Encryption laws and regulations in one of the Five Eyes: The case of New Zealand
by Michael Anthony C. Dizon and Philip James McHugh

Abstract

This article examines the laws that apply to encryption in New Zealand. Specifically, it analyses the different types of law that constitute an encryption legal framework in the country, namely: export control, substantive cybercrime, criminal procedure, human rights, and information security and data protection. The article then utilises the encryption laws and legal framework to evaluate a proposal by the Five Eyes intelligence alliance to regulate the use of end-to-end encryption in messaging services. The article concludes that the proposal is incompatible with the country's encryption legal framework.

1. The encryption dilemma

Encryption is a key technology in today's network information society. Many everyday activities depend on or involve encryption whether it is people using internet banking, shopping online, browsing the web, sending private messages, or protecting their electronic data and devices. Encryption is considered essential for information security and cybersecurity.[1] There is general consensus among many stakeholders, including government, that this technology is integral to safeguarding the security, privacy and other rights and interests of persons in a digitally connected environment.[2] The dilemma though is that the ability of encryption to provide secrecy and security of information and communications can become a significant threat or hindrance to public order and safety when it is used for illicit or criminal means and purposes. There have been many attempts and proposals to regulate encryption since the so-called Crypto Wars in the 1990s when the US Government unsuccessfully sought to formally enact new laws and regulation that prohibit or control the general development and distribution of encryption technology.[3] With the ever-increasing

---

[1] Jason Andress *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice* (Syngress Press 2011) 63.
[2] David Kaye, United Nations Human Rights Council, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (May 2015) 10; see also Wolfgang Shulz and Joris van Hoboken *Human Rights and encryption* (UNESCO 2016); see also 'International statement – End-to-end encryption and public safety' (12 October 2020) <https://www.beehive.govt.nz/release/international-statement-end-end-encryption-and-public-safety> accessed 12 November 2020.
[3] Simon Singh, *The Code Book: The Secret History of Codes and Codebreaking* (Fourth Estate 1999) 314; Steven Levy, *Crypto: How the Code Rebels Beat the Government – Saving Privacy in the Digital Age* (Viking 2001) 187.

ubiquity and embeddedness of computers, data and networks across the world today, proposals to regulate encryption have become more frequent as well. The Five Eyes intelligence alliance composed of Australia, Canada, New Zealand, the United Kingdom, and the United States have made joint international statements that call for stricter regulation of encryption, including greater cooperation from technology companies that develop and use encryption in their widely used products and services.[4] Recently, the Five Eyes alliance, together with India and Japan, released an international statement on end-to-end encryption where they called on technology companies to design or modify their encrypted messaging services to permit law enforcement to intercept and gain access to decrypted or plaintext copies of users' communications.[5] This proposal was opposed by technology companies, cybersecurity experts and civil society organisations.[6]

This and other government proposals to regulate encryption are often critiqued on the ground that governments do not appear to understand the technology of encryption or, despite having sufficient knowledge, persist in their instrumentalist approaches to regulating this technology.[7] Aside from this perceived lack of technical understanding, government attempts to regulate encryption can be further criticised for being seemingly oblivious or unaware of the fact that there are already existing laws that regulate encryption to a significant degree. Problematic, infeasible or misguided proposals to regulate encryption can be avoided if there is greater recognition of these laws that make up an overarching encryption legal framework.

---

[4] 'Five Country Ministerial 2017: Joint Communiqué' (27 June 2017) <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/fv-cntry-mnstrl-2017/index-en.aspx> accessed 30 May 2021.
[5] 'International statement – End-to-end encryption and public safety' (12 October 2020) <https://www.beehive.govt.nz/release/international-statement-end-end-encryption-and-public-safety> accessed 26 September 2021.
[6] 'CDT, GPD and Internet Society respond to new statement from Five Eyes alliance' <https://www.gp-digital.org/news/global-encryption-coalition-responds-to-new-statement-from-five-eyes/> accessed 30 May 2021; see also Aditi Agarawal, 'Backdoors To Encryption Are Bad, Civil Society Group Tells Five Eyes, India, Japan. Again' (*Medinama*, 14 October 2020) <http://www.medianama.com/2020/10/223-global-encryption-coalition-lambastes-for-encryption-backdoors/> accessed 30 May 2021.
[7] See 'New law would force Facebook and Google to give police access to encrypted messages' *The Guardian* (, 14 July 2017) <https://www.theguardian.com/technology/2017/jul/14/new-law-would-force-facebook-and-google-to-give-police-access-to-encrypted-messages> accessed 30 May 2021.

The principal aim of this article is to systematically set out and examine the existing laws and legal framework of encryption that already regulate the development, access to and use of encryption in New Zealand. Further, the article explains how this overarching encryption legal framework is based on well-established legal powers, procedures and rights. This means that any proposal to regulate encryption in general or specifically should be cognisant of or conform to this existing legal framework. Otherwise, the proposed regulation would either have to (a) overhaul all or a significant portion of the encryption laws and legal framework discussed below or (b) come into conflict with multifarious laws and potentially even breach the country's international obligations.

An examination of New Zealand law is significant because, as a member of the Five Eyes alliance, the country's laws and policies on encryption may potentially influence or reveal how the other members decide to regulate this technology. This article is also relevant in that not much has been written about encryption laws in New Zealand compared to the other Five Eyes countries. The article's description and explication of the applicable New Zealand laws can also be used as a basis to compare and contrast the encryption laws of the Five Eyes members. Further, a legal analysis of the proposed regulation of end-to-end encryption and whether or not it fits with New Zealand laws can provide useful insights for other jurisdictions as well.

The article's presentation and analysis proceed as follows. Part 2 provides a brief overview of technical elements of encryption. Parts 3 and 4 examine, respectively, the two general categories of law that apply to encryption: (1) substantive and procedural criminal and cybercrime laws and (2) human rights and cybersecurity laws. Part 3 focuses specifically on export control, substantive cybercrime, and criminal procedure laws, while Part 4 delves into the areas of human rights, information security, and data protection laws. In Part 5, the encryption legal framework is used as a standard or criteria to assess the legitimacy and

viability of the proposed regulation of end-to-end encryption in New Zealand. It discusses the main approaches the proposal to regulate end-to-end encryption may take and explains why they are not in line with the country's current encryption laws and legal framework. Part 6 closes with a short reflection on the value of utilising the encryption legal framework as a guide for developing encryption laws and policies.

