights and security, but as the Green Party criticises, it does so "with the effect of eroding the freedom and openness of society, in the name of security".[87]

Conclusion

Islamic terrorism in Western public consciousness has collided with rapid technological change to produce a political environment where the desire for expansive surveillance powers are tenable and welcomed.[88] Despite the Snowden revelations, the narrative that intelligence and security agencies will soon be 'in the dark' due to encryption has driven further reforms. Throughout these changes, governments have dominated the power to define, determine and review threats and their legislative responses. New Zealand is not immune to this trend. Successive governments have incrementally expanded surveillance powers. The remainder of this article gives an overview of the law — the TICSA and the ISA — and analyses whether the criticisms in this section are justified according to the *Necessary & Proportionate Principles*.

III THE LAW

The ISA is the framework for authorising otherwise unlawful interception. Key features to note are:

1. *The decision-maker*. Applications for Type 1 warrants must be made to the "authorising Minister" (the Minister responsible for the agency making the application)[89] and the Chief Commissioner of Intelligence Warrants (a former High Court judge, appointed by the Governor-General on the recommendation of the Prime Minister).[90] Applications for Type 2 warrants are made to the authorising Minister alone.[91]
2. *The decision-making process*. The formal requirements for an application are set out in s 55. Urgent applications may be made orally or by personal appearance.[92] Safeguards for urgent applications include, for example, requiring the Minister to record their reasons for issuing the warrant,[93]and automatically revoking the warrant after 48

86 Government Communications Security Bureau Act, s 14.
87 New Zealand Intelligence and Security Bill 2016 (158-2) (select committee report) at 13.
88 Will Dahlgreen "Broad support for increased surveillance powers" (18 January 2015) YouGov UK <https://yougov.co.uk>.
89 ISA, s 47.
90 Sections 55 and 112–113.
91 Section 55.
92 Sections 71(2) and 72(2).
93 Section 73.

hours.[94] Very urgent authorisations "must be referred as soon as practicable after it is given to the Inspector-General for review".[95]

3. *The standards and concepts by which decision-makers make their decisions*. Both Type 1 and Type 2 warrants may be issued for two purposes. They may be issued to "contribute to the protection of national security" against certain harms.[96] The harms are as set out in s 58(2) and include, for example, terrorism or espionage. Alternatively, they may also be issued to contribute to the international relations or economic wellbeing of New Zealand.[97]
4. *The substantive obligations those decisions impose*. Section 67 sets out a non-exhaustive list of activities authorised by a warrant, including, for example, conducting surveillance and intercepting private communications. Sections 68 and 68 set out the powers of the NZSIS and the GCSB, respectively, that are necessary to carry out those activities.

These features will be further analysed in Part IV.

The TICSA is the framework of obligations imposed on the telecommunications industry to enable authorisations under the ISA to be carried out effectively.[98] Key features to note are:

1. *The decision-maker*. The Minister of Communications is the sole decision-maker regarding the deem-in provisions.
2. *The decision-making process*. The Minister of Communications may, on application of a surveillance agency, deem a service provider or network operator subject to higher level duties. The agency must give reasonable notice to the affected network provider.[99] The Minister will then consult with the Ministers for the GCSB and NZIS.[100] If the Minister is satisfied on reasonable grounds that the direction is necessary for national security or law enforcement, the Minister may issue the direction.[101] The affected service provider may request a review of the Minister's decision.[102]
3. *The standards and concepts by which decision-makers make their decisions*. There are three matters that the Minister must take into account. These are: first, "whether the current level of interception capability on the affected network or service adversely affects national security or law enforcement", secondly, the cost of compliance on the network provider, and thirdly, "whether the new duties would unreasonably impair the provision of telecommunications services in New Zealand".[103]

94 Sections 74 –75.
95 Section 82. See also s 78.
96 Sections 58(1)(a) and 60(3)(a).
97 Sections 59(2)(a) and 60(3)(a).
98 TICSA, s 5(a).
99 Sections 19 and 38.
100 Sections 19(2) and 38(5)
101 Sections 19(1) and 38(6).
102 Section 39.
103 Sections 18(3)–18(4) and 38(7)–38(8).

4. *The substantive obligations those decisions impose*. Large network operators are obliged to have full interception capability.[104] Small network operators (those with fewer than 4,000 customers) need only be "intercept ready at all times".[105] A lower obligation is imposed on wholesale network service providers, who must be "intercept accessible".[106] Small network operators and wholesale network service providers also have a duty to assist when presented with a warrant or other authority.[107]

These key features will be analysed in Part IV.

IV ANALYSING THE LAW

This Part analyses the TICSA and the ISA for compliance with international best practice principles for communications surveillance. The first section introduces the *Necessary & Proportionate Principles* and proposes a series of questions to analyse the law based on those Principles. The subsequent sections answer these questions in turn, and find that both Acts fail to comply with the Principles in many aspects. The final section concludes that the New Zealand legislation creates unreasonable limits on basic freedoms.

Analytical Framework: the *Necessary & Proportionate Principles*

This article adopts the 13 *Necessary & Proportionate Principles* as a framework to assess the law.[108] The Principles were designed by privacy and security experts,[109] and have been signed by over 400 organisations, academics and politicians.[110] Their purpose is "to evaluate whether current or proposed surveillance laws … are compatible with human rights".[111]

This Part draws on nine of the 13 Principles to structure its analysis and argument. These are: legality; legitimate aim; competent judicial authority; necessity and proportionality; due process and user notification, transparency; and the integrity of communications systems. These Principles are usefully phrased as questions when evaluating the law.

