Title

Laws of encryption: An emerging legal framework

Author names and affiliations

Michael Anthony C. Dizon
Senior Lecturer in Law at the University of Waikato, New Zealand

Peter John Upson
Trustee at Public Trust New Zealand

Abstract

This article examines the emerging legal framework of encryption. It specifically analyses the different categories of law that make up this legal framework, namely: export control laws, substantive cybercrime laws, criminal procedure laws, human rights laws, and cybersecurity laws. For each category of law, illustrative examples of international and national laws are discussed. This article argues that understanding the legal framework of encryption is essential to determining how this technology is currently regulated and how these regulations can be improved. It concludes that the legal framework is the key to discerning the present state and future direction of encryption laws and policies.

Keywords

encryption laws, cybercrime, export control, criminal procedure, human rights, cybersecurity

Laws of encryption: A emerging legal framework

1. Tacit and implicit encryption laws

Encryption is essential in today's information society. It is integral to and underpins a host of common information and communications technologies (ICTs) that people use in their everyday lives. Encryption is crucial for protecting the security and authenticity of data and communications and preserving people's privacy in a digital and connected world. People would be unable to securely and privately create, store, transmit and process information in an online environment without using encryption. Despite its indispensability, encryption is an extremely contentious technology. This arises from the fact that it is a dual-use technology that can be used for both legitimate and illicit means and purposes. While it can provide security and privacy benefits, encryption can also be a hindrance to law enforcement. For example, police can face difficulties gathering evidence about a suspect who utilises encryption to make his or her data and communications unintelligible, inaccessible or unusable to third parties. This encryption dilemma is perfectly captured in oft-cited *Apple vs FBI* case, where a US federal law enforcement agency asked a court to issue an order to compel Apple to create a modified version of its mobile operating system in order to gain access to a locked and encrypted iPhone of a person who shot and killed people.[1] The *Apple v FBI* case and others like it illustrate the conundrum between the national security and law enforcement implications of encryption versus its usefulness in protecting human rights and privacy. This has perplexed people on both sides of this long-standing, well-worn debate since the so-called Crypto Wars in the 1990s.[2] Based on current events and discussions, it appears that the most pressing and seemingly unresolvable law and policy issue about encryption today is: Whether encryption can or should be regulated?

There is indeed a widely held belief that, aside from export control laws on dual-use goods and technologies,[3] encryption is a largely unregulated technology in most jurisdictions around the world.[4] While it is true that there are only a few international conventions and national statutes that expressly or directly address encryption, this article argues that there already exists a network of international and national laws that apply to and regulate encryption. For all intents and purposes, these existing laws and policies evince and embody a tacit and implicit legal framework that actually and considerably controls the development, access to and use of encryption. Cognisance of the existence of this existing legal framework of encryption is essential in order to discern of how this technology is presently subject to regulation and how it can be better regulated in the future. It would be unwise to propose new encryption laws and regulations without first understanding what laws govern and exert an influence over this technology.

The principal aim of this article then is to make explicit the laws that constitute this emerging legal framework of encryption. The laws of encryption are primarily concerned with the areas of cybercrime, human rights and cybersecurity. Specifically, the legal framework of encryption centres and revolves around the Convention on Cybercrime and international and national human rights and information security laws. The relevance of the Convention on Cybercrime to encryption is understandable given that it is an influential and authoritative international legal regime on crimes involving computers, computer data and systems.[5] Since the purpose of encryption is protect the security of data and communications (i.e., their confidentiality, integrity and authenticity), the pertinence of international and national cybercrime laws and procedures to the regulation of encryption is readily apparent. Human rights and cybersecurity laws are an equally important part of the legal framework of encryption as they embody and enact the specific rights and protections that check or counterbalance the powers and procedures provided under cybercrime laws.

---

[1] Michael Hack, "The implications of Apple's battle with the FBI" (2016) Network Security 8.
[2] Simon Singh, *The Code Book* 314; Steven Levy, *Crypto* 187.
[3] Wassenaar Arrangement.
[4] See Nathan Saper "International Cryptography Regulation and the Global Information Economy" (2012-2013) 11 Northwestern Journal of Technology and Intellectual Property 673.
[5] See Convention on Cybercrime, chap II s 1.

This article's explication of the legal framework of encryption proceeds in four parts. Part 2 briefly explains three dimensions and considerations of encryption regulation, namely: the technology of encryption, the relevant parties to encryption, and the different states and types of encrypted data. Parts 3 and 4 examine the main categories of law that make up the legal framework of encryption. Part 3 focuses on substantive and procedural criminal and cybercrime laws, specifically: export control laws, substantive cybercrime laws, and criminal procedure laws. Part 4 examines the countervailing human rights laws and cybersecurity laws that apply to encryption. For each category of law discussed in Parts 3 and 4, pertinent or illustrative examples of international and national laws are referred to and analysed. Part 5 concludes with a reflection on the current state and possible future direction of encryption laws and policies, and the potential key role that the emerging legal framework of encryption can play.

2. Encryption technology, parties and data

Before examining the laws that comprise the legal framework of encryption, it is necessary to first clarify the meaning of encryption, the parties involved in its development, access to and use, and the various data that this technology is applied to. For proposes of this article, encryption is defined as *a technology that transforms information or data into ciphers or code for purposes of ensuring its confidentiality, integrity and authenticity*.[6]

With regard to the parties to encryption, there are three main actors involved: developers, users and regulators. *Developers* include cryptographers and computer scientists, programmers and engineers who implement or use encryption in various products and services.[7] Another party to encryption are *users*. The last actor involved in encryption are *regulators* who control and regulate encryption through law making and law enforcement.

Encryption can be applied to different states and types of data. There are three basic states of data: data at rest, data in motion, and data in use. *Data at rest* is when it is stored in a physical or virtual location and is not being accessed, processed or used. It is a state where the data "is on a storage device of some kind and is not moving over a network, through a protocol, and so forth".[8] *Data in motion* takes place when the data is transmitted, transferred or sent over a medium, channel, network or other means of communication. Finally, there is *data in use* where the data is currently being accessed, processed, used or put through some form of computation or operation. The three states of data are also commonly known as stored data (data at rest), communications (data in motion), and processed data (data in use). There are also various types of data that are relevant to encryption that have been defined or referred to in laws. *Content data* is the "content of the communication; i.e., the meaning or purport of the communication, or the message or information being conveyed by the communication (other than traffic data)".[9] *Traffic data* (which includes metadata) is

> any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.[10]

There is also *subscriber information*, which is defined as "any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data".[11]A final crucial type of data associated with encryption is

[6] See Michael Dizon and others, *A study of the principles and values of encryption in New Zealand* 2 and 16.
[7] See Jason Andress, *The Basics of Information Security* 63.
[8] Jason Andress, *The Basics of Information Security* 75.
[9] Explanatory Report to the Convention of Cybercrime, para 209.
[10] Convention on Cybercrime, art 1(d).
[11] Convention on Cybercrime, art 18(3).

access information, which is described as including "*codes, passwords, and encryption keys*, and any related information that enables access to a computer system or any other data storage device".[12]

The foregoing represents the *three dimensions and considerations for a legal analysis of encryption.* The laws of encryption discussed below specifically focus on these three as targets or objects of regulation, namely: the technology of encryption, the parties to encryption, and encrypted data and communications.

3. Substantive and procedural criminal and cybercrime laws

3.1 Export control laws

The first category of law that applies to and forms part of the legal framework of encryption is export control laws relating to conventional arms and dual-use goods and technologies. This category of law is one of few that explicitly and specifically addresses the technology of encryption,[13] and reveals military and espionage origins and background of this technology.[14] The international legal regime that regulates the export of encryption is the Wassenaar Arrangement. The Wassenaar Arrangement was "established in order to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies".[15] It accomplishes this by controlling the export of two categories of goods through a licensing process.[16] The first category is conventional weapons (referred to as the "Munitions List") such as firearms, armaments and armoured vehicles.[17] The second is "dual-use goods and technologies" meaning products that could be used for both military and civilian purposes such as lasers, navigation equipment and encryption.[18] States participating in the Wassenaar Arrangement incorporate the principles and rules regarding the export of encryption products into their domestic law.[19] In the United Kingdom, the list of dual-use goods and technologies was codified in The Export Control Order 2008,[20] which is in line with the European Union Regulation No 428/2009 on dual-use items.[21] With regard to the United States, the export of encryption is covered by Export Administration Regulations.[22] In New Zealand, the Customs and Excise Act 2018 applies and the list of controlled items is published in the New Zealand Strategic Goods List.[23]

Encryption can be found in the Wassenaar Arrangement's "List of dual-use goods and technologies".[24] Category 5 - Part 2 ("Information Security") of this list describes the encryption technologies and products that must receive a license from their domestic governments before they can be exported.[25] Specific systems, equipment and components developed, produced and used for cryptographic and non-cryptographic information security are subject to export control