2. Encryption, encryption keys and encrypted data

Before examining the relevant laws, it would be useful to understand the technical elements and aspects of encryption. Encryption is basically *a technology that transforms information or data into ciphers or code for purposes of ensuring its confidentiality, integrity and authenticity.*[8] It achieves these purposes by converting plaintext (unencoded, comprehensible information) into ciphertext (encoded, unintelligible or indecipherable information) using an encryption algorithm and an encryption key.[9] The reverse process of transforming the ciphertext back into plaintext is called decryption and requires a decryption key (which may be the same or different from the encryption key).[10]

A key is basically a unique string of information such as a large random number that is used in the encoding or decoding process. When the encryption and decryption keys are one and the same, this is known as symmetric encryption.[11] Symmetric encryption is often used to secure and keep private stored data or data at rest (e.g., a message saved on a phone).[12] If the encryption and decryption keys are different, there is asymmetric encryption.[13] Asymmetric encryption is generally used for communications or data in motion (for instance, a message in the process of being transmitted to another person).[14] A common,

[8] See Alfred J Menezes, Paul C van Oorschot and Scott A Vanstone, *Handbook of Applied Cryptography* (CRC Press 1996) 4 and 11-12.
[9] Andress (n 1) 63 and 64.
[10] ibid 63.
[11] See Hans Delfs and Helmut Knebl, *Introduction to Cryptography: Principles and Applications* (Springer 2015).
[12] Andress (n 1) 75.
[13] Delfs and Knebl (n 11).
[14] Andress (n 1) 76-77.

widely-used example of asymmetric encryption is public key cryptography, which utilises a key pair consisting of a public key (used for encryption) and a private key (for decryption).[15]

End-to-end encryption is a specific kind of encryption where the communications between two parties are fully encrypted: from creation, transmission and receipt of the message. End-to-end encryption is distinctive in that the communicating parties have exclusive possession of their private or decryption keys. The messaging company, service provider or network operator do not have access to the keys. Further, even though messaging or service providers could potentially intercept, record or copy the encrypted messages on their services, the collected encrypted messages would be unintelligible to them since they are unable to decrypt the messages without the decryption keys.

3. Substantive and procedural criminal and cybercrime laws

3.1 Export control and substantive cybercrime laws

Export control and cybercrime laws are two types of law that directly affect the distribution and development of encryption. Export control laws cover dual-use goods and technologies such as encryption, which may be used for both civilian and military purposes.[16] The Wassenaar Arrangement is one of the major international instruments that require the implementation of export controls on dual-use technologies.[17] The Wassenaar Arrangement has been implemented in New Zealand through customs and excise laws[18] and pertinent Customs Export Prohibition Orders (CEPO).[19] The CEPOs allow for the publication of the New Zealand Strategic Goods List (NZSGL), which details the technologies that are subject to export restrictions.[20]

---

[15] Menezes, van Oorschot and Vanstone (n 8) 14; see also Andress (n 1) 72.
[16] NZ Ministry of Foreign Affairs and Trade, 'Trading weapons and controlled chemicals: Which goods are controlled?'.
[17] See The Wassenaar Arrangement <https://www.wassenaar.org/> accessed 30 May 2021.
[18] See Customs and Excise Act 1996, s 56; see also Customs and Excise Act 2018, s 2.
[19] See, for example, Customs Export Prohibition Order 2017.
[20] NZ Ministry of Foreign Affairs and Trade, New Zealand Strategic Goods List (October 2017).

The NZSGL effectively mirrors the Wassenaar Arrangement, which states that if an encryption product meets all of the following then it is not subject to export control: (a) generally available to the public by being sold, without restriction, from stock at retail selling points; (b) the cryptographic functionality cannot easily be changed by the user; or (c) designed for installation by the user without further substantial support by the supplier.[21] Many everyday goods and services employ encryption technologies that are exempt from the Wassenaar Arrangement. For example, copy-protection mechanisms for video streaming sites like Netflix, digital rights management (DRM) on DVD players and e-books, virtual private networks (VPNs), secure internet protocols (HTTPS), and email encryption are exempt from export license requirements. It should also be pointed out that these export control rules only apply to the export of encryption.[22] There are no restrictions on the importation of encryption into the country. People living in New Zealand can therefore freely access, download and use encryption technologies from abroad such as widely used encryption tools such VeraCrypt, OpenPGP and Signal. Since most encryption technologies are developed outside of the country and publicly available online, it is difficult to control access to and use of encryption domestically.

Cybercrime laws are also relevant to encryption. The Crimes Act 1961 is the principal substantive cybercrime statute in New Zealand, particularly sections 248-252.[23] The provision that is most pertinent to encryption is section 251, which is the crime of misuse of devices.[24] Pursuant to section 251, it is illegal for a person to make, sell, distribute or possess software or other information for committing a cybercrime such as unauthorised access.[25] The Crimes Act 1961 states that it is illegal to provide or possess 'any software or other

[21] ibid 193.
[22] See Nathan Saper, 'International Cryptography Regulation and the Global Information Economy' (2012-2013) 11 Northwestern Journal of Technology and Intellectual Property 673, 678.
[23] Crimes Act 1961, ss 248-252.
[24] ibid s 251.
[25] ibid.

information that would enable another person to access a computer system without authorisation'[26] for either of the following reasons: (1) 'the sole or principal use of which he or she knows to be the commission of an offence' or (2) 'that he or she promotes as being useful for the commission of an offence (whether or not he or she also promotes it as being useful for any other purpose), knowing or being reckless as to whether it will be used for the commission of an offence'.[27] Section 251 applies to encryption technologies such as encryption software because they can be used to facilitate or hide criminal activities. However, since encryption is dual-use technology, it is only a crime if the encryption is primarily designed or promoted to commit illegal acts.[28] This position is confirmed by reference to article 6 of the Convention on Cybercrime, on which section 251 is based. According to the drafters of the Convention, the crime of misuse of devices is only committed in cases where the technologies 'are objectively designed, or adapted, primarily for the purpose of committing an offence. This alone will usually exclude dual-use devices' (i.e., those can be used for both legitimate and illicit purposes). [29] Thus, the development and distribution of encryption is generally not prohibited nor penalised under the law.

3.2 Criminal procedure laws

Criminal procedure law is another type of law that exerts a significant influence on how encryption is developed, accessed and used. Based on the principle of lawful access, law enforcement officers (including those from regulatory agencies) have the power to access encrypted data if the proper process is followed. Such authorisation typically comes via search, seizure and surveillance warrants and other investigatory procedures. These law enforcement powers and procedures are generally provided for in the Search and Surveillance Act 2012, which represents a consolidation of New Zealand's search and surveillance

[26] ibid s 251(1).
[27] ibid.
[28] See Council of Europe, 'Explanatory Report to the Convention on Cybercrime', para 73.
[29] ibid.

framework into a single, overarching statute. Aside from the police, law enforcement officers at public agencies granted powers to ensure compliance with regulatory regimes are conferred search powers via their governing statute. For example, New Zealand Customs Officers are conferred search powers in the Customs and Excise Act 2018, Wine Officers via the Wine Act 2003, and Tax Commissioners through the Tax Administration Act 1994. There are over seventy such governing statutes.[30]