The overall question is one of legality: are any limitations to human rights provided for by law?[112] This is more than a positive requirement that Parliament passes the legislation. Rather, it requires a twofold substantive

104 Sections 9 and 10.
105 Sections 11(1) and 13(2).
106 Sections 12 and 15.
107 Section 24.
108 *Necessary & Proportionate Principles*, above n 1.
109 At 1.
110 "Sign the 13 Principles" Necessary & Proportionate <www.necessaryandproportionate.org>.
111 *Necessary & Proportionate Principles*, above n 1, at 2.
112 See Convention for the Protection of Human Rights and Fundamental Freedoms 213 UNTS 221 (opened for signature 4 November 1950, entered into force 3 September 1953), arts 9–11; and ICCPR, arts 12, 17–19 and 21. In New Zealand, s 5 of the New Zealand Bill of Rights Act 1990 states that the rights and freedoms in the Act are "subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society".

interrogation. First, does the law meet minimum standards of clarity, accessibility and predictability? Secondly, does the law ensure freedom from arbitrary interference?[113]

Numerous subsidiary principles and questions are nestled within the wider question of legality. Does the law limit human rights with the view of achieving a legitimate aim? If so, is the response both necessary and proportionate in the circumstances? Are decisions regarding interception delegated to an independent and competent judicial authority? Does that authority give respect to due process? Is the state transparent about the number, type and consequences of interception requests, so the public is able to comprehend the scope, nature and application of the law? And, finally, what are the consequences of the law for the integrity of communications systems and the public's ability to communicate privately and securely?

This Part argues that despite intentions to respect rights and freedoms and protect New Zealand as a free and democratic society, in general the legislative framework fails to meet the high standards set by the Principles.[114]

Legitimate Aim

This section introduces the legitimate aim Principle, and discusses why the TICSA and the ISA fail to comply with both elements of the Principle. The elements of the Principles are: first, a proven threat to the nation that justifies surveillance; and secondly, unambiguous definitions of the proven threat and aims of surveillance, for example, terrorism or national security.

1 Definition

The law should only permit surveillance that achieves a legitimate aim. This should correspond to an important and necessary interest in democratic society; [115] for example, the protection of national security and the advancement of economic well-being.[116] At least under European human rights law, this principle is rarely deliberated because concepts like national security are regarded as prima facie legitimate aims.[117]

However, the *Necessary & Proportionate Principles* framework requires a higher standard. The authors of the Principles argue that "'vague and unspecified' notions of 'national security' in particular [have] been unduly used to justify interception and access to communications without

113 See Necessary & Proportionate *International Principles on the Application of Human Rights Law to Communications Surveillance: Background and Supporting International Legal Analysis* (Electronic Frontier Foundation and Article 19, May 2014) [*Background Analysis*] at 16–18.

114 Cullen and Reddy, above n 53, at [1.5]–[1.7]; and ISA, s 3.

115 *Necessary & Proportionate Principles*, above n 1, at 7.

116 See, for example, Convention for the Protection of Human Rights and Fundamental Freedoms, above n 112, art 8.

117 *Klass v Germany* (1978) 2 EHRR 214 (ECHR) at [46]–[50]; and *The Right to Privacy in the Digital Age,* above n 21, at [24].

adequate safeguards".[118] The Principles' legitimate aim requirement counters this problem. Compliant law must be justified and have specific aims. First, it must respond to a concrete threat to an important, legally protected interest; for example, the "life, limb or liberty of a person" or "public goods, the endangering of which threatens the very bases or existence of the state".[119] In practice, this requires the legislature to prove a tangible threat to the nation or its people that justifies a legislative response. Secondly, it must provide unambiguous parameters for surveillance by including clear definitions of the threat, the interests it imperils and the aim. These two limbs are considered in turn.

2 Unproven Case for Expanding Powers

Did the Executive prove the need to expand surveillance powers when enacting the TICSA and the ISA? For both Acts, opposition parties and submitters questioned the lack of a tangible basis for expanding interception powers.[120] When enacting the TICSA, the Government cited the importance of using communications surveillance to maintain "national security" in a changing digital environment.[121] Similar claims of "an increasingly complex security environment" with "growing numbers of cyber threats and the rise of terrorist groups" were used to justify greater interception powers in the ISA.[122] The GCSB's inability to intercept the communications of a New Zealand hostage victim or Islamic State recruit was specifically cited as reason to expand spying to New Zealanders for intelligence purposes.[123] However, the number of times such situations had arisen, if any, was not substantiated. Similarly, no prosecutions or arrests were made following the GCSB's illegal spying on 88 New Zealanders prior to 2012.[124] Without such evidence, the case of a real threat to New Zealanders is not met.

The response to this failure to provide evidence is that "New Zealand does face a range of threats … [but they are] not disclosed to the public for a variety of reasons".[125] Intelligence's value lies in its secrecy. There are two problems with this argument. One practical, the other ideological. First, governments can provide aggregate data while keeping content confidential.

---

118 *Background Analysis*, above n 113, at 21. See also *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue* A/HRC/23/40 (2013) at [58].

119 *Background Analysis*, above n 113, at 22.

120 For TICSA, see Mega Ltd "Submission to the Law and Order Committee on the Telecommunications (Interception Capability and Security) Bill 2013"; Google New Zealand Ltd "Supplemental Submission to the Law and Order Committee on the Telecommunications (Interception Capability and Security) Bill" (12 July 2013) at [1.9]–[1.11]; and (8 May 2013) 689 NZPD 9697, 9700–9701 and 9704–9705. For ISA, see New Zealand Intelligence and Security Bill 2016 (158-2) (select committee report) at 13–15; InternetNZ *Intelligence and Security in a Free Society: An InternetNZ briefing* (9 March 2016) at 7; and (18 August 2016) 716 NZPD 13039.

121 See MBIE *Technical Paper,* above n 72, at [2] and [68]; and (8 May 2013) 689 NZDP 9694.

122 Key, above n 83; Cullen and Reddy, above n 53, at [1.33] and [1.57]; and (18 August 2016) 716 NZPD 13032–13033 and 13036.