---

[12] NZ Search and Surveillance Act 2012, art 3(1) (emphasis added).
[13] See Nathan Saper, "International Cryptography Regulation and the Global Information Economy" 677.
[14] See Simon Singh, *The Code Book* x.
[15] Wassenaar Arrangement, Founding Documents 4
[16] Wassenaar Arrangement, Founding Documents 6.
[17] Wassenaar Arrangement, Founding Documents 11-13.
[18] Wassenaar Arrangement, Founding Documents 6 and 15.
[19] Wassenaar Arrangement, Founding Documents 4.
[20] UK The Export Control Order 2008.
[21] Regulation No 428/2009 on the setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items [2008] OJ L 134/1.
[22] Export Administration Regulations Title 15 CFR § 740.17
[23] NZ Customs and Excise Act 2018 and relevant Customs Export Prohibition Orders.
[24] Wassenaar Arrangement, "List of Dual-Use Goods and Technologies and Munitions List" (December 2019) 93.
[25] Wassenaar Arrangement, "List of Dual-Use Goods and Technologies and Munitions List" (December 2019) 93-100.

requirements.[26] The main types of encryption or cryptographic technologies and products controlled under the Wassenaar Arrangement include: (a) those that use cryptography for data security;[27] (b) a cryptographic activation token;[28] (c) those that use or perform quantum cryptography;[29] (d) those that generate scrambling codes for systems using ultra-wideband techniques;[30] (e) those that generate spreading code for spread spectrum systems;[31] (f) those used for "defeating, weakening or bypassing" information security;[32] and (g) those that can "extract raw data from a computer or communications device" and "circumvent authentication or authorisation controls of the device… in order to" extract raw data.[33]

Despite the seemingly broad scope of these export control regulations, they are subject to many exemptions. In general, the export restrictions do "not apply to products when accompanying their user for the user's personal use".[34] Furthermore, the export license requirements do not apply "to technology in the public domain, to basic scientific research, or to the minimum necessary information for patent applications".[35] There are also so-called mass market exemptions for encryption that complies with the following conditions: (1) "[g]enerally available to the public by being sold with restrictions" whether by over-the-counter, mail order or electronic transactions; (2) "cryptographic functionality cannot easily be changed by the user"; and (3) can be used "without further substantial support by the supplier".[36]

In relation to cryptography used for data confidentiality, the following functions are excluded from the license requirement: authentication, digital signatures, data integrity, non-repudiation, digital rights management and copy-protection software, encryption and decryption for "entertainment, mass commercial broadcasts or medical records management", and key management for these exempted functions.[37] Other exempted cryptographic technologies and products include: smart cards and smart card readers; those used for banking use or money transactions; "cordless telephone equipment not capable of end-to-end encryption"; "portable or mobile radiotelephones and similar client wireless devices for civil use, that implement only published or commercial cryptographic standards"; "routers, switches, gateways or relays… implementing only published or commercial cryptographic standards".[38] The restrictions on technologies with cryptanalysis functions do not apply to debuggers

[26] Wassenaar Arrangement, "List of Dual-Use Goods and Technologies and Munitions List" (December 2019) 94 and 98.
[27] Wassenaar Arrangement, "List of Dual-Use Goods and Technologies and Munitions List" (December 2019), s 5.A.2.a.
[28] Wassenaar Arrangement, "List of Dual-Use Goods and Technologies and Munitions List" (December 2019), s 5.A.2.b.
[29] Wassenaar Arrangement, "List of Dual-Use Goods and Technologies and Munitions List" (December 2019), s 5.A.2.c.
[30] Wassenaar Arrangement, "List of Dual-Use Goods and Technologies and Munitions List" (December 2019), s 5.A.2.d.
[31] Wassenaar Arrangement, "List of Dual-Use Goods and Technologies and Munitions List" (December 2019), s 5.A.2.e.
[32] Wassenaar Arrangement, "List of Dual-Use Goods and Technologies and Munitions List" (December 2019), s 5.A.4.a.
[33] Wassenaar Arrangement, "List of Dual-Use Goods and Technologies and Munitions List" (December 2019), s 5.A.4.b; see also s 5.B.2 (for certain test, inspection and production equipment).
[34] Wassenaar Arrangement, "List of Dual-Use Goods and Technologies and Munitions List" (December 2019) 93.
[35] Wassenaar Arrangement, "List of Dual-Use Goods and Technologies and Munitions List" (December 2019) 3.
[36] Wassenaar Arrangement, "List of Dual-Use Goods and Technologies and Munitions List" (December 2019) 3 and 93.
[37] Wassenaar Arrangement, "List of Dual-Use Goods and Technologies and Munitions List" (December 2019) 94.
[38] Wassenaar Arrangement, "List of Dual-Use Goods and Technologies and Munitions List" (December 2019) 95-97.

and hypervisors, those limited to logical data extraction, those that use chip-off or JTAG, and those "specifically designed and limited to jail-breaking or rooting".[39]

In light of the numerous exemptions provided under the Wassenaar Arrangement, most encryption and cryptographic technologies used by ordinary users in their normal day-to-day lives would not be subject to export control rules. With regard to the three dimensions and considerations of encryption (i.e., technology, parties and data), these rules are primarily concerned with the export of encryption as technology. The Wassenaar Arrangement does not prohibit or regulate the development, production, use and even import of encryption. As technology regulation, the Wassenaar Arrangement has a precise and delineated scope. In relation to the parties to encryption, users are not directly affected. These export control rules mainly impact developers of encryption, but only with respect to the export of their encryption technologies. Finally, these rules do not regulate access to and use of encrypted data.

3.2 Substantive cybercrime laws

Unlike export control laws, substantive cybercrime laws regulate the development, production and use of encryption. The pertinent legal provision is the cybercrime of misuse of devices. Under Article 6 of the Convention of Cybercrime, it is a criminal offence to commit "intentionally and without right… the production, sale, procurement for use, import, distribution or otherwise making available of:" (a) "a device, including a computer program, designed or adapted primarily for the purpose of committing"[40] any "[o]ffences against the confidentiality, integrity and availability of computer data and systems";[41] or (b) "a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed… with intent that it be used for the purpose of committing" such offences.[42] Possession of such devices and access codes is also an offence.[43]

In the United States, three sections of Title 18 of the US Code mirror Article 6 of the Convention on Cybercrime.[44] Title 18 US Code § 1029 prohibits the use an "access device" for an illegitimate purpose.[45] Similarly, Title 18 US Code § 1030 makes it illegal to obtain, use and distribute information that was obtained by unauthorised access to a computer.[46] Finally, Title 18 US Code § 2512 makes communication intercepting devices illegal and they can be confiscated by the US government under § 2513.[47] While New Zealand is not yet a signatory to the Convention on Cybercrime, misuse of devices is penalised under section 251 of the Crimes Act 1961.[48]

With regard to encryption, the key aspect of the crime of misuse of devices is that it does not normally apply to dual-use items (i.e., technologies or devices that can be used for both legitimate and illicit purposes). The drafters of the Convention explain that

> The alternative to include all devices even if they are legally produced and distributed, was also rejected…. As a reasonable compromise the Convention restricts its scope to cases where the devices are objectively designed, or adapted, primarily for the purpose of committing an offence. This alone will usually exclude dual-use devices.[49]

---

[39] Wassenaar Arrangement, "List of Dual-Use Goods and Technologies and Munitions List" (December 2019) 99.
[40] Convention on Cybercrime, art 6(a).
[41] Convention on Cybercrime, chap 2, s 1.
[42] Convention on Cybercrime, art 6(a).
[43] Convention on Cybercrime, art 6(b).
[44] Crimes and Criminal Procedure 18 USC § 1029.
[45] Crimes and Criminal Procedure 18 USC § 1029.
[46] Crimes and Criminal Procedure 18 USC § 1030.
[47] Crimes and Criminal Procedure 18 USC § 2512 and 2513.
[48] NZ Crimes Act 1961, s 251.
[49] Council of Europe, Explanatory Report to the Convention on Cybercrime, para 73.

Encryption can be used to commit crimes or hide criminal activities. However, encryption as a technology is only illicit if its principal or sole purpose is to commit an offence. Since the primary purposes of encryption are to preserve the confidentiality, integrity and authenticity of data, the development, possession and use encryption should be deemed by default or at least *prima facie* legitimate. It is only when encryption is principally designed or used to commit illegal acts that the crime of misuse of devices is committed. This view is supported by the drafters of the Convention who explain that "there must be the specific (i.e., direct) intent that the device is used for the purpose of committing" an offence.[50] Therefore, unless encryption is primarily or specifically designed or promoted for the commission of cybercrimes, people are generally free to develop, possess and use this technology. To illustrate, the development or use of an encrypted instant messaging program such as Signal will not be illegal since it was designed for the legitimate purpose of ensuring secure and private communications of ordinary users.

The substantive cybercrime of misuse of devices is one of the handful of laws that directly affects the technology of encryption. While the law also deals with illegally obtained access information (e.g., stolen passwords and access codes), it is not specifically concerned with the encrypted data itself. With regard to parties, developers and users of encryption may be held criminally liable if they produce, distribute or make available or possess encryption that is primarily or specified designed to commit offences. On their part, regulators can use the crime of misuse of devices to prosecute persons (whether developers or users) for their unlawful development and use of encryption.