3.2.1 Search and seizure

The power of search and seizure applies to encryption. Encrypted computers and devices can be physically seized and inspected, while encrypted stored data can be accessed, searched and copied. Under the Search and Surveillance Act 2012, 'search power' encompasses the authority of police and other law enforcement officers to enter, search, seize, inspect and examine 'any place, vehicle, or other things, or to search a person'.[31] The search of a particular place, vehicle or thing 'extends to the search of any computer system or data storage device located in whole or in part at the place, vehicle or thing'.[32] Law enforcement officers also have the power to access a computer or stored data (i.e., 'use any reasonable measures to access a computer system or other data storage device located (in whole or in part) at the place, vehicle, or other thing if any intangible material that is the subject of the search may be in that computer system or other device').[33] In relation to computers and computer data, a search involves the ability to access, 'seek, read, inspect or review data',[34] while seizure is 'to take away the physical medium upon which data or information is recorded, or to make and retain a copy of such data or information'.[35] A

[30] See Law Commission, *Review of the Search and Surveillance Act 2012* (NZLC IP40, 2016), para 1.11.
[31] Search and Surveillance Act 2012, s 3(1); see also Warren Young, Neville Trendle and Richard Mahoney, *Search and Surveillance: Act and Analysis* (Thomson Reuters 2012).
[32] ibid 183.
[33] Search and Surveillance Act 2012, s 110(h).
[34] Council of Europe (n 28)para 191.
[35] Council of Europe (n 28) para 197.

specific type of data that is crucial for gaining access to computers and stored data is access information. Access information is defined as including 'codes, *passwords*, and *encryption keys*, and any related information that enables access to a computer system or any other data storage device'.[36]

In addition to the general search and seizure power, law enforcement officers have the authority 'to request any person to assist with the entry and search'.[37] Moreover, under section 130 of the Search and Surveillance Act 2012, they have the power to require a user, owner, or provider of a computer system to provide information including access information. Section 130 of the Search and Surveillance Act 2012 states:

> A person exercising a search power in respect of any data held in a computer system or other data storage device *may require a specified person to provide access information and other information or assistance that is reasonable and necessary* to allow the person exercising the search power *to access that data*.[38]

With regard to scope, section 130 covers both users ('a user of a computer system or other data storage device or an Internet site who has relevant knowledge of that system, device, or site;') and providers ('a person who provides an Internet service or maintains an Internet site and who holds access information').[39] This means that the power to require provision of necessary information is not limited to users who are subject to or involved in the search, but also third parties providers such as website hosts, cloud computing companies and online intermediaries located or doing business in New Zealand. In section 130, the term 'user' is broadly defined and may include even those who are suspected of or charged with the commission of an offence.[40] Under subsection (1) of section 130, suspects or accused persons can be ordered to divulge their passwords, encryption and decryption keys and other access information as part of a search. Subsection (2) though provides an exception based on the

[36] Search and Surveillance Act 2012, s 3(1) (emphasis added).
[37] ibid s 110(b).
[38] ibid s 130(1) (emphasis added)
[39] ibid s 130(5).
[40] ibid s 130(5).

privilege against self-incrimination that 'a specified person may not be required… to give any information tending to incriminate the person'.[41] However, subsection (2) is subject to a further qualification in subsection (3), which states that:

> Subsection (2) does not prevent a person exercising a search power from requiring a specified person to provide information or providing assistance that is reasonable and necessary to allow the person exercising the search power to access data held in, or accessible from, a computer system or other data storage device that contains or may contain information tending to incriminate the specified person.[42]

While subsection (3) seems to contradict or nullify the express intent of subsection (2), subsection (4) also explicitly states that the preceding 'Subsections (2) and (3) are subject to subpart 5 of this Part (which relates to privilege and confidentiality)', which confirms the protection of the privilege against self-incrimination.[43] In spite of the confusing language, a reasonable interpretation of section 130 would be that a user can refuse to provide information if it will incriminate or tend to incriminate that person. Section 130 is not as problematic when it comes to providers since they normally act as third parties so they are not themselves involved in the crime being investigated and the privilege against self-incrimination is not generally available to them. The privilege against self-incrimination is discussed in more detail later in the article.

Customs officers similarly have powers to search and seize as well as to demand access to encrypted devices and stored data at the border and other ports of entry. Pursuant to the Customs and Excise Act 2018, they can conduct an initial search or a full search of an electronic device or storage medium.[44] Customs officers can further require a user to allow access or provide access information to an electronic device so that it can be searched.[45] Compared to the Search and Surveillance Act 2012, a user is defined more narrowly under

[41] ibid s 130(2).
[42] ibid s 130(3).
[43] ibid s 130(4).
[44] Customs and Excise Act 2018, s 228.
[45] ibid s 228(3)(c) and (d).

the Customs and Excise Act 2018 as it only refers to 'a person who owns, leases, possesses, or controls a device (or an employee of such a person) and who has relevant knowledge of the device.'[46] If a user has no reasonable excuse for failing to provide access information, then that person can be liable for a fine not exceeding $5,000.[47] Customs can also retain the device to arrange to gain access to it,[48] and the device may be condemned to the Crown, destroyed, or returned to the user at the court's discretion.[49]

It is evident from the above discussion that law enforcement officers have significant powers in relation to encryption. They have the power to search, seize and even break or break into encryption, encrypted data and encrypted computers. They also have the authority to compel the disclosure of passwords, encryption and decryption keys, and other access information from specific persons (including third party providers) as part of a search. With regard to border searches, Customs can similarly search and seizure electronic devices and require access information under specific conditions.

3.2.2 Surveillance

The power of surveillance is relevant to encryption, particularly with regard to the interception of encrypted communications. Surveillance power is regulated under the surveillance device regime of the Search and Surveillance Act 2012.[50] The surveillance device regime permits the use of interception devices to monitor and record communications. In addition, a surveillance device warrant authorises law enforcement officers to: 'use any assistance that is reasonable in the circumstances'; use 'any force that is reasonable in the circumstances to do so, in order to install, maintain, or remove the surveillance device, or to access and use electricity to power the surveillance device'; and obtain 'the content of a

[46] ibid s 228(5).
[47] ibid s 228(8).
[48] ibid s 228(9).
[49] ibid s 228(11).
[50] See Search and Surveillance Act 2012, ss 45-64.

telecommunication' and 'direct the relevant network operator to provide call associated data'.[51]

The Telecommunications (Interception Capability and Security) Act 2013 (TICSA) is another statute that is relevant to the surveillance of encrypted communications. The TICSA imposes obligations on network operators, which are defined as the owners, controllers or operators of public telecommunications networks.[52] Network operators have the duty to ensure that their public telecommunications networks and telecommunications services have full interception capability.[53] Full interception capability means a surveillance agency is able to obtain from a network operator's system the contents of the telecommunication in a useable format and the call associated data of a telecommunication.[54] The TICSA also applies to service providers, which are defined as 'any person who, from within our outside New Zealand, provides or makes available in New Zealand a telecommunications service to an end-user'.[55] Under the TICSA, both network operators and service providers are required to provide assistance to a surveillance agency. This entails assisting the surveillance agency identify, intercept and obtain both the content of the telecommunication and the metadata associated with the telecommunication at the time of the transmission of the telecommunication or as close to that time as is practicable, without unduly interfering with any telecommunication not authorised to be intercepted.[56] It should be noted though that network operators and service providers are only required to decrypt their users' encrypted communication if they provided the means of encryption.[57] Otherwise, they have no

[51] ibid s 55(3)(f-h).
[52] Telecommunications (Interception Capability and Security) Act 2013, s 3.
[53] ibid ss 9 and 24.
[54] ibid s 10(1)(b) and (c), and (5).
[55] ibid s 3.
[56] ibid s 24(3).
[57] ibid ss 24(3)(vi) and 10(4).

obligation under the law to ensure that a surveillance agency has the capability to decrypt such communications.[58]

In sum, law enforcement officers possess the power to use interception devices to monitor and collect encrypted and non-encrypted communications, call associated data and metadata using the surveillance device regime provided in the Search and Surveillance Act 2012. Such collection may be carried out by law enforcement officers themselves or with the assistance of network operators or service providers. In addition, network operators are mandated to ensure that their networks are interception ready or accessible in order to allow lawful access to such communications.