123 Cullen and Reddy, above n 53, at [5.69]–[5.70].

124 Vance, above n 63.

125 Cullen and Reddy, above n 53, at [1.33].

Secondly, the public and the House of Representatives cannot deliberate for themselves when they are not informed of the true scale and nature of the purported threat. This is contrary to any "nominally democratic social contract" whereby "the right to define the public good and threats to it, the right to deliberate and determine laws including those which address threats, and the right to adequately review both" remains with the people.[126]

Cullen and Reddy's report argue that the balance between privacy and surveillance should reflect national values.[127] Recent surveys show that 63 per cent of New Zealanders oppose government surveillance of their Internet and phone use.[128] 48 per cent believe New Zealand faces minimal or no risk from terrorism, cyberattacks and espionage.[129] These figures suggest that the public may not favour extensive domestic spying laws. However, if tangible threats were openly discussed, New Zealanders might desire greater surveillance powers. The issue is that the government did not provide evidence or give the public the opportunity to deliberate the appropriate balance. Thus, the TICSA and the ISA fail to comply with the first limb of the legitimate aim Principle.

3 Ambiguous Aims and Parameters

The TICSA and the ISA contain numerous aims: the protection of national security,[130] contributing to international relations and economic well-being,[131] and law enforcement.[132] Regardless of whether the legislation was justified, the important second question is whether these aims and the threats they face clearly define the parameters for communications surveillance.

(a) National Security: the ISA

The definition of "national security" in the ISA was a central issue during the legislative process, both for submitters[133] and during the Committee of the Whole House.[134] Initially, the Bill defined "national security" as protection against "threats, or potential threats, that may cause serious harm to the safety or quality of life of the New Zealand population".[135] The Select Committee replaced this definition with specified harms like terrorism or espionage that

126 Anderson, above n 32, at 19.
127 Cullen and Reddy, above n 53, at [1.5].
128 Amnesty International "New Zealanders part of global opposition to USA big brother mass surveillance" (18 March 2015) <www.amnesty.org.nz>.
129 Curia Market Research "Security Issues Poll" (October 2014) New Zealand Intelligence Community <www.nzic.govt.nz>.
130 ISA, s 58; and TICSA, ss 3(1), 19(1)(c) and 38(6)(c).
131 ISA, s 59.
132 TICSA, ss 3(1), 19(1)(c) and 38(1)(c).
133 See New Zealand Law Society "Submission to the Foreign Affairs, Defence and Trade Committee on the Intelligence and Security Bill" (11 October 2016) at [2.3]; Privacy Commissioner "Submission to the Foreign Affairs, Defence and Trade Committee on the New Zealand Intelligence and Security Bill 158-1" at [3.4]–[3.5]; and New Zealand Human Rights Commission "Submission to the Foreign Affairs, Defence and Trade Committee on the New Zealand Intelligence and Security Bill" at [27]–[28].
134 (15 March 2017) 720 NZPD 16716.
135 New Zealand Intelligence and Security Bill, s 5(c).

are now in s 58(2).[136] "National security" itself is not defined. It is to be determined by the Minister and Commissioner on a case-by-case basis in order to "be adaptive and responsive to a dynamic security environment".[137] Terrorism would threaten "national security" in almost all cases, but a serious crime would have to be extreme to constitute a threat to "national security".[138]

The Privacy Commissioner and Law Society both favoured the original approach.[139] The Law Society raised concerns that the enacted "definition" carries an "unacceptably high risk" that warrants will be issued without a genuine need to protect national security.[140] The Inspector-General of Intelligence and Security raised similar concerns, though recognised that the specified harms were useful from a transparency perspective.[141]

Both the original definition and the specified harms are required for the protection of national security to be a potentially legitimate aim. Even if both were present, the definitions struggle to comply with the Principle. The specified harms alone clearly expand the grounds that intelligence agencies can use to conduct surveillance for protecting national security. A departmental analysis released during the legislative process demonstrates that five out of six harms potentially or unlikely to be covered by the original definition would be covered by the current provision.[142] "National security" is admittedly "adaptive" and undefined.[143] This, combined with uncertainty about what amounts to a threat to "the operations of the Government of New Zealand", for example, fails to indicate adequately what might constitute a ground to spy on New Zealanders. Section 19 maintains some protection, including that the exercise of freedom of expression "does not of itself justify an intelligence and security agency taking any action".[144] However, one can envisage a range of dissenting parties being spied on for potentially threatening government infrastructure or operations in some way. In short, the definition of "national security" leaves the possibility for s 58 warrants to be used as a tool for political oppression. This is far from a legitimate aim.

(b) Undefined Aims

There are similar criticisms of "international relations and well-being" and "economic well-being" in the ISA, and "national security" in the TICSA.

136 ISA, s 58(2)(a)–(b).
137 (18 August 2016) 716 NZPD 13037.
138 John Beaglehole *New Zealand Intelligence and Security Bill: Further Advice on "National Security" Definition 13 December 2016 Meeting* (Department of the Prime Minister and Cabinet, Advice to Foreign Affairs, Defence and Trade Committee, 13 December 2016) at 2.
139 Privacy Commissioner, above n 133, at [3.4]–[3.5]; and New Zealand Law Society, above n 133, at [2.5]–[2.10].
140 At [2.5] and [2.9].
141 John Beaglehole *New Zealand Intelligence and Security Bill: Information Requests Arising from the Committee's 8 December 2016 Meeting* (Department of the Prime Minister and Cabinet, Advice to Foreign Affairs, Defence and Trade Committee, 12 December 2016) at 1.
142 *New Zealand Intelligence and Security Bill: Departmental Report to the Foreign Affairs, Defence and Trade Committee from the Department of Prime Minister and Cabinet* (December 2016) at 302–304.
143 (18 August 2016) 716 NZPD 13037.
144 ISA, s 58(2)(g)(ii).