3.3 Criminal procedure laws

The category of law that constitutes a significant part of the legal framework of encryption is criminal procedure laws. Principally contained in the Convention on Cybercrime and national procedural laws, the three main powers and procedures available to law enforcement that are germane to encryption are: (a) search and seizure, (b) surveillance, and (c) production order. These law enforcement powers have a significant influence and effect on encryption because they can be used to gain lawful access to encrypted data and communications. As a result, criminal procedure laws affect all three dimensions and considerations of encryption. With regard to the parties to encryption, these procedural powers can be applied by regulators against developers and users of encryption. This can, in turn, impact the development of and access to the technology of encryption. Lastly, the main targets of these powers are the encrypted data and communications themselves.

The Convention on Cybercrime contains rules on criminal procedure and investigations for combatting cybercrime that states that sign and ratify must incorporate into their domestic laws.[51] In the United Kingdom, existing laws already covered some of the procedural powers required under the Convention on These rules can be found in different laws such as the Police and Criminal Evidence Act 1984, the Computer Misuse Act 1990, the Terrorism Act 2002, and the Proceeds of Crime Act 2002.[52] To give effect to the country's obligations under the Convention, legislation had to be enacted to create new procedural powers. These powers are provided in the Investigatory Powers Act 2016 (IPA) and The Investigatory Powers (Technical Capability) Regulations 2018.[53] In contrast, Australia and Canada introduced new legislation that amended all relevant existing legislations and created new procedural powers under an omnibus law. The pertinent law in Canada is the Protecting Canadians from Online Crime Act 2014, while Australia enacted the Cybercrime Legislation Amendment Act 2012.[54] In New Zealand, substantive cybercrime provisions are found in the Crimes Act 1961 and procedural rules are set out in the Search and Surveillance Act 2012.[55]

---

[50] Council of Europe, Explanatory Report to the Convention on Cybercrime, para 76.
[51] Convention on Cybercrime, s 2.
[52] UK Police and Criminal Evidence Act 1984; UK Computer Misuse Act 1990; UK Terrorism Act 2002; UK Proceeds of Crime Act 2002.
[53] UK Investigatory Powers Act 2016; UK Investigatory Powers (Technical Capability) Regulations 2018.
[54] Protecting Canadians from Online Crime Act 2014; Cybercrime Legislation Amendment Act 2012.
[55] NZ Crimes Act 1961; NZ Search and Surveillance Act 2012.

3.3.1 Search and seizure including reasonable provision of necessary information

The power and procedure to search and seize stored computer data is provided in Article 19 of the Convention on Cybercrime.[56] This power was included in the Convention in acknowledgement of the fact that evidence of a crime particularly cybercrime tended to be stored in the form of electronic data.[57] Article 19 gives competent authorities the ability to "search or similarly access a computer system or part of it and computer data stored therein".[58] In this context, a search involves the ability to access, "seek, read, inspect or review data".[59] With regard to seizure, it "means 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".[60] According to the drafters of the Convention, the term "competent authorities" refers to "law enforcement authorities",[61] and the phrase "search or similarly access" also means searching "for" and "of" data.[62] This allows law enforcement authorities to examine the pertinent data, as well as look for it among other unrelated data. The phrase "similarly access" is included because it "reflects more accurately computer terminology".[63]

Article 19 further empowers law enforcement authorities to search a "computer-data storage medium",[64] which is defined as "any related computer-data storage medium (e.g., diskettes) in the immediate vicinity of the computer system".[65] The Convention allows law enforcement to seize the actual physical computer system or storage device.[66] In addition, they are permitted to safeguard any computer data and electronic evidence found in the search.[67] Law enforcement authorities have the power to "make and retain a copy of", "maintain the integrity of", and "render inaccessible or remove" stored computer data.[68]

The power to search and seize stored computer data applies to encryption. Encrypted data (together with the computers, systems and electronic devices on which they are stored) can be physically or electronically searched, seized, inspected or copied. The problem though is that being able to access and understand the content of the encrypted data is another matter entirely. Because encryption protects the confidentiality, integrity and authenticity of data (including the prevention of unauthorised access), encryption can be a hindrance to law enforcement gaining access to computers and data that are subject of a search and seizure.

Due to the difficulties with gaining access to the content of encrypted stored data and making such encrypted data intelligible, the Convention on Cybercrime grants law enforcement authorities the additional power "to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein *to provide, as is reasonable, the necessary information*, to enable the undertaking of the measures" for the search and seizure of stored computer data.[69] Necessary information means "information… that which is necessary to enable the undertaking of the search and seizure, or the similarly accessing or securing".[70] This may include access information such as passwords, encryption keys and security certificates. The requirement of

[56] Convention on Cybercrime, art 19.
[57] Council of Europe, Explanatory Report to the Convention on Cybercrime, para 184.
[58] Convention on Cybercrime, art 19(1)(a).
[59] Council of Europe, Explanatory Report to the Convention on Cybercrime, para 191.
[60] Council of Europe, Explanatory Report to the Convention on Cybercrime, para 197.
[61] Council of Europe, Explanatory Report to the Convention on Cybercrime, paras 138 and 188.
[62] Council of Europe, Explanatory Report to the Convention on Cybercrime, para 191.
[63] Council of Europe, Explanatory Report to the Convention on Cybercrime, para 191.
[64] Convention on Cybercrime, art 19(1)(b).
[65] Council of Europe, Explanatory Report to the Convention on Cybercrime, para 189.
[66] Convention on Cybercrime, art 19(3)(a).
[67] Convention on Cybercrime, art 19(3).
[68] Convention on Cybercrime, art 19.
[69] Convention on Cybercrime, art 19(4) (emphasis added).
[70] Council of Europe, Explanatory Report to the Convention on Cybercrime, para 202.

assistance is considered necessary because the data that law enforcement are searching for will often be stored in computers or systems that they are unfamiliar with and are further protected by security features and measures such as encryption.[71] Pursuant to this power, law enforcement authorities may therefore "compel a system administrator to assist, as is reasonable, the undertaking of the search and seizure".[72] The administrator's assistance can help law enforcement quickly and easily locate and access the relevant data sought, and such legal compulsion "may also relieve the administrator of any contractual or other obligations not to disclose the data".[73]

This power to compel *reasonable provision of necessary information* in computer data searches is subject to a qualification. It is "restricted to that which is 'reasonable'".[74] While the Convention does not provide the standard of reasonableness, the drafters offer examples of what forms of assistance are reasonable or not:

> In some circumstances, *reasonable provision may include disclosing a password or other security measure* to the investigating authorities. However, in other circumstances, this *may not be reasonable*; for example, where the *disclosure of the password or other security measure would unreasonably threaten the privacy of other users or other data that is not authorised to be searched*.[75]

In general, requiring an administrator or a third-party provider to give up its encryption keys would not be reasonable, fair or just because the secrecy and inviolability of encryption keys are paramount in order to preserve the security and integrity of stored computer data. This is so because disclosure of encryption keys, passwords and other access information may result in compromising the security of a computer system, weakening its ability to resist an attack, and endangering the privacy and security of all of its users and not just the one who is subject of a search.

Another important qualification to the power to require assistance is that it is limited to the *provision of information* and does not appear to cover the performance of other acts. The text of Article 19(4) is very clear: "provide, as is reasonable, the necessary information".[76] The duty of assistance is therefore *communicative rather than a performative*. It only gives law enforcement the authority to require persons to disclose information and not force the latter to perform activities outside of their existing processes and technical capabilities. This means the power cannot be used to forcibly compel a person to carry out a positive act such as create a backdoor, modify a software or system, or remove or weaken any security protection.

In New Zealand, this procedural power is contained in the Search and Surveillance Act 2012.[77] Section 130 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.[78]

While it may appear that the above section gives NZ law enforcement officers the added ability to compel a person to carry out a positive act of assistance (e.g., create a backdoor), the word "assistance" should be construed as modifying or relating to the informative act (i.e., "to provide

---

[71] See Council of Europe, Explanatory Report to the Convention on Cybercrime, para 200.
[72] Council of Europe, Explanatory Report to the Convention on Cybercrime, para 200.
[73] Council of Europe, Explanatory Report to the Convention on Cybercrime, para 201.
[74] Council of Europe, Explanatory Report to the Convention on Cybercrime, para 202.
[75] Council of Europe, Explanatory Report to the Convention on Cybercrime, para 202 (emphasis added).
[76] Convention on Cybercrime, art 19(4).
[77] NZ Search and Surveillance Act 2012.
[78] NZ Search and Surveillance Act 2012, s 130(1) (emphasis added).

access information"). This interpretation is in accord with the meaning and purpose of Article 19(4) of the Convention on which section 130 is based.