3.2.3 Production order

Production orders are also pertinent to encryption. A production order is an investigatory regime introduced in the Search and Surveillance Act 2012.[59] Pursuant to a production order, a person must provide 'any documents described in the order that are in his or her possession or control, and to disclose to the best of his or her knowledge or belief the location of any documents not in his or her possession of control'.[60] Productions order are generally applicable to documents and other recorded information (e.g., paper and electronic documents, subscriber information and metadata),[61] and are mainly used by law enforcement officers to officially request documents about individuals from businesses that regularly collect data such as customer records.[62] The coverage of documents that may be subject to a production order is quite broad and can include 'disks and data storage devices, and any material by means of which information is supplied to a device used for recording, storing or processing information'.[63]

[58] ibid s 24(4)(b).
[59] Law Commission (n 30), para 14.1.
[60] Young, Trendle and Mahoney (n 31) 10.
[61] Search and Surveillance Act 2012, s 71(1).
[62] Law Commission (n 30), para 14.1.
[63] Young, Trendle and Mahoney (n 31) 135.

Despite the broad scope of production orders, the use of encryption may diminish their efficacy. A person subject to a production order is only required to produce existing documents and data in their possession or control and there is no legal obligation to decrypt any encrypted documents. This means that while law enforcement officers may be able to obtain encrypted documents and data from a person or service provider these may be of little evidentiary value since they are in an unintelligible or readable format. Encryption though is less of a hindrance when it comes to non-content data such as subscriber data, traffic data and other metadata. These forms of data are much harder to conceal or keep private even with the use of encryption. Moreover, these data are generally in the possession or control of the service provider rather than the end user. Subscriber information is especially useful in criminal investigations because it can help disclose or determine the suspect's identity, location and activities. Furthermore, production orders may be used to secure a particular kind of access information: encryption and decryption keys. These keys are random strings of information (e.g., a mix of letters, numbers and other symbols) that are normally saved or stored digitally as computer files but can also be printed on paper. Since generated encryption and decryption keys fall within the meaning of documents, they can be the subject of production orders. Law enforcement officers may therefore require persons and service providers to produce their keys or disclose the keys' location. Given the criticality of encryption and decryption keys to preserving the confidentiality, integrity and authenticity of encrypted data, the authority to compel the disclosure of such keys is a powerful measure available to law enforcement.

4. Human rights and cybersecurity laws

4.1 Human rights laws

The laws relating to law enforcement discussed in the preceding part are intimately connected to two types of law that are also relevant to encryption: human rights laws and

cybersecurity laws. This is confirmed in the express purpose of the Search and Surveillance Act 2012, which states: '*the investigation and prosecution of offences*' must be done 'in a manner that is *consistent with human rights values*'.[64] The law enforcement powers and procedures in the Search and Surveillance Act 2012 and other enactments must therefore be read together with the rights and principles in the New Zealand Bill of Rights Act 1990 (NZBORA) and related laws and cases.

4.1.1 Right against unreasonable search and seizure (including surveillance)

The right against unreasonable search and seizure provides an essential counterbalance to the search, seizure and surveillance powers. Section 21 of the NZBORA provides that: 'Everyone has the right to be secure against unreasonable search or seizure, whether of the person, property, or correspondence or otherwise'.[65] This right applies 'not only to acts of physical trespass but to any circumstances where state intrusion on an individual's privacy in this way is unjustified'.[66] It includes 'not only to the interception of mail… but also to the electronic interception of private conversations and other forms of surveillance'.[67] Reference to 'correspondence' means secrecy of communications is also protected under this right. Section 21 offers broad protection and is applicable to warranted and warrantless searches, surveillance device warrants, and production orders. This means that the right against unreasonable search and seizure provides crucial legal protection against any unreasonable search, seizure or surveillance of encrypted devices, data or communications conducted pursuant to the law enforcement powers and procedures discussed in the preceding part. Pursuant to this right, a person subject to a search, seizure or

[64] Search and Surveillance Act 2012, s 5 (emphasis added).
[65] New Zealand Bill of Rights Act 1990, s 21.
[66] Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act: A Commentary* (2nd ed, LexisNexis 2015) 904.
[67] ibid 904.

surveillance can question the reasonableness and lawfulness of law enforcement actions and investigations.

The right against unreasonable search and seizure is intimately connected to the concept of reasonable expectation of privacy. The Supreme Court explained that reasonable expectation of privacy is:

> directed at protecting a 'biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination by the state' and includes information 'which tends to reveal intimate details of the lifestyle and personal choices of the individual'. [68]

Reasonable expectation of privacy is comprised to two limbs. First, the person complaining of a breach must have a subjective expectation of privacy in the place or thing being searched, or time of the police activity. Second, that expectation must be one that society is prepared to recognise as reasonable.[69] If both limbs are met, then section 21 of the NZBORA applies.

Searches of computers and other electronic devices 'raise special privacy concerns, because of the nature and extent of the information that they hold'.[70] When assessing the significance of privacy interests, outward signs of an increased subjective expectation of privacy needs to be taken into account. For instance, an electronic device with a PIN lock indicates a higher subjective expectation of privacy.[71] The focus of the second limb is on the inherent privacy of the area or thing being searched or observed.[72] The second limb is also 'a contextual one, requiring consideration of the particular circumstances of the case'.[73] Therefore, encrypted devices or data are only supposed to be seen by those who hold the access information. When encryption is applied to or used on an electronic device, data

[68] *R v Alsford* [2017] NZSC 42 [63].
[69] See Butler and Butler (n 66) 936.
[70] *Dotcom v AG* [2014] NZSC 199 [191]; see Law Commission (n 30), para 12.9.
[71] *W v R* [2017] NZCA 522 [30].
[72] ibid [38].
[73] *R v Alsford* (n 68) [63].

storage device, or a file or folder on such device, this should be taken as an indication that there is an increased subjective expectation of privacy. It is also likely that this heightened subjective expectation would be reasonable, and society would be prepared to recognise the expectation of privacy exhibited in encrypted information.