Intelligence warrants may be issued under the ISA to contribute to international relations and well-being, and economic well-being.[145] While these seem to be noble goals, the terms are not defined and, as the Green Party argues, "can mean virtually anything".[146] The Human Rights Commission raised concerns that these aims may amount to:[147]

> … licence to direct [GCSB and SIS] functions towards monitoring the activities of groups or individuals who pose no national security risk but who hold legitimate views about economic, environmental or social policy that may be contrary or in opposition to the government's economic policy objectives.

Again, the legislation could permit politically motivated surveillance of New Zealanders without a sufficient security basis.

Furthermore, "national security" is defined in the TICSA in terms of economic well-being, which is undefined itself.[148] There are no public guidelines outlining what the Minister may regard as pertaining to national security. Effectively, one Minister decides what national security and economic well-being mean in order to impose large-scale decryption duties on international service providers. This uncertainty is a clear derogation from the second limb of the legitimate aim Principle.

Overall, the executive failed to prove the need for the powers in the ISA and the TICSA. It enacted definitions that provide substantial latitude to decision makers (often Ministers) to intercept communications where there is no real threat to life, limb or liberty of New Zealand or its people.

Necessary and Proportionate Response

This section defines the eponymous Principles of the analytical framework. It explains that while the ISA superficially recognises the importance of necessity and proportionality, in reality the legislation fails to comply with these requirements. The TICSA fails to recognise these Principles at all.

1 Definition

The Principle of necessity requires surveillance powers to be no more than "strictly and demonstrably necessary [in a free and democratic society] to achieve a legitimate aim".[149] Proportionality requires that surveillance's interference with human rights is relative to the legitimate aim it seeks to fulfil.[150] Communications surveillance is proportionate where there is a "high degree of probability that a serious crime or specific threat to a [l]egitimate [a]im has been or will be carried out"; it is highly likely that relevant evidence

145 Sections 59 and 60(3)(a)(ii).
146 New Zealand Intelligence and Security Bill 2016 (158-2) (select committee report) at 14.
147 New Zealand Human Rights Commission, above n 133, at [30].
148 TICSA, s 3(1).
149 *Necessary & Proportionate Principles*, above n 1, at 7.
150 At 8.

will be obtained from the surveillance; and "other less invasive techniques have been exhausted or would be futile".[151] Surveillance is disproportionate when techniques are used that undermine the essence of the right to privacy or other fundamental freedoms.[152] The last point is relevant to the decryption obligations in the TICSA, and will be discussed below.

2 Superficial Recognition: the ISA

ISA was enacted with the intention that exercise of surveillance powers be "necessary and proportionate".[153] While the Act purports to maintain these principles, it fails in substance.

(a) Necessity

Type 1 and 2 warrants for national security purposes, including their urgent versions, must be "necessary to contribute to the protection of national security".[154] As discussed above, however, "national security" arguably fails the legitimate aim test. This means authorisations cannot be "necessary to achieve a legitimate aim".[155] In addition, there is no requirement for the decision maker to show why the warrant is necessary.[156] However, it is more concerning that international relations and well-being authorisations fail even superficially to refer to necessity. They may be granted at a considerably lower threshold: merely to "contribute" to either of those aims.[157] This shortcoming compounds their failure at the legitimate aim hurdle. Section 61 of the ISA is applicable to all authorisations. It requires that surveillance is necessary for the performance of agencies' functions in ss 10–11, being "intelligence collection and analysis" and "protective security services, advice, and assistance", respectively.[158] However, functions are not legitimate aims. Rather, they check that the agencies are acting within the bounds of their designated functions. As such, they fail to meet the necessity requirement.

(b) Proportionality

Section 61 of the ISA requires that surveillance be "proportionate to the purpose for which it is to be carried out" and that "the purpose of the warrant cannot reasonably be achieved by a less intrusive means".[159] While the latter limb complies with the proportionality principle, the former is ineffective in

151 At 8.
152 At 8.
153 Cullen and Reddy, above n 53, at [12], [5.77] and [6.3]; and New Zealand Intelligence and Security Bill 2016 (158-1) (explanatory note) at 2.
154 ISA, ss 58(1)(a)(i), 60(3)(a)(i), 71(2)(b)(ii), 72(2)(b), 78(3)–(4), 71(2)(a)(b) and 72(2).
155 *Necessary & Proportionate Principles*, above n 1, at 7.
156 See ISA, s 66. However, note that under s 55(1)(c) the Director-General must set out why he or she believes the legal requirements for the warrant are met.
157 Sections 59(2) and 60(3)(a)(ii).
158 Sections 10–11 and 61(a).
159 Section 61(b)–(c).

substance. This is because the authorising sections do not require a high probability that a serious crime or threat to a legitimate aim has or will be carried out, nor a high probability that the interception will gather relevant evidence.[160] Section 58(1)(a)(ii), regarding national security, merely requires that the surveillance identify, enable the assessment of or protect against a specified harm. It does not even impose any requirement that the harm be more likely than not. Suspicion of harm appears to be sufficient. Section 59 more explicitly fails to meet the high probability threshold. It requires only "reasonable grounds to suspect" that a New Zealander is acting on behalf of a foreign government, organisation or terrorist entity.[161]

Type 2 warrants further breach the proportionality Principle. There is no imminence or probability threshold, nor a requirement that a specified harm be suspected.[162]

3 Total Failure: the TICSA

The key issue in the TICSA is whether it is necessary and proportionate to have powers to extend full interception capability obligations to service providers, and decryption obligations as a whole. These are discussed in turn.