3.3.2 Surveillance including requirement of technical assistance

The second main power and procedure that law enforcement authorities may utilise in relation to encryption is surveillance. In contrast to search and seizure where the focus is on gaining access to stored data (data at rest), surveillance is concerned with intercepting and collecting communications (data in motion). The Convention on Cybercrime grants law enforcement authorities the powers to intercept content data and to conduct real-time collection of traffic data.[79] Under Article 21, law enforcement authorities are empowered to do on its own or "compel a service provider, within its existing technical capability" to "collect or record through the application of technical means… content data, in real-time, of specified communications in its territory transmitted by means of a computer system".[80] A similarly worded Article 20 grants the same power albeit in relation to traffic data.[81] The Convention's drafters describes "real time" as collecting data "at the time of the communication" and "collection" as involving "a recording (i.e., a copy) made of the data being communicated".[82] In the United Kingdom, these powers are contained in the Regulation of Investigatory Powers Act (RIPA),[83] while in Canada, the use of a transmission data recorder for real-time collection of traffic data is authorised under clause 492.2 of the Protecting Canadians from Online Crime Act.[84]

Articles 21 and 20 of the Convention on Cybercrime permit law enforcement authorities to compel service providers to assist with the collection of content data and traffic data, including the duty "to co-operate and assist the competent authorities in the collection or recording of" such data.[85] This means that a service provider must help if it is able to do so and can only refuse a lawful request if it has a valid or legal reason or excuse.[86] A service provider's duty to assist is generally subject to the condition that it is "within its existing technical capability".[87] These surveillance powers do not require a service provider to "acquire or develop new equipment, hire expert support or engage in costly re-configuration of their systems".[88] However, this technical excuse does not cover situations where a service provider can or has the technical ability to use its existing hardware, software and systems in order to assist with the surveillance.[89] For instance,

> the system may be configured in such a manner, or computer programs may already be possessed by the service provider, which would permit such measures to be taken, but they are not ordinarily executed or used in the normal course of the service provider's operation. The article would require the service provider to engage or turn-on these features, as required by law.[90]

In any event, even "if a service provider does not have the technical ability to assume the collection or recording" of the specified communications, law enforcement authorities have the power "to undertake [the surveillance] themselves".[91] In this case, a service provider must grant law

[79] Convention on Cybercrime, arts 20 and 21.
[80] Convention on Cybercrime, art 21(1) (emphasis added).
[81] Convention on Cybercrime, art 20(1).
[82] Council of Europe, Explanatory Report to the Convention on Cybercrime, para 208.
[83] UK Regulation of Investigatory Powers Act 2000, s 22.
[84] Canadian Protecting Canadians from Online Crime Act, c 492.2.
[85] Convention on Cybercrime, arts 21(1)(b)(ii) and 20(1)(b)(ii).
[86] See Council of Europe, Explanatory Report to the Convention on Cybercrime, para 221.
[87] Convention on Cybercrime, arts 21(1)(b) and 20(1)(b).
[88] Council of Europe, Explanatory Report to the Convention on Cybercrime, para 221.
[89] See Council of Europe, Explanatory Report to the Convention on Cybercrime, para 221.
[90] Council of Europe, Explanatory Report to the Convention on Cybercrime, para 221.
[91] Council of Europe, Explanatory Report to the Convention on Cybercrime, para 223.

enforcement authorities physical and electronic access to the relevant premises and systems to allow the latter to install and operate the necessary equipment and devices to conduct surveillance.[92]

These surveillance powers have been subject to further development and expansion. In the United Kingdom, the Investigatory Powers Act 2016 gives the Secretary of State the power to issue a technical capability notice whereby a telecommunications operator can be compelled to undertake certain obligations including the "removal by a relevant operator of electronic protection applied by or on behalf of that operator to any communications or data".[93] In Australia, the enactment of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act has created a similar albeit expanded system where authorities can issue technical assistance notices, technical assistance requests, and technical capability notices to thirst party providers.[94]

The surveillance powers under the Convention and national procedural laws can be utilised to intercept and collect all forms of communications, including encrypted communications. However, encryption and encrypted communications can still pose significant technical and legal challenges. Even though law enforcement authorities are able to intercept encrypted communications, encryption renders the collected content data meaningless since the data is unintelligible without the encryption key. Under most national telecommunications laws, while network operators and service providers are required to make their networks interception capable and to assist with surveillance warrants and lawful access requests, they have no legal duty to decrypt the intercepted communications if they did not provide the means of encryption and have no control over the encryption process (e.g., users implementing their own encryption). It is important to emphasise that while lawful access legislation have historically mandated that telecommunications networks should be capable of being wiretapped by law enforcement, there is no corresponding obligation on the part of network operators to ensure that users' communications over their networks should be intelligible since network operators cannot prevent the communicating parties from speaking in codes or ciphers (e.g., in a language only understood by them). Furthermore, it is a generally accepted principle that that service providers and intermediaries have "[n]o general obligation to monitor" its users.[95] This rule is enunciated in the EU Electronic Commerce Directive:

> Member States shall *not impose a general obligation* on providers, when providing the services… *to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity*.[96]

This means that, absent a data retention law or rule, providers are not required to monitor, record or store their users' communications and information, and they can only be made to adhere to specific procedural rules and measures in relation to specified communications.

Despite the above limitations, surveillance power can still be effectively utilised to deal with encrypted communications. Encryption is less of a hindrance when it comes to non-content data such as traffic data, metadata and subscriber data. While law enforcement authorities may not be able to decipher encrypted content data, they can still collect and analyse traffic data, which is valuable because it can reveal the identity, location, activities and associates of a person subject to a criminal investigation. These forms of data are much harder to hide or keep secret even with the use of encryption since such data (whether in motion or in use) are generally accessible to or in the possession or control of the service provider and outside the control of the user. To illustrate, while

[92] See Council of Europe, Explanatory Report to the Convention on Cybercrime, para 223.
[93] UK Investigatory Powers Act 2016, ss 253 and 253(5)(c).
[94] Australian Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018.
[95] Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market [2000] OJ L178, art 15; see also Thibault Verbiest, Gerald Spindler and Giovanni Maria Riccio, "Study on the Liability of Internet Intermediaries".
[96] Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market [2000] OJ L178, art 15(1).

the content of an email may be encrypted, the relevant network operator or service provider (e.g., the user's internet service provider and email provider) are normally in a position to know which email addresses sent and received the email and at what time. Even the operator of an end-to-end encrypted messaging service such as WhatsApp could potentially be ordered to record or provide traffic data and other metadata about its users and their communications. Moreover, due to technical reasons or limitations, traffic data and metadata of service may not even be encrypted at all. Encrypted communications are generally known for leaking metadata.

3.3.3 Production order including provision of subscriber information

A production order is another procedural power and measure available to law enforcement to gain access to stored data (data at rest) including electronic and paper documents and records. Article 18 of the Convention on Cybercrime grants law enforcement authorities the power to order "a person… to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium" or "a service provider… to submit subscriber information relating to such services in that service provider's possession or control".[97] A production order is considered a species of the power of search and seizure. The drafters of the Convention explain that a production order is a "flexible measure" to secure evidential material in contrast to "more intrusive or more onerous" investigatory measures such as search and seizure.[98] It may also be used as a "preliminary measure in the investigation, preceding further measures such as search and seizure or real-time interception of other data".[99] This power is mainly utilised in cases where law enforcement authorities request providers to produce existing data and documents about their users that they already collect and store in their normal course of business. Countries like Canada and the United States authorise the use of production orders.[100]

One specific type of data that is an ideal target of a production order is subscriber information. The Convention on Cybercrime defines subscriber information as "any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services *other than traffic or content data*", which can be used to establish: (a) "the type of communication service used, the technical provisions taken thereto and the period of service"; (b) "the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement"; or (c) "any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement".[101] Subscriber information is essentially information about the identity of users and any information about them that are normally recorded and stored by the provider that is not traffic or content data. The term subscriber covers "a broad range of service provider clients, from persons holding paid subscriptions, to those paying on a per-use basis, to those receiving free services. It also includes information concerning persons entitled to use the subscriber's account".[102] Subscriber information can be crucial in criminal investigations because they provide valuable data about a user and the services used and help disclose a user's identity or location. It can also reveal the services or technical measures used by specified users.[103] In addition, payment data can be particularly useful in investigating "computer fraud and other economic crimes".[104]

Production orders affect the parties to encryption differently. For regulators, encryption can limit the effectiveness of production orders. While law enforcement authorities can compel a provider or a user

[97] Convention on Cybercrime, art 18(1).
[98] Council of Europe, Explanatory Report to the Convention on Cybercrime, para 171.
[99] Council of Europe, Explanatory Report to the Convention on Cybercrime, para 175.
[100] See Canadian Protecting Canadians from Online Crime Act 2014, c 492.2; see also US Crimes and Criminal Procedure 18 USC § 2703.
[101] Convention on Cybercrime, art 18(3) (emphasis added).
[102] Council of Europe, Explanatory Report to the Convention on Cybercrime, para 177.
[103] See Council of Europe, Explanatory Report to the Convention on Cybercrime, paras 178-179.
[104] Council of Europe, Explanatory Report to the Convention on Cybercrime, para 178.

to provide encrypted data and documents, such data offers little evidentiary value or usefulness since they are unintelligible. As with the power of surveillance, encryption is less of an obstacle for law enforcement when it comes to non-content data such as subscriber data, traffic data, and metadata. These forms of data, especially subscriber data, are generally in the possession or control of providers.