In case a search, seizure or surveillance is deemed unreasonable by a court, then the evidence may be considered improperly obtained.[74] Whether the evidence obtained through an unreasonable search is admissible in court is determined under section 30 of the Evidence Act 2006.[75] The court decides on the balance of probabilities whether the evidence was improperly obtained, and then determines whether exclusion of that evidence is proportionate to the impropriety.[76]

4.1.2 Privilege against self-incrimination

The privilege or right against self-incrimination also acts as a crucial safeguard to the use of law enforcement powers in relation to encryption. The privilege is provided for in the Evidence Act 2006. Self-incrimination is defined in the Act as 'the provision of information that could reasonably lead to, or increase the likelihood of, the prosecution of that person for a criminal office'.[77] Section 60 of the Evidence Act 2006 sets out the extent of the privilege. It states:

> (a) a person [cannot be] required to provide specific information –
>
> (i) in the course of a proceeding; or
> (ii) by a person exercising a statutory power or duty; or
> (iii) by a Police officer or other person holding a public office in the course of an investigation into a criminal offence or possible criminal offence; and
>
> (b) the information would, if so provided, be likely to incriminate the person under New Zealand law for an offence punishable by a fine or imprisonment.[78]

[74] Evidence Act 2006, s 30(5)(a).
[75] ibid s 30.
[76] ibid s 30(2).
[77] ibid s 4.
[78] ibid s 60(1)(a-b).

Subsection (2) of section 60 further provides that 'the person… cannot be prosecuted or penalised for refusing or failing to provide the information, whether or not the person claimed the privilege when the person refused or failed to provide the information'.[79]

The core principle underlying this privilege is that the state cannot require persons to provide information which may expose them to incurring a criminal penalty.[80] The privilege against self-incrimination 'presupposes that the prosecution in a criminal case seek to prove their case against the accused without resort to evidence obtained through methods of coercion or oppression in defiance of the will of the accused'.[81] This is in line with the common law rule that 'no person can be forced to make an incriminating statement against his or her will'.[82] Furthermore, 'at common law the right to refuse to answer incriminatory questions embraces not just answers to *oral* interrogation, but also requests for the production of *documentation* (including pre-existing documents) and any other incriminating evidence'.[83] The privilege includes the right 'to decline to produce pre-existing documentary material', which may be interpreted as including access information.[84]

As with any right or privilege, the privilege against self-incrimination is not absolute and is subject to reasonable limitations and conditions as prescribed by law. It is possible for laws to impose an obligation on a person to provide information while also expressly retaining the privilege against self-incrimination.[85] The previously cited section 130 of the Search and Surveillance Act 2012 is an example of this. Subsections (1) and (3) of section 130 impose an obligation on a person to provide access information if required by law enforcement officers as part of a search and seizure.[86] However, subsections (2) and (4)

[79] ibid s 60(2)(b).
[80] Law Commission, *The Privilege against Self-Incrimination* (NZLC PP25, 1996), para 1.
[81] Butler and Butler (n 66) 1436.
[82] ibid 1437.
[83] ibid.
[84] ibid 1439.
[85] Law Commission (n 80) para 6.
[86] Search and Surveillance Act 2012, s 130(1).

explicitly and by implication affirm the privilege against self-incrimination in computer system searches.[87] This interpretation is in accord with section 60 of the Evidence Act 2006, which provides that the privilege against self-incrimination applies:

> (a) unless an enactment removes the privilege against self-incrimination either expressly or by necessary implication; and
> (b) to the extent that an enactment does not expressly or by necessary implication remove the privilege against self-incrimination.[88]

Legal experts are similarly of the view that:

> the definition of 'self-incrimination' in s 4 of the Evidence Act 2006 refers to information 'that could reasonably lead to, or increase the likelihood of,… prosecution'. Arguably, *access information* or *information as to the whereabouts* would meet that definition if the fact that the person had that information established the link between him or her and the evidential material. In that event… *the person may not be required to provide the information*.[89]

In general, the above-cited laws do not distinguish between physical and electronic searches of tangible versus intangible evidence. The privilege against self-incrimination can apply in all of these cases. The privilege then provides a legal basis for persons suspected of or charged with a crime to lawfully refuse to provide passwords and other access information to encrypted data and devices as part of a computer system search under section 130 of the Search and Surveillance Act 2012 if doing so would reasonably lead to and increase the likelihood of their prosecution. The privilege against self-incrimination offers robust protection as it safeguards persons from being coerced against their will to decrypt or provide access to encrypted information that can be used against them in a criminal proceeding.

4.1.3 Other rights

Freedom of expression is another right that is pertinent to encryption. This right can be exercised as a negative action or as inaction: 'freedom of expression encompasses the right not to express an opinion or information'.[90] It thus includes the freedom not to speak,

[87] ibid s 130(2).
[88] Evidence Act 2006, s 60(3)(a-b).
[89] Young, Trendle and Mahoney (n 31) 175 (emphasis added).
[90] Butler and Butler (n 66) 671.

which is closely connected to the so-called silence immunities such as the right to silence, privilege against self-incrimination, and right not to be compelled to be a witness or to confess guilt.[91] In relation to encryption, a person can assert his or her right not to speak when asked to provide information including passwords and other access information as part of a search. Freedom of expression is also significant to encryption when this right is expressed in a positive manner. This freedom protects a person's right to communicate in codes and ciphers.[92] It further guarantee a person's ability to write code (i.e., encryption software or cryptographic algorithms), which are considered protected forms of expression .[93]

The right to privacy is another right that is often mentioned together with encryption. It is essential to point out that, while specific rights to privacy have been recognised in case law and the Privacy Act 2020,[94] there is no *general* right to privacy in New Zealand.[95] While other jurisdictions have interpreted the existence of an independent, separate or standalone right to privacy based on or as an essential part of their Bill of Rights (specifically, the right against unreasonable search and seizure), this has not been done in the country. Despite the absence of a general right that offers broad privacy protection, it is possible to claim specific privacy protections under section 21 of the NZBORA and case law.

4.2 Information security and data protection laws

4.2.1 Data protection

[91] ibid 1431-1432.
[92] ibid 528; see also International Covenant on Civil and Political Rights, art 19(2).
[93] See Gabriella Coleman, 'Code is Speech: Legal Tinkering, Expertise, and Protest among Free and Open Source Software Developers' (2009) 24 Cultural Anthropology 420; see also *Bernstein v US Dept of Justice* 176 F.3d 1132 (1999).
[94] For example, see *Hosking v Runting* [2005] 1 NZLR 1 (CA). Note that the Privacy Act 2020 is a data protection law and is discussed in the next section.
[95] See *R v Jefferies* [1994] 1 NZLR 290; see also Stephen Penk, 'Thinking About Privacy' in S Penk and R Tobin (eds), *Privacy Law in New Zealand* (2nd ed, Thomson Reuters 2016) 20 and 23; see also Petra Butler, 'The Case for a Right to Privacy in the New Zealand Bill of Rights Act' (2013) 11 NZJPIL 213; see also Ursula Cheer, 'The Future of Privacy: Recent Legal Developments in New Zealand' (2007) 13 Canterbury Law Review 169.