(a) Deem-In Powers

The necessity and proportionality of Ministerial deem-in powers can be considered in two ways: first, including the powers in the legislation at all; secondly, in terms of their substantive scope and effect.[163]

In its Select Committee submission, Mega, an E2EE cloud computing provider, said the case for discretionary Ministerial powers to extend full interception obligations to service providers had not been proved. They argued that since the government does not know the size of the total "problem" (that is, the number of impugned messages sent via OTT services) it was unnecessary and disproportionate to include the Ministerial deem-in powers "'just in case' they are required in the future".[164] While it is a creative argument, the widespread use of OTT applications makes it untenable. Following a global trend in uptake of OTT services,[165] in 2013, 65 per cent of New Zealanders surveyed had used messaging applications, with 32 per cent using them daily.[166] Communications of interest will almost certainly be transmitted through service providers' applications. It is thus reasonable to say that deem-in powers are necessary to ensure impugned OTT networks are amenable to full obligations. The disproportionate harm of this ability,

160 Sections 58–60.
161 Section 59(2)(b)(i).
162 Section 60.
163 Sections 19 and 38.
164 Mega Ltd, above n 120, at 4.
165 Deloitte *Short messaging services versus instant messaging: value versus volume* (London, 2014).
166 Charles Crothers and others *Internet Trends in New Zealand 2007–2013* (Institute of Culture, Discourse & Communication, Auckland University of Technology, 2014) at 16.

however, and the integrity of the communications system is discussed later in this Part.

Given widespread OTT service use, the greater issue is that the TICSA does not require that including the service in the regime be necessary for national security or law enforcement, nor that deeming-in be proportionate. The standard is that the lack of interception capability "adversely [affects] national security or law enforcement".[167] This is a low threshold, as any instance of a suspicious communication being sent via an OTT service could be said to affect the aims adversely.[168] It is likely that certain communications would meet this threshold without interception being necessary, given the large digital exhausts available.

(b) Decryption Obligations

Decryption obligations are arguably unnecessary given the swathe of other data available to intelligence and security agencies. Under the TICSA, agencies can obtain call-associated data: the sending and receiving numbers, time, duration and location of communication.[169] In addition, intelligence warrants allow agencies to conduct human surveillance, use visual and tracking devices, photograph, make video and sound recordings, access and retrieve data from information infrastructures such as Wi-Fi networks, and "do any other act … reasonably required to achieve the purposes" of the warrant.[170] The benefits of decryption obligations are also highly disproportionate to the harm done because of how much they undermine the whole communications infrastructure. This will be discussed in detail below. In short, surveillance agencies' ability to access the content of OTT messages undermines the privacy and security of all messages on that service. Overall, neither Act requires interception to be necessary or proportionate.

Competent Judicial Authority Giving Effect to Due Process

This section defines and discusses two interrelated Principles. They concern the competency of the decision maker and the fairness of the decision-making process. This section determines that the Acts fail to comply with both Principles due to the primacy of Ministerial decision-making in both Acts, and the ex parte and limited review processes in the ISA and the TICSA, respectively.

167 TICSA, s 38(7)(a).
168 Mega Ltd, above n 120.
169 Sections 3(1), 10(1)(c) and 24(3)(b)(i).
170 ISA, ss 67–69.

1 Definition

A competent judicial authority acting in accordance with due process should make decisions about communications surveillance, such as the issuing of warrants. A competent judicial authority is a person or body:[171]

> … separate and independent from the authorities conducting Communications Surveillance; conversant in issues related to and competent to make judicial decisions about the legality of Communications Surveillance, the technologies used and human rights; and [has] adequate resources in exercising the functions assigned to them.

The Principles particularly warn against executive authorisation, as allowing "the same government ministers who are responsible for the activities of the intelligence services [to be] responsible for authorising interception warrants" is "hardly a credible safeguard against abuse".[172]

Due process also requires that authorisation be made "in a manner compatible with the fundamental rights of the affected individual", particularly the right to a fair and public hearing.[173] The Principles recognise that notification and a hearing may not always be possible, such as in an emergency where there is an imminent risk to human life. Nevertheless, they still require that any delay is authorised by a competent judicial authority, and that the target be notified after the fact so they have the opportunity to seek available remedies.[174]

Most models of surveillance authorisation are ex parte and run contrary to this standard. This is based on the view that the "very nature and logic of secret surveillance dictate[s] that not only the surveillance itself but also the accompanying review should be effected without the individual's knowledge".[175] This subversion of fair trial rights in favour of intelligence and security concerns is an unjustifiable position according to the Principles, unless notification would itself cause grave harm.

2 Incompetent Authorities

Both the ISA and the TICSA fail to comply with the competent judicial authority requirement because decision-making power is largely held by government Ministers.

(a) Token Judicial Authority: the ISA

Under the ISA, the Minister responsible for the relevant agency and a Commissioner of Intelligence Warrants authorise Type 1 warrants. Standard

171 *Necessary & Proportionate Principles*, above n 1, at 9.
172 *Background Analysis*, above n 113, at 26.
173 At 27.
174 At 9–10 and 27.
175 *Klass v Germany*, above n 117, at [55].

and urgent Type 2 warrants are issued by the Minister alone,[176] and urgent Type 1 warrants may be issued by the Minister alone at the Minister's discretion.[177] The Director-General of an agency may make very urgent Type 1 and 2 authorisations.[178] However, the Chief Commissioner and Inspector-General have oversight in urgent cases,[179] and the Chief Commissioner may revoke urgent warrants and very urgent authorisations.[180] The Inspector-General cannot unilaterally revoke an authorisation; they can only draw the Minister and Commissioner's attention to any irregularity.[181]

The most rigorous authorisation is thus only jointly authorised by a potentially competent judicial authority: a Commissioner. Commissioners are former High Court judges appointed on the advice of the Prime Minister in consultation with the Leader of the Opposition.[182] They are arguably more independent from surveillance agencies than the Minister, but still less than a sitting judge, and without the accountability provided by open courts. Prioritising Ministerial decision-making does not comply with the Principles and undermines any check that Commissioners may provide. The only conceivable function of Ministerial decision-making is to interpret "national security" more broadly than a Commissioner, or to exercise politically inclined judgment. This is the antithesis of competent judicial authority. The potential for both is contrary to the apparent goal sought by legislators: Ministerial awareness of and responsibility for the exercise of surveillance powers.[183] To give effect to this goal, the Minister could be briefed on the Commissioner's decisions and perform a non-binding review function akin to the Inspector-General.