With respect to providers, they can only be required to give encrypted data and documents in their possession or control.[105] This means that even though a provider that uses end-to-end encryption can be ordered to produce the encrypted data sought, it has no legal obligation to provide decrypted or plaintext copies of such data if the provider does not collect and store unencrypted versions as part of its normal operations. Without any data retention laws or other similar rules, providers have no general duty to keep records of the identities of their subscribers or to monitor or record how their subscribers use their services.[106] Further, production orders cannot be used to compel a provider to subvert or weaken its technical systems to comply with the order.

On the part of users, certain access information may be producible pursuant to a production order. A key distinction should be made between two types of access information: encryption keys and passwords. Encryption keys are random strings of information (e.g., a mix of letters, numbers and other symbols) that are normally stored digitally as computer files but can also be printed on paper. Since generated encryption keys are in the form of stored data or documents, they can be subject to a production order since they are already in existence and in the possession or control of a person. A user or even a provider can possibly be compelled to produce their encryption keys or SSL keys, which may be considered documents.[107] It should be noted though that, due the critical nature of encryption keys for preserving the confidentiality, integrity and authenticity of data, the production of encryption keys may be unreasonable in certain situations. For example, requiring a company like Apple to give up the encryption keys that it uses to sign, authenticate or secure its products and service would be unreasonable. In contrast to encryption keys, passwords do not have to be written down or saved in a file and can be stored in a person's mind. Unless the passwords are stored in some form, a user cannot be compelled to produce or write down their passwords pursuant to a production order.

4. Human rights and cybersecurity laws

4.1 Human rights laws

The criminal procedure laws discussed above comprise a major part of the legal framework of encryption. However, an integral and concomitant aspect of these law enforcement powers is the consideration and protection of the rights of persons. The category of human rights law, particularly those involving individual or civil rights, is a crucial part of the laws of encryption. The principal human rights that concern encryption are the (a) right against unreasonable searches and seizures, (b) right to privacy, (c) right against self-incrimination, and (d) right to freedom of expression

4.1.1 Right against unreasonable searches and seizures including surveillance

The right against unreasonable searches and seizures is an essential counterpoint to balance the criminal powers and procedures granted to law enforcement. It is considered a "broad and general right" that "protects an amalgam of values including property, personal freedom, privacy and dignity".[108] This right preserves others values such as "liberty, dignity, bodily integrity, privacy, and

[105] See Council of Europe, Explanatory Report to the Convention on Cybercrime, para 172.
[106] See Council of Europe, Explanatory Report to the Convention on Cybercrime, para 181.
[107] See Ladar Levinson, "Secrets, lies and Snowden's email: why I was forced to shut down Lavabit" The Guardian <https://www.theguardian.com/commentisfree/2014/may/20/why-did-lavabit-shut-down- snowden-email> accessed 2 July 2019; see also Kim Zetter "Long Before the Apple-FBI Battle, Lavabit Sounded a Warning" Wired <https://www.wired.com/2016/03/lavabit-apple-fbi/> accessed 11 September 2020.
[108] Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act* 916 and 940

the right to peaceful enjoyment by people of their property".[109] The right against unreasonable searches and seizures generally protects individual persons from "unwarranted state intrusions.... [or] interferences with [their] person, property, correspondence, personal information or electronic communications".[110] The right essentially "protect[s] against unwarranted intrusions into the affairs of citizens by the state relating to the investigation and prosecution of offences or other penalties".[111] It should be noted that 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".[112] The right extends "not only to the interception of mail... but also the electronic interception of private conversations, and other forms of surveillance".[113] While the right against unreasonable searches and seizures has been traditionally construed as providing protections to property, the modern and current approach is to construe it as protecting a person's reasonable expectation of privacy.[114] It is worth noting that the right to privacy has been read into or deemed to arise out of the right against unreasonable searches and seizures. These two rights are distinct yet intimately connected.

The right against unreasonable searches and seizures is enunciated in Article 12 of the Universal Declaration of Human Rights, which states: "No one shall be subjected to arbitrary interference with his… home or correspondence…. Everyone has the right to the protection of the law against such interference or attacks".[115] The International Convention on Civil and Political Rights also provides that "No one shall be subjected to arbitrary or unlawful interference with his… home or correspondence…. Everyone has the right to the protection of the law against such interference or attacks".[116] A similar article can be found in the European Convention on Human Rights: "Everyone has the right to respect for… his home and his correspondence".[117] Another well-known formulation of this right is contained in the US Constitution:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[118]

The right against unreasonable searches and seizures provides an essential safeguard in the legal framework of encryption. With regard to the parties to encryption, this right protects users and developers against actual or possible unlawful searches, seizures and surveillance conducted by regulators. While, as third-party provider, developers cannot claim direct protection under this right, they may utilise this right to challenge the reasonableness of any provision of information or technical assistance sought from them. For regulators, this right serves as a check on their law enforcement powers. In relation to data, the right against unreasonable searches and seizures protects different states and types of encrypted data. The right applies to data at rest (i.e., stored data whether in paper or digital format), data in motion (both paper correspondences and digital communications), and data in use (processed data). This right also legally proscribes the ability of law enforcement to access, collect or record content data, traffic data and subscriber information.

4.1.2 Right to privacy

---

[109] NZ Legislation Design Advisory Committee, "Legislation Guidelines" 100.
[110] Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act* 916; see also Paul Rishworth and others, *The New Zealand Bill of Rights* 418 and 421.
[111] Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act* 932 and 935.
[112] Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act* 904
[113] Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act* 904
[114] Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act* 916-917; see also Paul Rishworth and others, *The New Zealand Bill of Rights* 419-420; see also UK Legislation Design Advisory Committee, "Legislation Guidelines" 100.
[115] Universal Declaration of Human Rights, art 12.
[116] International Convention on Civil and Political Rights, art 17.
[117] European Convention on Human Rights, art 8(1).
[118] US Constitution, Fourth Amendment.

Privacy is complex concept that defies easy or precise definition. While formulating a definitive or a universal definition of privacy appears to be an impossible task, describing the extent, elements and characteristics of privacy has proven less problematic. Privacy is intimately related to the human rights goals of individual autonomy, dignity and equality.[119] Even though privacy has been described as simply "the right to be let alone",[120] it is not merely a negative freedom since it also involves the positive freedom of "self-development".[121] Privacy has been further characterised as being composed of distinct yet interdependent elements such as solitude, intimacy, secrecy (or confidentiality) and anonymity (or inconspicuousness).[122] According to Koops and others, there are possibly nine "ideal types of privacy", namely: bodily, intellectual, spatial, decisional, communicational, associational, proprietary, behavioural, and informational privacy.[123] Despite the lack of conceptual clarity or precision with regard to the meaning of privacy, this has not prevented legislative and judicial bodies at both international and national levels from establishing or recognising a right to privacy.

Article 12 of the Universal Declaration of Human Rights explicitly provides for the right to privacy: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks".[124] Furthermore, the International Convention on Civil and Political Rights states "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation…. Everyone has the right to the protection of the law against such interference attacks".[125] In the case of *Griswold v Connecticut*, the US Supreme Court recognised a constitutional right to privacy.[126] The US Supreme Court also ruled in *Katz vs US* that a person had a "reasonable expectation of privacy" particularly in the context of electronic surveillance.[127] In the United Kingdom, an express right to privacy is provided in Article 8 of the Human Rights Act 1998:

> Everyone has the *right to respect for his private and family life*, his home and his correspondence.
>
> There shall be *no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society* in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[128]

Curiously, despite the development of the right to privacy around the world, neither New Zealand or Australia has enacted or recognised a general right to privacy.[129]

Privacy is an essential right in the digital age and highly relevant to encryption. The right to privacy mainly benefits users from unlawful interference by regulators into their private lives, homes, documents and correspondences. It limits and controls the use by regulator of law enforcement powers and measures. The right to privacy encompasses all the states and types of data including encrypted electronic and paper documents, voice and text communications, and processed data. In

---

[119] Stephen Penk, "Thinking About Privacy" 16.
[120] Samuel Warren and Louis Brandeis, "The Right to Privacy" 193 and 205.
[121] Bert-Jaap Koops and others, "A Typology of Privacy" 565 and 566.
[122] See Bert-Jaap Koops and others, "A Typology of Privacy" 564 and 566; see also Ruth Gavison, "Privacy and the Limits of Law" 433-434 and 436; see also Stephen Penk, "Thinking About Privacy" 7 and 27.
[123] Bert-Jaap Koops and others, "A Typology of Privacy" 566.
[124] Universal Declaration of Human Rights, art 12.
[125] International Convention on Civil and Political Rights, art 17.
[126] *Griswold v Connecticut*, 381 US 479 (1965).
[127] *Katz v US,* 389 US 347 (1967)
[128] UK Human Rights Act 1998, art 8 (emphasis added).
[129] See Stephen Penk, "Thinking About Privacy" 20 and 23.

fact, this extensive right also protects the underlying activities that produce, store, transmit and process these data.