In spite of the absence of a general right to privacy in New Zealand, the narrower area of informational privacy or data protection is protected under the Privacy Act 2020. The Privacy Act 2020 generally follows and conforms to the overarching approach and principles of the EU General Data Protection Regulation.[96] While the EU General Data Protection Regulation only applies to New Zealand companies doing business in the EU or are processing personal data of people in that region, the Regulation and its implementation by Data Protection Authorities and interpretation in case law in the EU may provide persuasive guidance to New Zealand courts and authorities, particularly the Privacy Commissioner.

The Privacy Act 2020 is principally concerned with the protection of a person's specific 'right to privacy of personal information' – in other words, data protection.[97] Personal information is defined broadly to mean information about an identifiable individual.[98] The Privacy Act 2020 sets out general Information Privacy Principles (IPP) relating to the collection, use and disclosure of personal information held by agencies (i.e., data controllers and data processors), and the access of individuals to ascertain and correct the information held about them by an agency.[99] The most pertinent IPP relating to encryption is IPP 5, regarding the storage and security of personal information.[100] This is similar to the principle of integrity and confidentiality in the EU General Data Protection Regulation.[101] Essentially, this principle requires an agency to ensure that the information they hold is protected and secured by such security safeguards as it is reasonable in the circumstances to take. Assessing what is reasonable in the circumstance depends on the sensitivity or confidentiality of the information involved and what safeguards could have

[96] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.
[97] Privacy Act 2020, s 3(a).
[98] ibids 7(1).
[99] ibid s 22 (agency is the term used for a private or public data controller or data processor in New Zealand).
[100] ibid s 22.
[101] EU General Data Protection Regulation, art 5(1)(f) and 32.

been put in place to protect that information.[102] An agency also has an ongoing responsibility to develop and maintain appropriate security safeguards for their information.[103]

With regard to the role of and use of encryption for securing personal information, the Privacy Commissioner does appear to require that data must be encrypted to be stored on a cloud service,[104] and that data physically transmitted between New Zealand government departments must be encrypted when being transferred.[105] In these cases, encryption helps provide greater security and privacy protection to personal information. The Privacy 101 workbooks published by the Commissioner as part of their online learning tools only mentions encryption as something that an agency may consider when transmitting information.[106]

4.2.2 Industry-specific regulation and government information security standards

The Privacy Commissioner is authorised under the Privacy Act 2020 to issue codes of practise that become part of the law.[107] These codes modify the operation of the Privacy Act 2020 for specific industries. Three such codes that involve IPP 5 are: (1) Telecommunications Information Privacy Code; (2) Credit Reporting Privacy Code; and (3) Health Information Privacy Code.[108] These codes do not alter IPP 5 in any significant way. However, the first two concern industries where the use of encryption has long been a default. In 2017, the Ministry of Health published the Health Information Governance

[102] See *Case Note 26781* [2003] NZ PrivCmr 21.
[103] *Case Note 269784* [2016] NZ PrivCmr 3.
[104] Privacy Commissioner, 'What do you have to do to keep information secure?'.
[105] Privacy Commissioner, 'Privacy Commissioner requires data encryption' (21 February 2008).
[106] See Privacy Commissioner, 'Privacy 101: An Introduction to the Privacy Act. Facilitation Guide' (December 2015) 61; and Privacy Commissioner, 'Privacy 101: An Introduction to the Privacy Act. Participant Guide' (December 2015) 48.
[107] See Privacy Act 2020, part 3 subpart 2; see also Privacy Commissioner, 'Codes of Practise' <https://www.privacy.org.nz/the-privacy-act-and-codes/codes-of-practice/> accessed 30 May 2021; see also Privacy Commissioner, 'Guidance Note on Codes of Practice under Part VI of the Privacy Act'.
[108] Out of the three remaining codes, two amend IPP12 (unique identifiers) and the other one concerns authorised disclosure of information during a civil defence national emergency. See Privacy Commissioner, 'Codes of Practise' <https://www.privacy.org.nz/the-privacy-act-and-codes/codes-of-practice/> accessed 30 May 2021.

Guidelines, which provided information on policies and procedures that must be implemented for a health provider to meet its legal obligation regarding health information.[109] These guidelines require a health provider to comply with the Health Information Security Framework,[110] which contains detailed reference to cryptography.[111] Most significantly, this framework requires that a health provider establish and document a cryptographic policy by adopting or adapting the Protective Security Requirements and the New Zealand Information Security Manual (NZISM) as a security baseline.[112] Furthermore, when building a risk profile, a health provider must consider upgradeable solutions so that encryption protocols and algorithms can be upgradable over a system's lifetime and, when decommissioning, ensuring the encryption keys used cannot be compromised.[113]

The NZ Government is also concerned about information security and data protection and it recognises the key role that encryption plays in preserving them. It has published guidelines on the IPPs, which suggest that an agency should ask itself if the information is protected by reasonable safeguards.[114] The Government has also provided advice that an agency should check to see what security requirements apply since some agencies (public service departments and selected others) fall within the scope of the Protective Security Requirements.[115] The NZ Government itself is required to adhere to the NZISM,[116] which contains a detailed chapter on cryptography and how it should be implemented in the New Zealand context.[117] The NZISM recognises the importance of encryption to information security and data protection when it states that:

---

[109] Ministry of Health, 'HISO 10064:2017 Health Information Governance Guidelines' (August 2017), para 1.
[110] ibid para 5.2.1.
[111] Ministry of Health, 'HISO 10029:2015 Health Information Security Framework' (December 2015), chap 15.
[112] ibid para 15.3.3.
[113] ibid appendix C.
[114] New Zealand Government, 'Information privacy principles. Descriptions and examples of breaches of the IPPs' 19.
[115] ibid 20.
[116] See Protective Security Requirements <https://protectivesecurity.govt.nz/> accessed 1 June 2021.
[117] New Zealand Information Security Manual (September 2020).

> Encryption is primarily used to *provide confidentiality protecting against the risk of information being exploited by an attacker*. More broadly, *cryptography can also provide authentication, non-repudiation and integrity*. Cryptography is also used in the *establishment of secure connectivity*.[118]

The NZISM explicitly requires the use and implementation of encryption in cases where 'data is transmitted between data centres over insecure or unprotected networks such as the Internet, public infrastructure or non-agency controlled networks' or when agencies 'wish to communicate over insecure or unprotected networks such as the Internet, public networks or non-agency controlled networks'.[119]

It is evident from the above discussion that the security and protection of computer systems and personal information are major concerns of both public and private actors. Government, private individuals and entities are keenly aware that encryption is crucial for ensuring the information security and data protection of their computers, data and networks.