Even if jointly authorised Type 1 warrants did comply with this Principle, the case for compliance collapses when responsibility falls to the Minister as urgency increases. To improve the law in this regard, the current position should be reversed, with urgent authority falling to a Commissioner (or even a sitting judge) and review by the Minister.

The inclusion of Commissioners of Intelligence Warrants is positive. However, the progressive reduction of their role for urgent and non-New Zealander warrants undermines the independence and robustness of the warranting process.

(b) All Power to the Minister: the TICSA

The TICSA breaches the competent judicial authority principle in starker ways. The Minister of Communications is the sole decision maker regarding the deem-in provisions. These extend higher-level interception duties to

176 Sections 60 and 72.
177 Section 71(2)(b).
178 Section 78.
179 Sections 73, 77, 82, 79(3) and 89(3).
180 Sections 72(3) and 82.
181 Section 163(1)(a).
182 Sections 112–113.
183 New Zealand Intelligence and Security Bill 2016 (158-2) (select committee report) at 4.

service providers, smaller network operators and wholesale and infrastructure level operators.[184] The Ministry of Business, Innovation & Employment (MBIE) explicitly noted that the Minister alone should have decision-making power because of the importance of non-public deliberation.[185] This is due to national security concerns. Understandably, several submitters and opposition parties were deeply concerned about the broad discretion of the Minister, and the lack of consultation and transparency within the deem-in process.[186]

3 Undue Process

The ISA does not have a provision for notifying affected individuals, nor any alternative mechanisms to ensure their views are represented.[187] The Privacy Bill does not change this position.[188]

Under the TICSA, operators and providers subject to a deem-in application must be notified and given a reasonable time to make submissions.[189] However, during the legislative process, the New Zealand Telecommunications Forum (NZTF) raised the concern that the opportunity to be heard is limited. This is because agencies have no obligation to state the grounds upon which they apply for the provider or operator to be deemed-in to higher obligations.[190] The result, NZTF argues, is that the Minister is "in the invidious position of having to consider a recommendation that has not had the benefit of full consultation and views from the impacted party".[191] These concerns have not been resolved in the enacted version.

In light of competent judicial authority and due process concerns, NZTF recommended that an intermediary independent panel advise the Minister.[192] This view was adopted by the Labour Party, but it did not eventuate.[193] Vodafone also recommended instituting a right of appeal to an independent tribunal.[194] Currently, there is no right of review or appeal for network operators deemed-in under s 19 of the TICSA. Service providers deemed-in under s 38 may seek an independent review by persons appointed by the Minister, but the finding is non-binding.[195] Although these are

184 TICSA, ss 19 and 38.

185 MBIE *Written advice on the submission from the Regulations Review committee requested 130807* (Advice to Law and Order Committee, 15 August 2013) at 2.

186 InternetNZ "Submisson to the Law and Order Committee on the Telecommunications (Interception Capability and Security) Bill" (13 June 2013) at [13]; Google New Zealand Ltd, above n 120, at 1 and [3.3]; New Zealand Telecommunications Forum "Submission to the Law and Order Committee on the Telecommunications (Interception Capability and Security) Bill 2013" at [25]; and (16 October 2013) 694 NZPD 13967–13971.

187 For an alternative model, see Public Interest Monitor Act 2011 (Vic).

188 See the exceptions in Privacy Bill, cls 52(1)(a)(i), 54(a), 60(4)(b) and 61(4)(b).

189 Sections 17(2) and 18(1).

190 New Zealand Telecommunications Forum, above n 186, at [26] and [29].

191 At [30].

192 At [33]–[34].

193 Supplementary Order Paper 2013 (370) Telecommunications (Interception Capability and Security) Bill 2013 (108-1).

194 Vodafone New Zealand Ltd "Submission to the Law and Order Committee on the Telecommunications (Interception Capability and Security) Bill" (13 June 2013) at [60].

195 TICSA, s 39.

improvements, decision-making would still ultimately lie with the Minister and be fundamentally incompatible with the competent judicial authority requirement.

Transparent Framework

This section considers the transparency Principle in two parts: transparency through data reporting and the transparency of Ministerial directions in the TICSA. Both Acts fail to report data against the Principles' standard sufficiently. In addition, the deem-in provisions in the TICSA provide for intentionally opaque directions about which providers are subject to which obligations.

1 Definition

The principle of transparency is twofold. First, states must:[196]

> … publish, at a minimum, aggregate information on the specific number of requests approved and rejected, a disaggregation of the requests by [agency], type, and purpose, and the specific number of individuals affected by each.

Secondly, states should provide enough information for individuals to comprehend fully the nature, scope and application of surveillance laws.[197] These are considered below.

2 Insufficient Data Reporting

In its 2016/2017 annual report, completed under the former legislation,[198] the GCSB reported that 33 interception warrants were in force and 26 were issued during the year.[199] The NZSIS, also under subsequently repealed legislation,[200] similarly reported that 53 domestic and 22 foreign intelligence warrants were in force for the 2016/2017 year.[201] The agencies do not report the number of individuals affected, the number of requests rejected, or any details about the purpose of each warrant beyond the NZSIS vaguely ensuring the security of New Zealand.