4.1.3 Right against self-incrimination

The right or privilege against self-incrimination (including the right to silence and other rights of the accused) are important human rights in relation to encryption. The right to silence is an allied right to the right against self-incrimination although the former is claimed when a person is arrested or detained.[130] The right against self-incrimination and other "silence immunities"[131] are meant to "ensure the reliability of confessions", "protect persons from abuse of power by the state", and "recognise the individual's inherent right to privacy, autonomy, and dignity".[132]

The right against self-incrimination has legal foundations in statutory law, case law, and international law.[133] It is essentially "[t]he right of a person not to be compelled by the threat of punishment to answer questions" that might incriminate that person.[134] This means that, in general, the state cannot require persons to provide information which may expose them to criminal liability.[135] This right "does not require that individuals respond to criminal allegations made by the state; criminal guilt must be proved beyond reasonable doubt through the evidence of others".[136] The underlying premise of this right is that the "proper rules of battle between government and the individual require that the individual... not be conscripted by his opponent to defeat himself".[137]

It should be noted that the right against self-incrimination encompasses "not just answers to oral interrogation, but also requests for the production of documentation (including pre-existing documents) and any other incriminating evidence".[138] This includes the ability "to decline to produce pre-existing documentary material", which may be interpreted to include access information.[139] In Canada, "the act of producing pre-existing documents may be inadmissible if that act provides an incriminating link to incriminating evidence".[140] Under European law, "the right against self-incrimination applies to the forced disclosure of the existence and location of pre-existing documents, that is, to documentation which was in existence prior to any order or request to make it available to the authorities".[141]

The right against self-incrimination is expressly provided for in the International Convention on Civil and Political Rights: "In the determination of any criminal charge against him, everyone shall be entitled to the following minimum guarantees, in full equality…. Not to be compelled to testify against himself or to confess guilt".[142] In the United States, the Fifth Amendment of the US Constitution states that: "No person… shall be compelled in any criminal case to be a witness against himself".[143] Under the Canadian Charter of Rights and Freedoms, "Any person charged with an

[130] New Zealand Bill of Rights Act 1993, s 23(4); see also Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act* 1431; see also Paul Rishworth and others, *The New Zealand Bill of Rights* 661.
[131] Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act* 1431;
[132] Paul Rishworth and others, *The New Zealand Bill of Rights* 646.
[133] See International Covenant on Civil and Political Rights, art 14(3)(g); see European Convention on Human Rights, art 6; see also Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act* 1430, 1433, 1434, 1437, 1438 and 1439; see also Paul Rishworth and others, *The New Zealand Bill of Rights* 646 and 647.
[134] Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act* 1430.
[135] See NZ Law Commission, *The Privilege against Self-Incrimination* (NZLC PP25, 1996), para 1.
[136] Paul Rishworth and others, *The New Zealand Bill of Rights* 647.
[137] Paul Rishworth and others, *The New Zealand Bill of Rights* 647.
[138] Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act: A Commentary* 1437.
[139] Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act: A Commentary* 1439.
[140] Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act: A Commentary* 1441.
[141] Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act: A Commentary* 1440.
[142] International Covenant on Civil and Political Rights, art 14(3)(g).
[143] US Constitution, Fifth Amendment.

offence has the right… (c) not to be compelled to be a witness in proceedings against that person in respect of the offence".[144]

While the right against self-incrimination is considered a criminal procedure right,[145] it may be claimed by any person and not just people who are labelled criminals. The right applies to all people, including users of encryption who are accused of or charged with a crime. Developers and providers of encrypted products and services cannot generally claim protection under this right unless they are also implicated in the crime. The right against self-incrimination does not concern the technology of encryption or the encrypted data itself. It does protect against the forced *provision of information (including passwords and other access information) of a testimonial nature or character* that would allow law enforcement to gain access to encrypted data and communications.[146]

4.1.4 Freedom of expression including the right to communicate in and write code

Unlike the three human rights discussed above, the right to freedom of expression is not normally associated with nor directly affected by law enforcement matters. However, this freedom is crucial to the use of encryption. It should be noted that freedom of expression is both a positive and a negative right. Freedom of expression therefore includes the *right not to speak*. This negative right is particularly relevant in criminal or judicial proceedings as it can be asserted in the form inaction – "freedom of expression encompasses the right not to express an opinion or information".[147] Exercised in this manner, it is akin to the traditional silence immunities granted to suspects or accused persons (e.g., right against self-incrimination, right to silence, or right not to be compelled to be a witness or to confess guilt).[148]

Freedom of expression is more commonly expressed as a positive right. In relation to encryption, the exercise of this right can take two forms: the right to *communicate in code* and the right to *write code*. The Universal Declaration of Human Rights clearly provides that: "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas *through any media and regardless of frontiers*".[149] A similar right is recognised in the European Convention on Human Rights and many other national laws around the world.[150] Speaking, writing or communicating in ciphers and codes is covered by the right to freedom of expression because the term expression has an expansive and encompassing definition and scope.[151] The meaning and ambit of freedom of expression are considered "as wide as human thought and imagination".[152] This is borne out by the expanded wording in the International Convention on Civil and Political Rights, which states: "this right shall include freedom to seek, receive and impart *information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice*".[153] Furthermore, the accepted legal limitations to freedom of expression (e.g., laws against libel and defamation, racist or hate speech, obscenity and pornography, and harmful content)[154] do not specifically apply to nor prohibit the use of encryption or encrypted communications *per se*.

---

[144] Canadian Charter of Rights and Freedoms, art 11(c).
[145] See NZ Legislation Design Advisory Committee, "Legislation Guidelines" 32.
[146] Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act: A Commentary* 1442.
[147] Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act* 671.
[148] Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act* 1431-1432.
[149] Universal Declaration of Human Rights, art 19 (emphasis added).
[150] European Convention on Human Rights, art 10(1); see US Constitution, First Amendment; see New Zealand Bill of Rights Act 1990, s 14.
[151] See Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act: A Commentary* 528.
[152] *Moonen v Film and Literature Board of Review* [2000] 2 NZLR 9, [15]; see also Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act: A Commentary* 528.
[153] International Convention on Civil and Political Rights, art 19(2) (emphasis added).
[154] See Organization for Security and Co-operation in Europe, "Freedom of Expression on the Internet" 48; see also Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act: A Commentary* 536.

Furthermore, the right to freedom of expression protects both the act of writing code as well as the code itself. Encryption as embodied or implemented in software is a form of expression. Whether source code or machine code, a computer program is considered a literary work and protected by copyright.[155] As stated in the WIPO Copyright Treaty, copyright "protection applies to computer programs, *whatever may be the mode or form of their expression*".[156] This means that freedom of expression in relation to encryption safeguards not only a person's ability to communicate in secret, but also the right to develop and use a secret code or language. Freedom of expression thus extends to the development, publication and distribution of the technology of encryption – that is, the ciphers and code themselves.

Encryption software is considered a form of speech and therefore subject to protection.[157] This was the ruling in the seminal US case of *Bernstein v US Department of Justice*, which involved US export control laws that required a government license before an academic could publish and distribute information about the encryption method he developed (specifically a paper, the source code of computer programs, and other instructions).[158] The US Court of Appeals held that the export control regulations "constitute a prior restraint on speech that offends the First Amendment".[159] It explained that "Bernstein and other scientists have been effectively chilled from engaging in valuable scientific expression".[160] The Court also made far-reaching comments about the regulation of encryption. It said

> the government is intentionally retarding the progress of the flourishing science of cryptography. To the extent the government's efforts are aimed at interdicting the flow of scientific *ideas* (whether expressed in source code or otherwise), as distinguished from encryption *products*, these efforts would appear to strike deep into the heartland of the First Amendment.[161]

The Court further explained:

> Government efforts to control encryption thus may well *implicate not only the First Amendment rights of cryptographers* intent on pushing the boundaries of their science, *but also the constitutional rights of each of us* as potential recipients of encryption's bounty. Viewed from this perspective, the government's efforts to retard progress in cryptography may *implicate the Fourth Amendment, as well as the right to speak anonymously, the right against compelled speech, and the right to informational privacy*. While we leave for another day the resolution of these difficult issues, it is important to point out that Bernstein's is a suit *not merely concerning a small group of scientists laboring in an esoteric field, but also touches on the public interest broadly defined*.[162]

The US Court of Appeals affirmed that freedom of expression and the other human rights discussed in the previous sections are closely associated with and impacted by encryption, and vice versa.