5. Proposed regulation of end-to-end encryption

Based on the foregoing discussion, the applicable laws and legal framework of encryption in New Zealand can be used to assess the legitimacy and viability of the proposal by members of the Five Eyes alliance to regulate the use of end-to-end encryption in messaging services. The proposal is broadly stated and sparse on details as to what sort of regulation it will be and what legal obligations it will impose. Regardless of this, the proposal can be evaluated based on the general or likely regulatory approaches that the government will consider, namely: (a) encryption ban or prohibition; (b) regulation of encryption keys; and (c) mandated backdoors and weakening of encryption.[120] While the foregoing are non-exclusive, they are common approaches that governments have proposed to regulate encryption over the past decades.[121]

---

[118] ibid s 17.1.3 (emphasis added).
[119] ibid ss 17.1.48.C.03 and 17.1.48.C.04.
[120] See Bert-Jaap Koops, *The Crypto Controversy: A Key Conflict in the Information Society* (Kluwer Law International 2009) part II, chaps 6-10; see also Kaye (n 2) 14-16.
[121] ibid part II, chaps 6-10.

5.1 Encryption ban or prohibition

A prohibition or ban on the use of end-to-end encryption in messaging services and apps such as Signal, Telegram or WhatsApp may appear *prima facie* too extreme or unworkable,[122] but this has not prevented other countries from proposing or actually banning these apps.[123] Telegram has been banned in Russia, China and Iran.[124] The United Kingdom and the European Union have considered restricting the use of end-to-end encryption.[125] In the New Zealand context, a ban on encrypted messaging apps or a prohibition against these apps from implementing end-to-end encryption would be unprecedented and infeasible.[126] Further, it would not be in accord with the existing laws of encryption. Most popular messaging services are developed and provided by international companies with headquarters outside of New Zealand. Export control laws do not apply since these messaging apps and services are imported, downloaded and used in, rather than exported out of, the country.

Substantive cybercrime laws also do not support a prohibition or ban on end-to-end encryption in the New Zealand. In general, the crime of misuse of devices does not apply to dual-use technologies like encryption. It is only a crime if the sole or principal purpose of encryption is to commit an offence.[127] Thus, unless an encrypted messaging service is primarily or specifically designed or promoted for the commission of a crime, developers and users are generally free to develop, distribute, possess or use these messaging apps within the country.

---

[122] Ibid 131.
[123] See Cath Everett, 'Should encryption software be banned?' Network Security (August 2016).
[124] Palko Karasz, 'What Is Telegram, and Why Are Iran and Russia Trying to Ban It?' *New York Times* (2 May 2018) <www.nytimes.com/2018/05/02/world/europe/telegram-iran-russia.html> accessed 30 May 2021; Diana Goovaerts, 'Telegram tackles bans in Iran, China' (*Mobile World Live*, 22 June 2020) <www.mobileworldlive.com/apps/news-apps/telegram-tackles-bans-in-iran-china> accessed 30 May 2021.
[125] See Rory Cellan-Jones, 'Does the government really want to ban WhatsApp, iMessage and Skype?' (*BBC News*, 31 July 2015) <https://www.bbc.com/news/technology-33737813> accessed 30 May 2021; see also Dale Walker, 'EU inches closer to ban on end-to-end encryption' (IT Pro, 10 November 2020) <http://www.itpro.co.uk/security/357699/leaked-memo-suggests-eu-ban-on-end-to-end-encryption-imminent> accessed 30 May 2021.
[126] See InternetNZ, 'Encryption: ways forward that protect the Internet's potential' 4.
[127] See Council of Europe (n 28) para 73.

A ban or a prohibition against the use of encryption in messaging services can also negatively impact and potentially infringe freedom of expression.[128] As discussed in Part 4, users have a right to speak in code or a secret language. Furthermore, the encryption software that Signal uses to provide end-to-end encryption can deemed a protected form of written expression that may only be subjected to 'reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society'.[129] While the government may object to the uses of end-to-end encryption software, it is doubtful that the *content or code* of the encryption software *itself* would fall within any of the traditional or justified limitations to freedom of expression.[130]

5.2 Regulation of encryption keys

Another approach the government may pursue is to regulate the possession and control of encryption and decryption keys. It can seek to accomplish this in three main ways. First, it can require service providers to surrender their encryption and decryption keys as part of doing business in New Zealand. Second, it can impose a mandatory key escrow scheme where encryption and decryption keys are deposited with and held by a trusted third party. Third, the government can utilise a key disclosure law where specified persons can be compelled to produce their keys in specific situations.

The first two ways (encryption key surrender and key escrow) do not appear to be workable since they introduce exceedingly difficult problems such as reduced information security, new risks and vulnerabilities (e.g., the trusted party becomes a prime target of cyberattacks), unwanted complexity and unreliability in information systems, and increased

[128] New Zealand Bill of Rights Act 1990, s 14; see also Allen Cook Barr, 'Guardians of Your Galaxy S7: Encryption Backdoors and the First Amendment' (2016) 101 Minnesota Law Review 301.
[129] ibid ss 5 and 14.
[130] See Butler and Butler (n 66) 552-553.

costs for users and providers.[131] While it is true that, under TICSA, network operators and service providers may be required to decrypt communications if they provided the means of encryption, when it comes to end-to-end encryption, the decryption keys are held by users. This means that the government would need to demand the keys from individual users.

Key disclosure is the third way to regulate encryption keys. As explained in Part 3, law enforcement officers already have this power under section 130 of the Search and Surveillance Act 2012 and section 228 of the Customs and Excise Act 2018.[132] Users and providers of encrypted messaging apps and services may be obligated to reasonably provide necessary information including encryption and decryption keys and access information as part of a search or seizure. Of course, as discussed in Part 4, this power is subject to the privilege against self-incrimination, right against unreasonable search and seizure, and other legal rights.[133] It is a legal principle that persons cannot be compelled to make statements or provide information if these would violate their human or civil rights. Any proposed broadening or expansion of this authority to demand decryption (e.g., exclusion of the privilege against self-incrimination in cases of terrorism or child pornography) is legally objectionable[134] and democratically suspect on human rights grounds.

5.3 Mandated backdoors and weakening of encryption

Backdoors in encryption is a frequently mentioned government proposal.[135] Encryption backdoors and proposals for so-called ghost protocols[136] result in compromised or

[131] Hal Abelson and others, 'The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption' (May 1997); see also Harold Abelson and others, 'Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications' (July 2015); see also InternetNZ (n 126) 3.
[132] Search and Surveillance Act 2012, s 130; Customs and Excise Act 2018, s 228.
[133] See New Zealand Bill of Rights Act 1999, ss 21-25.
[134] See Bert-Jaap Koops, 'Commanding decryption and the privilege against self-incrimination' in CM Breur and others (eds), *New trends in criminal investigation and evidence Volume II* (Intersentia 2000).
[135] See Ryan Budish, Herbert Burkert and Urs Gasser, 'Encryption Policy and Its International Impacts: A Framework for Understanding Extraterritorial Ripple Effects' Aegis Series Paper No 1804, 10-14. See also InternetNZ (n 126) 3.
[136] See Zak Doffman, 'Slack, WhatsApp, Snapchat And Ghost Protocol All Security Risks, Says Wickr CTO' *Forbes* (2 June 2019) <https://www.forbes.com/sites/zakdoffman/2019/06/02/wickr-cto-questions-security-of-slack-whatsapp-snapchat-and-the-ghost-protocol/?sh=2fd69e8222d2> accessed 30 May 2021; see also Ian Levy

weakened encryption. From a technical standpoint, creating a backdoor in encryption would be tantamount to introducing a security vulnerability or zero-day flaw into a computer system.[137] The resulting impaired or diminished security potentially exposes people to increased and undue risks and threats to their information security and data privacy. Cryptographers, cybersecurity experts and legal scholars have long pointed out the inherent problems and disastrous consequences of backdoors and other attempts to weaken encryption.[138] Mandatory backdoors therefore do not appear to be a viable option because they go against the very purpose of encryption, which is to ensure the confidentiality, integrity and authenticity of data.[139]

Moreover, the mandated use of backdoored or weakened encryption may result in providers and businesses being in breach of their data protection and information security obligations as required by the Privacy Act 2020.[140] With respect to the government, since its very own information security manual requires the use of strong encryption in its systems and communications, it would be very strange and troublesome indeed if private individuals and entities are required to use insecure messaging services while the government has access to full end-to-end encryption.