During the ISA's legislative process, the Privacy Commissioner was supportive of greater reporting. The Commissioner considered that aggregate data could be published to inform the public of the extent of intelligence powers without harming national security.[202] The ISA somewhat adopts this view by requiring both agencies to report the number of applications for

196 *Necessary & Proportionate Principles*, above n 1, at 10.
197 At 10.
198 Government Communications Security Bureau Act.
199 Government Communications Security Bureau *Annual Report 2017* (G35, 2017) at 11.
200 New Zealand Security Intelligence Service Act 1969.
201 New Zealand Security Intelligence Service *Annual Report 2017* (G35, 2017) at 34.
202 Privacy Commissioner, above n 133, at [2.6.10].

intelligence warrants, the type requested, the number approved and declined, and the number of authorisations given by the Director-General.[203] The agencies are not required to report on whether any urgent warrants or very urgent authorisations were revoked. However, the Inspector-General must report on his or her enquiries regarding urgent and very urgent authorisations.[204] This is an improvement compared to the former Acts but it still falls short of the Principles' standards. It does not require reporting, for example, of the number of individuals affected.

MBIE, governing the TICSA, does not report any data regarding network operator assistance to intelligence and security agencies.

3 Secret Ministerial Directions

This analysis has discussed several problematic factors of the Ministerial deem-in powers contained in the TICSA.[205] A further concern is that the form of the power — a Ministerial direction — has been chosen specifically to avoid public notification of affected providers.[206] Thus by intention and in effect, Ministerial directions under the TICSA secretly impose interception obligations on individual service providers or network operators.[207] Secret rules do not have the quality of law,[208] so they breach Principles of transparency and legality.

During the TICSA's legislative process, Facebook, Google and Microsoft argued that the extension of duties should fall to Parliament so that any changes are fully transparent and have the benefit of a scrutinising legislative process.[209] Perhaps these companies hoped that they would be excluded altogether, as Mega argued.[210] To ensure transparency and allow public scrutiny, a list of deemed-in providers should be publicised so the public has the opportunity to decide which services they use.[211]

Respect for the Integrity of Communications Systems

Finally, this Part examines what the New Zealand scheme, particularly the TICSA, means for the integrity of the communications networks and products

203 ISA, ss 221(2)(c)–(e).
204 Section 222.
205 Sections 19 and 38.
206 MBIE *Telecommunications Industry – Paper 2: Updating Interception Capability Obligations* (Paper to Cabinet Committee on Domestic and External Security Coordination, MBIE-MAKO-7109052, March 2013) at [109]; and MBIE *Technical Paper*, above n 72, at [104].
207 Vikram Kumar "Revealed: govt plans secret orders to service providers once spy bill becomes law" *The National Business Review* (online ed, Auckland, 18 August 2013).
208 *Malone v The United Kingdom* (1984) 7 EHRR 14 (ECHR) at [67]–[68].
209 Google New Zealand Ltd, above n 120, at [3.4]; Facebook Australia & New Zealand "Submission to the Law and Order Committee regarding the Telecommunications (Interception Capability and Security) Bill" (7 July 2012) at 4; and Microsoft New Zealand Ltd "Submission to the Law and Order Committee on the Telecommunications (Interception Capability and Security) Bill" (20 June 2013).
210 Mega Ltd, above n 120.
211 Tech Liberty "Submission to the Law and Order Committee on the Telecommunications (Interception Capability and Security) Bill 2013".

that New Zealanders use. Government-mandated back doors into communications networks allow the government to intercept communications when they consider it justified. However, this also compromises the security of communications against other actors, such as foreign governments and hackers. This section concludes that the decryption obligations in the TICSA undermine the security and privacy of communications systems and thus do not comply with this final Principle.

1 Definition

The Principles state that legislation should not compel communications providers to "build surveillance or monitoring capability into their systems".[212] To do so would undermine the system for all users. The position is summarised as follows:[213]

> Just as it would be unreasonable for governments to insist that all residents of houses should leave their doors unlocked just in case the police need to search a particular property … it is equally disproportionate for governments to interfere with the integrity of everyone's communications in order to facilitate its investigations …

The effects of this interference are not merely abstract. Encryption protects basic freedoms — the right to privacy and freedoms of association and expression — as well as being crucial for the security of online commerce and personal records held by banks and medical providers.[214]

2 Decryption as Destruction

The TICSA's decryption obligations undermine the integrity of New Zealand communications systems. The duty to have full interception capability includes decrypting a communication where the operator provided the encryption.[215] In the most basic case this would mean the operator holding a decryption key and using it to decrypt the communication for agencies, when called upon. This raises key security issues. A risk arises when Transport Layer Security and Secure Sockets Layer encryption is used.[216] The key may be taken and used by a hostile third party to decrypt retrospectively all communications sent using that key. Because of this vulnerability, many providers are moving towards "forward secrecy" forms of encryption, where a new key is generated at the start of each communication and destroyed at

212 *Necessary & Proportionate Principles,* above n 1, at 11.
213 *Background Analysis*, above n 113, at 33.
214 Mike McConnell, Michael Chertoff and William Lynn "Why the fear over ubiquitous data encryption is overblown" *The Washington Post* (online ed, Washington DC, 28 July 2015); and Susan Landau "The National-Security Needs for Ubiquitous Encryption" as cited in Zittrain and others, above n 11, at Appendix A.
215 Section 10(3).
216 For an explanation of Transport Layer Security and Secure Sockets Layer, see Holly Lynne McKinley *SSL and TLS: A Beginners' Guide* (SANS Institute, 2003).

the end of it, avoiding the retrospective decryption issue.[217] However, compelled decryption as used in the TICSA is incompatible with forward secrecy. If the provider cannot decrypt while the communication is occurring, it will be required to retain the key after the communication has ended in order to decrypt it. The retention of keys again raises issues of security, though it is on a smaller scale as the key relates to a particular communication. Key retention in order to comply with the TICSA duties leaves communications vulnerable to attack at varying scales.