The US Court's position is supported by international human rights laws. A UN Special Rapporteur explains that, with respect to the protection of freedom of expression "through any media",

> *the forms and means through which information is transmitted and received are themselves protected*, since any restriction imposed on the means necessarily interferes

[155] WIPO Copyright Treaty, art 4; see also Berne Convention, art 2.
[156] WIPO Copyright Treaty, art 4 (emphasis added).
[157] Gabriella Coleman, "Code is Speech" 434 and 436.
[158] See *Bernstein v US Dept of Justice* 176 F.3d 1132 (1999), 1136.
[159] *Bernstein v US Dept of Justice* 176 F.3d 1132 (1999), 1135.
[160] *Bernstein v US Dept of Justice* 176 F.3d 1132 (1999), 1145.
[161] *Bernstein v US Dept of Justice* 176 F.3d 1132 (1999), 1145.
[162] *Bernstein v US Dept of Justice* 176 F.3d 1132 (1999), 1146.

> with the right to receive and impart information. In this case, *encryption* and anonymity *technologies are specific media through which individuals exercise their freedom of expression*[163]

The UN Special Rapporteur also came to the same conclusion about encryption regulation:

> *Encryption* and anonymity, and the security concepts behind them, *provide the privacy and security necessary for the exercise of the right to freedom of opinion and expression in the digital age*. Such security may be *essential for the exercise of other rights, including economic rights, privacy, due process, freedom of peaceful assembly and association, and the right to life and bodily integrity*.

It is evident from the above discussion that the right to freedom of expression is highly relevant to encryption and impacts all three dimensions and considerations of encryption. This right protects the technology of encryption, which means developers are generally free to develop and distribute encryption as a form of expression. Pursuant to this freedom, users have a right to communicate in code on their own or with the use of encryption technologies. The power of regulators to regulate encryption is significantly circumscribed by this right. Finally, freedom of expression safeguards encrypted data and communications as forms of speech.

4.2 Information security and data protection laws

Together with human rights laws, information security and data protections laws are categories of law that offer a much-needed counterbalance to the wide-ranging substantive and procedural criminal and cybercrime laws that apply to encryption. Cybersecurity laws are exceedingly relevant to encryption because they require or recommend the use of this technology for the dual or alternative purposes of ensuring: (a) the confidentiality, integrity and authenticity of data (information security) and (b) the lawful processing of data (data protection).

4.2.1 Data protection

There has been a growing recognition of the importance of encryption in information security and data protection laws. For instance, the word encryption is stated thrice in the text of the EU General Data Protection Regulation.[164] This is noteworthy because encryption is merely alluded to and not expressly mentioned in the preceding EU Data Protection Directive.[165] There is a clear awareness of the criticality of encryption for information security and data protection. As the explained in the preamble of the EU General Data Protection Regulation:

> *In order to maintain security and to prevent processing in infringement of this Regulation*, the controller or processor should evaluate the risks inherent in the processing and *implement measures to mitigate those risks, such as encryption*. Those measures should *ensure an appropriate level of security, including confidentiality,* taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected.[166]

The Regulation specifically requires data controllers and processors to "implement appropriate technical and organisational measures to *ensure a level of security appropriate to the risk*, including inter alia as appropriate: (a) the pseudonymisation and *encryption of personal data*".[167] This is part of

---

[163] David Kaye, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression" (2015) 10 (emphasis added).
[164] EU General Data Protection Regulation, arts 6(4)(e), 32(1)(a) and 34(3)(a).
[165] See entire text of EU Data Protection Directive; but see EU Data Protection Directive, art 17.
[166] EU General Data Protection Regulation, recital 83 (emphasis added).
[167] EU General Data Protection Regulation, art 32(1)(a) (emphasis added).

a general legal duty to protect the security of personal data processing, which also includes "the ability to *ensure* the ongoing *confidentiality, integrity*, availability and resilience of processing systems and services".[168] It is notable as well that the application of encryption on personal data may exempt a data controller from the requirement of notifying a data subject in case of a personal data breach.[169] These rules on the use of encryption are in accord with the sixth data protection principle of integrity and confidentiality, which requires that personal data must be "processed in a manner that *ensures appropriate security* of the personal data, including *protection against unauthorised or unlawful processing and against accidental loss, destruction or damage*, using appropriate technical or organisational measures".[170] Effective compliance with this principle would likely require the use of encryption.

4.2.2 Industry-specific cybersecurity regulations

A number of industry-specific regulations and codes have specific rules concerning information security and the use of encryption. In the health and medical sector, an example is the US Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule. While the HIPAA Security Rule does not strictly mandate the use of encryption, it acknowledges the importance of this technology and broadly recommends its application.[171] The HIPAA Security Rule provides that "A covered entity or business associate must…. [i]mplement a mechanism to encrypt and decrypt electronic protected health information"[172] and "[i]mplement a mechanism to encrypt electronic protected health information whenever deemed appropriate".[173]

In the banking and financial industry, a number of regulations require the implementation of encryption for purposes of cybersecurity. For example, the European Banking Authority (EBA) has issued Guidelines on ICT and security management, which require financial institutions to implement ICT security procedures and measures such as "implementation of network segmentation, data loss prevention systems and the *encryption of network traffic* (in accordance with the data classification)" and "*encryption of data at rest and in transit* (in accordance with the data classification)".[174] With regard to internet payments, the EBA has released Final guidelines on the security of internet payment that require payment services providers to

> ensure that when exchanging sensitive payment data via the internet, *secure end-to-end encryption is applied* between the communicating parties throughout the respective communication session, in order *to safeguard the confidentiality and integrity of the data, using strong and widely recognised encryption techniques*.[175]

4.2.3 Government information security standards

Notably, governments have become cognisant of the criticality of encryption for securing their computer systems and networks. In the United States, the US National Institute of Standards and Technology (NIST) together with the US Department of Commerce published a Standard for Security Requirements for Cryptographic Modules as part of its Federal Information Processing Standards. One of the responsibilities of NIST is to "develop standards and guidelines, including minimum requirements, for *providing adequate information security for all agency operations and assets*"

---

[168] EU General Data Protection Regulation, art 32(1)(b) (emphasis added).
[169] EU General Data Protection Regulation, art 34(3)(a).
[170] EU General Data Protection Regulation, art 5 (1)(f).
[171] See US Omnibus HIPAA Final Rule, 45 CFR Parts 160 and 164 (the HIPAA Security Rule).
[172] US HIPAA Administrative Simplification Regulations, 45 CFR § 164.312(a)(2)(iv).
[173] US HIPAA Administrative Simplification Regulations, 45 CFR § 164.312(e)(2)(ii).
[174] European Banking Authority, Guidelines on ICT and security management (EBA/GL/2019/04), para 36 (c) and (f) (emphasis added).
[175] European Banking Authority, Final guidelines on the security of internet payment (EBA/GL/2014/12_Rev1), s 11.2

although excluding national security systems.[176] This standard applies to "all Federal agencies that use cryptography-based security systems to protect sensitive information in computer and telecommunication systems (including voice systems)" and it "specifies the security requirements for a cryptographic module utilized within a security system". The coverage of this standard is comprehensive since

> Cryptography-based security systems may be utilized in various computer and telecommunication applications (e.g., data storage, access control and personal identification, network communications, radio, facsimile, and video) and in various environments (e.g., centralized computer facilities, office environments, and hostile environments).[177]

While not mandatory, the standard is "available to private and commercial organizations" to adopt or use.[178]

New Zealand also has a similar New Zealand Information Security Manual (NZISM), which is "intended for use by New Zealand Government departments, agencies and organisations" and "any other organisations that have entered into a formal Agreement with the New Zealand Government to have access to classified information".[179] The Manual provides that "[c]rown entities, local government and private sector organisations are also encouraged to use this manual".[180] The main objective of the NZISM is to set out the "processes and controls essential for the protection of all New Zealand Government information and systems".[181] In general, compliance with the NZISM is mandatory. It explicitly states that covered agencies and entities must "understand and follow the requirements of the New Zealand Information Security Manual. *Protection of government information and systems is a core accountability*".[182] The NZISM recognises the vital role encryption plays in data protection and safeguarding the security of data at rest and in transit.[183] According to the Manual,

> 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*.[184]

The NZISM specifically requires the application or use of encryption in situations such as "when data is transmitted between data centres over insecure or unprotected networks such as the Internet, public infrastructure or non-agency controlled networks" or where agencies "wish to communicate over insecure or unprotected networks such as the Internet, public networks or non-agency controlled networks".[185]

The human rights and cybersecurity laws discussed in this Part have substantial effects on the technology, parties and data involved in encryption. For instance, information security laws concern the development, application and use of the technology of encryption itself. Pursuant to these laws, encryption must be implemented in specific contexts and comply with minimum or prescribed technical standards or specifications. Government agencies as systems administrators or data

---

[176] Computer standards program 15 US Code § 278g–3 (a)(3).
[177] Federal Information Processing Standards (FIPS) Publication, Standard for Security Requirements for Cryptographic Modules (FIPS PUB 140-3) iv.
[178] Federal Information Processing Standards (FIPS) Publication, Standard for Security Requirements for Cryptographic Modules (FIPS PUB 140-3) iv.
[179] New Zealand Information Security Manual (September 2020), s 1.2.3.
[180] New Zealand Information Security Manual (September 2020), s 1.1.2.
[181] New Zealand Information Security Manual (September 2020), s 1.1.1.
[182] New Zealand Information Security Manual (September 2020), s 1.2.1 (emphasis added).
[183] New Zealand Information Security Manual (September 2020), ss 17.1.5, 17.1.8 and 17.1.9.
[184] New Zealand Information Security Manual (September 2020), s 17.1.3 (emphasis added).
[185] New Zealand Information Security Manual (September 2020), ss 17.1.48.C.03 and 17.1.48.C.04.

controllers must similarly use encryption to safeguard cybersecurity. Further, human rights and cybersecurity laws protect data in its various states and types, especially data at rest and data in motion. These laws include both rights and duties to secure data. Finally, the parties to encryption are affected by these laws in differing ways. For users, their access to and use of encryption are specifically protected by specific human rights and freedoms such as the right against self-incrimination and freedom of expression. On their part, developers have obligations to protect users' data through the use of encryption in their products and services. Regulators are also greatly impacted by these laws. For one, these laws prescribe controls and limitations on their law enforcement powers. On top of this, regulators need to use encryption to ensure the information security and data protection of people living within their jurisdictions. Regulators too recognise the necessity of relying on and using encryption.