In addition, as explained in Part 3, law enforcement officers already have extensive powers and procedures available to them to gain access to encrypted computers, data and

---

and Crispin Robinson, 'Principles for a More Informed Exceptional Access Debate' (*Lawfare*, 29 November 2018) <https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate> accessed 30 May 2021.

[137] Hugh J McCarthy, 'Decoding the Encryption Debate: Why Legislating to Restrict Strong Encryption Will Not Resolve the 'Going Dark' Problem' (2016) 20 Journal of Internet Law 1, 19.

[138] See Ronald L Rivest, 'The Case Against Regulating Encryption Technology' Scientific American (October 1998); see also ENISA, 'Opinion Paper on Encryption: Strong Encryption Safeguards our Digital Identity' (December 2016); see also Bert-Jaap Koops and Eleni Kosta, 'Looking for some light through the lens of "cryptowar" history: Policy options for law enforcement authorities against "going dark"' (2018) 34 Computer Law & Security Review 890; see also Abelson and others (n 131) 3 and 10; see also US Homeland Security Committee 'Going Dark, Going Forward: A Primer on the Encryption Debate' (June 2016) 14.

[139] See Shulz and van Hoboken (n 2) 24-25; see also InternetNZ 'Encryption: what it is and why it's important' 13.

[140] Privacy Act 2020, s 22.

communications. Rather than requiring backdoors in end-to-end encryption, law enforcement officers are better off using their existing powers and improving their digital investigation and forensic tools and techniques.[141] It may also be possible for the government to obtain a declaratory order from a court confirming that the use of hacking techniques by law enforcement is reasonable and legally permissible.[142]

The oft-cited *Apple v FBI* case (where the US Federal Bureau of Investigation (FBI) sought a court order to compel Apple to create a modified version of its smartphone operating system to allow access to the San Bernardino shooter's locked iPhone)[143] has shown that law enforcement authorities do not need backdoors to access encrypted devices and data of suspects or persons charged with crimes since they can gain access in other ways. A subsequent US Department of Justice report came to the conclusion that the FBI's request on Apple to create a backdoor was unwarranted given that the law enforcement agency should have first exhausted other available methods and means.[144] It has been confirmed that the FBI was able to break into the shooter's locked iPhone with the assistance of an Australian cybersecurity firm.[145] Currently, there are devices such as GrayKey that are being sold to law enforcement authorities to unlock encrypted iPhones.[146] The *Apple v FBI* case and its after-

[141] See Koops and Kosta (n 138); see also Orin S Kerr and Bruce Schneier, 'Encryption Workarounds' (2018) 106 The Georgetown Law Journal 989.
[142] See Search and Surveillance 2012, s 65; see also Directorate General for Internal Policies, European Parliament 'Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices' PE 583.137 (March 2017).
[143] See Michael Hack, 'The implications of Apple's battle with the FBI' Network Security (July 2016); see also Electronic Privacy Information Center, 'Apple v. FBI: Concerning an Order Requiring Apple to Create Custom Software to Assist the FBI in Hacking a Seized iPhone' <https://epic.org/amicus/crypto/apple/#background> accessed 30 May 2021.
[144] US Department of Justice, 'A Special Inquiry Regarding the Accuracy of FBI Statements Concerning its Capabilities to Exploit an iPhone Seized During the San Bernardino Terror Attack Investigation' (March 2018).
[145] Ellen Nakashima and Reed Albergotti, 'The FBI wanted to unlock the San Bernardino shooter's iPhone. It turned to a little-known Australian firm' *The Washington Post* (14 April 2021) <http://www.washingtonpost.com/technology/2021/04/14/azimuth-san-bernardino-apple-iphone-fbi/> accessed 30 May 2021.
[146] Thomas Reed, 'GrayKey iPhone unlocker poses serious security concerns' (*Malwarebytes*, 15 March 2018) <https://blog.malwarebytes.com/security-world/2018/03/graykey-iphone-unlocker-poses-serious-security-concerns/> accessed 30 May 2021.

effects illustrate why backdoors in encryption are not only technically and legally problematic, but also unnecessary.

It is evident that the proposed regulation of end-to-end encryption in messaging services is incongruous with the existing laws and legal framework of encryption in New Zealand and should not be pursued.

6. Encryption legal framework

As this article has explained, there are a number of existing laws that apply to and regulate encryption in New Zealand. The export of encryption technologies is regulated by export control rules, while the development and implementation of encryption is subject to substantive cybercrime laws. Pursuant to criminal procedure laws, law enforcement officers already possess significant powers and measures to deal with or get around encryption. Using search and seizure powers, they can conduct searches and gain access to encrypted data and devices. Law enforcement officers also have the authority to require reasonable assistance from third parties including the ability to compel disclosure of access information such as encryption keys from persons subject to or involved in a search. Law enforcement officers can likewise utilise use surveillance powers to intercept and collect encrypted communications. Furthermore, telecommunications service providers have a duty to provide reasonable assistance to law enforcement in carrying out surveillance operations, and network operators and service providers can be required to provide content data, traffic data and other metadata as part of surveillance operations.

Such law enforcement powers and procedures that apply to encryption though are not absolute and they are carefully checked and counterbalanced by protections offered by human rights and cybersecurity laws. Human rights such as the right against unreasonable search and seizure, privilege against self-incrimination and even freedom of expression provide significant legal protections to the development, access to and use of encryption.

There are also pertinent cybersecurity laws and policies that promote the use of encryption to ensure information security and data protection.

The above laws constitute an overarching legal framework that controls and regulates encryption. It is crucial then to be cognisant of these laws to gain a better understanding of what rules actually apply to encryption. The laws and legal framework of encryption are not unique to New Zealand. Comparable laws and a similar legal framework exist in the member countries of the Five Eyes alliance as well as in other states. It is therefore key for any legal proposal to regulate encryption, whether in New Zealand or in other jurisdictions, to be evaluated against this or an equivalent encryption legal framework. Even though encryption is a complex technology that appears difficult to control, it is subject to multiple laws and regulations.