Key security, however, was not the primary concern of submitters on the Telecommunications (Interception Capability and Security) Bill 2013. They were concerned about the effect of decryption duties on E2EE, an increasingly popular form.[218] With E2EE, while a service provider may enable encryption on their platform, and even automatically institute it, the users are the ones that hold the keys. The problem with this technology under the TICSA is that the duties to assist and to have full interception capability could impose decryption obligations on E2EE service providers. The basis is that they "provided the encryption", even though they do not hold the key and have no technical capability to do so.[219] Mega queried whether the legislation therefore compels services that allow E2EE to engineer back doors to break the encryption.[220] Tech Liberty, a New Zealand civil liberties group, commented that the "government's decision not to clarify this would seem to indicate that this is the intention".[221] If called upon under the duty to assist, providers may be able to argue that decryption in such circumstances is not reasonable assistance.[222] However, if deemed-in to full interception capability duties, the duty is strict. It is unclear whether MBIE would require back doors when administering the legislation. This approach is not novel for governments, as was seen in the Apple and Federal Bureau Investigation debate.[223]

If the legislation was interpreted in such a way as to compel the engineering of back doors into E2EE equipped systems, the effects would be negative and twofold. First, encryption would lose its privacy and security value. When compelling back doors, governments intend that only they will use those tools, and use them responsibly. However, even if one can trust governments in this regard, governments cannot ensure that back doors will never come into the hands of hostile third parties. This would compromise not only privacy but the physical, psychological and economic well-being of the

217 Nicole Perlroth and Vindu Goel "Twitter Toughening Its Security to Thwart Government Snoops" *The New York Times* (online ed, New York, 22 November 2013); and Harold Abelson and others "Keys under doormats: mandating insecurity by requiring government access to all data and communications" (2015) 1 Journal of Cybersecurity 69 at 74.

218 Tech Liberty, above n 211; Mega Ltd, above n 120; Microsoft New Zealand Ltd, above n 209; and Facebook Australia & New Zealand, above n 209, at 1.

219 TICSA, s 24(3)(vi).

220 Mega Ltd, above n 120.

221 Thomas Beagle "Changes to the TICS Bill" (16 October 2013) Tech Liberty NZ <www.techliberty.org.nz>.

222 Mega Ltd, above n 120.

223 See Schulze, above n 41.

state's citizens. The 2017 WannaCry attacks on the United Kingdom's National Health Service demonstrate this reality.[224] Secondly, and more generally, the obligations may create barriers to new and innovative technologies, contrary to the purpose of the TICSA.[225] This discourages truly secure communications services being offered in New Zealand and was a key concern for Facebook and Microsoft.[226] Microsoft highlighted that a requirement to decrypt content would put them and other American companies in conflict with United States privacy law — "an invidious position if they [were] forced to choose which country's laws to break, or discontinue a service".[227] In addition, providers may be reluctant to develop or provide new products in New Zealand if they could be subject to interception capability duties at short notice.[228]

Conclusion: Unjustifiable Limits in a Free and Democratic Society

When they were first proposed, the TICSA and the ISA were framed as progressive legislation, ensuring security while respecting human rights. They were supposed to: guarantee clarity and flexibility; "improve transparency and oversight arrangements to give the public greater confidence"; reflect "New Zealand's long-standing commitment to human rights, democracy, accountability, and the rule of law"; and ultimately "protect New Zealand as a free, open and democratic society".[229] The actual law presents a different view.

Contrary to the legality Principle, the TICSA and the ISA are not clear, accessible or predictable, nor do they ensure freedom from arbitrary interference. The basis for their existence is unsubstantiated. They are said to ensure the protection of New Zealand from internal and external threats, but what exactly those threats are and when a warrant may be issued is unclear. It is largely at the discretion of political decision makers. The measures for which they provide do not need to be necessary or proportionate. At best, mildly fettered government Ministers decide what is *necessary* to protect against malleable harms like threats to "the sovereignty of New Zealand".[230] There are few to no due process obligations and agencies are not required to say how many people are subject to surveillance. Finally, the obligations imposed on network operators (and potentially service providers through secret directives) undermine the security and privacy of a communications system that has increasingly native E2EE. This is a response itself to

224 Brad Smith "The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack" (14 May 2017) Microsoft <https://blogs.microsoft.com>.
225 Section 5(b).
226 Facebook Australia & New Zealand, above n 209, at 1; and Microsoft New Zealand Ltd, above n 209.
227 Microsoft New Zealand Ltd, above n 209.
228 Facebook Australia & New Zealand, above n 209, at 1; and Microsoft New Zealand Ltd, above n 209.
229 New Zealand Intelligence and Security Bill 2016 (158-1) (explanatory note) at 1–2; and TICS Bill explanatory note, above n 71, at 1–2.
230 ISA, s 58(2)(g)(iii).

revelations of earlier privacy invasions by governments. As a whole, non-compliance with these Principles is contrary to New Zealand's supposed commitment to human rights and protection of its free and democratic society. Rather, the Acts create unjustifiable limits on basic rights and freedoms.

V CONCLUSION

As the privacy and security debate continues among academics and social commentators, government legislative agendas and intelligence and security agencies carry on. The public carry on as well: texting, calling and e-mailing. A few days after New Zealanders went to the ballot box to elect their 52nd Parliament, the bulk of the ISA came into force without comment, either then or during the campaign.[231] The law governing New Zealand intelligence and security agency powers to intercept private communications is settled for now. Although it was debated briefly but fiercely during its inception and enactment, it now hums quietly in the background. This article, in the limited way it can, seeks to provide a record of the statutes' imperfections and, in doing so, a reason why they should not be forgotten.

Part II discussed the context for New Zealand's expansion of government surveillance powers. It highlighted key drivers and discourses globally, and how these manifested locally to produce the TICSA and the ISA. Part III outlined the law to ensure familiarity with the statutes being critiqued. Part IV introduced the analytical framework and systematically explained why the law is concerning in its breaches of basic human rights. Despite the purported good intentions of the Acts, they produce unjustifiable limits to rights of privacy, free speech and association in the free and democratic society New Zealand aspires to be.

231 Section 2.