At this point, it is worth commenting on the relationship between regulators and encryption. It is evident that regulators and governments realise the importance of encryption for cybersecurity, data protection and privacy. It is ironic though that regulators are the ones who are dead set on weakening or compromising the security of encryption through controversial and problematic legislative and policy proposals such as mandatory backdoors, compulsory key escrow, and ghost protocols in encryption.[186] Such proposed encryption laws may be objected to on the ground that they are ill-suited for being incongruous or incompatible with the laws and legal framework of encryption.

5. The present and future of encryption laws

The legal dilemma or debate about encryption typically revolves around the question of whether encryption can or should be regulated. This article has shown that this problem is moot since encryption is already the subject of existing laws and regulations. It is *not a matter of if but how* encryption is controlled and regulated by law. As discussed above, the following categories of law currently apply to encryption: export control, substantive cybercrime, criminal procedure, human rights, and information security and data protection. These laws make up the emerging legal framework that regulates the development, access to and use of encryption on both international and national levels. Making this legal framework explicit is imperative in order to gain a better understanding of what these prevailing legal rules are, how they can be improved, and what future direction encryption regulation should take.

The legal framework of encryption can be used as a standard or guide to critically analyse and assess the legitimacy, acceptability and viability of any proposed encryption laws and regulations. To illustrate, government proposals for mandatory backdoors in encryption would be at odds with the legal framework of encryption. It is true that surveillance power and lawful access regulations grant regulators the authority to intercept and collect communications. However, only network operators are subject to the obligation of making their networks interception capable. Further, the duty to assist on the part of network operators and communications providers only pertains to the act of intercepting a communication and does not extend to ensuring that the content itself of the communication is intelligible. This so because, unless they provided the means of encryption, network operators and communications providers have no specific legal duty to decrypt the intercepted encrypted communications. Moreover, with regard to human rights and cybersecurity laws, users of network operators and service providers have the right to freedom of expression, and there is no law that prohibits users from communicating in code or using unintelligible words or language. Government mandated-backdoors could also potentially violate people's right to privacy and right against unreasonable searches and seizures. In addition, backdoors would compromise the security of

[186] See US Department of Justice, "International Statement: End-To-End Encryption and Public Safety" <https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety> accessed 13 November 2020; see Alex Hern, "Apple and WhatsApp condemn GCHQ plans to eavesdrop on encrypted chats" *The Guardian* <https://www.theguardian.com/uk-news/2019/may/30/apple-and-whatsapp-condemn-gchq-plans-to-eavesdrop-on-encrypted-chats> accessed 13 November 2020.

people's data and also undermine the legal principles and obligations set out in information security and data protection laws.

As demonstrated in the above example, the legal framework of encryption is the key to deciphering and determining the present state and future direction of encryption laws and policies.

Reference List

Andress J, *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice* (Syngress Press 2011)

Butler A and Butler P, *The New Zealand Bill of Rights Act: A Commentary* (LexisNexis NZ Limited 2015)

Coleman G, "Code is Speech: Legal Tinkering, Expertise, and Protect among Free and Open Source Software Developers" (2009) 24 Cultural Anthropology 420

Council of Europe, Explanatory Report to the Convention of Cybercrime

Dizon, M and others, *A study of the principles and values of encryption in New Zealand* (New Zealand Law Foundation and University of Waikato 2019)

Gavison R, "Privacy and the Limits of Law" (1980) 89 Yale Law Journal 421

Hack, M, "The implications of Apple's battle with the FBI" (2016) Network Security

Hern A, "Apple and WhatsApp condemn GCHQ plans to eavesdrop on encrypted chats" The Guardian <https://www.theguardian.com/uk-news/2019/may/30/apple-and-whatsapp-condemn-gchq-plans-to-eavesdrop-on-encrypted-chats> accessed 13 November 2020

Kaye D, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression" (2015)

Koops BJ and others, "A Typology of Privacy" (2017) 38 University of Pennsylvania Journal of International Law 483

Levinson L, "Secrets, lies and Snowden's email: why I was forced to shut down Lavabit" The Guardian <https://www.theguardian.com/commentisfree/2014/may/20/why-did-lavabit-shut-down- snowden-email> accessed 2 July 2019

Levy S, *Crypto: How the Code Rebels Beat the Government – Saving Privacy in the Digital Age* (Viking 2001)

Nathan Saper N, "International Cryptography Regulation and the Global Information Economy" (2012-2013) 11 Northwestern Journal of Technology and Intellectual Property 673

NZ Law Commission, The Privilege against Self-Incrimination (NZLC PP25, 1996)

Organization for Security and Co-operation in Europe, "Freedom of Expression on the Internet: Study of legal provisions and practices related to freedom of expression, the free flow of information and media pluralism on the Internet in OSCE participating States"

Penk S, "Thinking About Privacy" in S Penk and R Tobin (eds), *Privacy Law in New Zealand* (Thomson Reuters 2016)

Rishworth P and others, *The New Zealand Bill of Rights* (Oxford University Press 2003)

Singh S, *The Code Book: The Secret History of Codes and Codebreaking* (Fourth Estate 1999)

US Department of Justice, "International Statement: End-To-End Encryption and Public Safety" <https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety> accessed 13 November 2020

Verbiest T, Spindler G and Riccio GM, "Study on the Liability of Internet Intermediaries" (2007)

Warren S and Brandeis L, "The Right to Privacy" (1890) 4 Harvard Law Review 193

Zetter K, "Long Before the Apple-FBI Battle, Lavabit Sounded a Warning" Wired <https://www.wired.com/2016/03/lavabit-apple-fbi/> accessed 11 September 2020

Treaties, statutes and regulations

Australian Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018

Berne Convention

Canadian Charter of Rights and Freedoms

Canadian Cybercrime Legislation Amendment Act 2012

Canadian Protecting Canadians from Online Crime Act 2014

Convention on Cybercrime

EC Electronic Commerce Directive

EC Regulation No 428/2009 on the setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items [2008] OJ L 134/1

EU Data Protection Directive

EU General Data Protection Regulation

European Banking Authority, Final guidelines on the security of internet payment (EBA/GL/2014/12_Rev1)

European Banking Authority, Guidelines on ICT and security management (EBA/GL/2019/04)

European Convention on Human Rights

International Convention on Civil and Political Rights

NZ Crimes Act 1961

NZ Customs and Excise Act 2018

NZ Customs Export Prohibition Orders

NZ Information Security Manual (September 2020)

NZ Legislation Design Advisory Committee, Legislation Guidelines

NZ New Zealand Bill of Rights Act 1993

NZ Search and Surveillance Act 2012

UK Computer Misuse Act 1990

UK Export Control Order 2008

UK Human Rights Act 1998

UK Investigatory Powers Act 2016

UK Investigatory Powers (Technical Capability) Regulations 2018

UK Police and Criminal Evidence Act 1984

UK Proceeds of Crime Act 2002

UK Regulation of Investigatory Powers Act 2000

UK Terrorism Act 2002

Universal Declaration of Human Rights

US Computer standards program 15 US Code § 278g–3

US Constitution

US Crimes and Criminal Procedure 18 USC § 1029

US Export Administration Regulations Title 15 CFR § 740.17

US Federal Information Processing Standards (FIPS) Publication, Standard for Security Requirements for Cryptographic Modules (FIPS PUB 140-3)

US HIPAA Administrative Simplification Regulations

US Omnibus HIPAA Final Rule

Wassenaar Arrangement

Wassenaar Arrangement, "List of Dual-Use Goods and Technologies and Munitions List" (December 2019)

WIPO Copyright Treaty

Cases

Bernstein v US Dept of Justice 176 F.3d 1132 (1999)

Griswold v Connecticut 381 US 479 (1965)

Katz v US, 389 US 347 (1967)

Moonen v Film and Literature Board of Review [2000] 2 NZLR 9