A matter of security, privacy and trust:

A study of the principles and values of encryption in New Zealand

Michael Dizon
Ryan Ko
Wayne Rumbles
Patricia Gonzalez
Philip McHugh
Anthony Meehan

The Law Foundation NEWZEALAND
SUPPORTING INDEPENDENT LEGAL THINKING.

THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

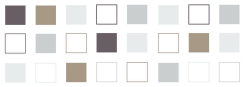
Acknowledgements

This study was funded by grants from the New Zealand Law Foundation and the University of Waikato. We would like to express our gratitude to our project collaborators and members of the Advisory Board – Prof Bert-Jaap Koops (Tilburg University), Prof Lyria Bennett Moses (UNSW Sydney), Prof Alana Maurushat (Western Sydney University), and Associate Professor Alex Sims (University of Auckland) – for their support as well as feedback on specific parts of this report. We would also like to thank Patricia Gonzalez, Joseph Graddy, Philip McHugh, Anthony Meehan, Jean Murray and Peter Upson for their valuable research assistance and other contributions to this study.

Michael Dizon, Ryan Ko and Wayne Rumbles

Principal investigators

December 2019



Executive summary

Cybersecurity is crucial for ensuring the safety and well-being of the general public, businesses, government, and the country as a whole. New Zealand has a reasonably comprehensive and well-grounded legal regime and strategy for dealing with cybersecurity matters. However, there is one area that deserves further attention and discussion – encryption. Encryption is at the heart of and underpins many of the technologies and technical processes used for computer and network security, but current laws and policies do not expressly cover this significant technology.

The principal objective of this study is to identify the principles and values of encryption in New Zealand with a view to informing future developments of encryption-related laws and policies. The overarching question is: What are the fundamental principles and values that apply to encryption? In order to answer this question, the study adopts an interdisciplinary approach that examines the technical, legal and social dimensions of encryption. With regard to the technical dimensions, this requires exploring the technical elements and aspects of encryption and how they can impact law and society. In relation to law, existing and proposed encryption law and policies in New Zealand and other jurisdictions are examined in terms of how they affect and are affected by encryption. On the social dimension, the perceptions, opinions and beliefs of three groups of stakeholders most concerned about encryption (i.e., the general public, businesses and government) are recognised and considered.

Technologies of encryption

From a technical perspective, encryption is a relatively complex technology both in theory and in practice. It can be viewed as a science, a technology or a process. Despite its innate complexity, encryption can be defined as *a technology that transforms information or data into ciphers or code for purposes of ensuring the confidentiality, integrity and authenticity of such data*. There are various kinds of encryption (e.g., symmetric, asymmetric, homomorphic, etc.) and it can be used with different types and states of data (i.e., data at rest, data in motion, and data in use). In terms of implementation and use, encryption can range from the use of a simple encryption algorithm to a full-blown cryptosystem. Depending on its level of

complexity, encryption can be or take the form of: (1) a cryptographic primitive (including an encryption algorithm); (2) a cryptographic protocol; or (3) a cryptosystem.

From an examination of the architecture and technical aspects of encryption, certain key, underlying principles and rules are readily apparent. First, encryption is integral to preserving information security. It is purposefully designed and used to realise the crucial information security objectives of confidentiality, integrity and authenticity. Second, there is the principle of the primacy of encryption keys. Since encryption keys are the lynchpin of the security of encryption and any related system that implements it, the secrecy and inviolability of these keys are paramount. Third, the principle of openness requires that the underlying source code and architecture of encryption would ideally be publicly accessible, transparent and auditable. Openness ensures that the encryption is actually safe and secure to use and it inspires the all-important trust among developers and users. Fourth, encryption is inherently adversarial in nature. This means that innovation in cybersecurity should be prioritised and continuous improvements to strengthen encryption should be encouraged. Fifth, due to the adversarial nature of encryption, it must be able to resist various forms of attacks. Sixth, the ability of encryption to resist attacks is dependent on having and achieving the appropriate level of security.

These technical principles and rules play a significant role in determining and shaping not just what encryption is and how it is used, but also how it affects law and society. From the perspective of law and policy, this means that encryption is not a simple and easy target of regulation because it involves a complex and dynamic network of diverse actors using specific technologies. Encryption is integral to preserving information security and many common and widely used technologies and systems rely on it. This means that any attempt to completely ban the development and use of encryption would be impracticable and impossible to justify whether from a cybersecurity or a law and policy standpoint. Furthermore, encryption is meant to preserve and protect information security. Therefore, a legislative proposal for mandatory backdoors for law enforcement and other purportedly legitimate purposes would be extremely problematic since it would intentionally compromise the security of encryption.

Laws of encryption

It is generally believed that encryption is largely unregulated in New Zealand and in other jurisdictions. On the face of it, this appears to be true since export control rules on dual-use goods and technologies are the main category of law that expressly addresses encryption. Export control rules generally require the developer of specific kinds of encryption or technologies that use encryption to seek prior government or regulatory approval before exporting the technology due to their potential military uses. However, export control rules actually form part of a broader, existing network of laws, regulations and rules that apply to and determine how encryption is accessed and used in the country. These laws and policies and their resulting effects and outcomes constitute a tacit and implicit framework that to a large degree controls and governs encryption. This network of laws of encryption includes export control rules, cybercrime laws, laws pertaining to law enforcement powers and measures (including search and surveillance laws and customs and border searches), and human rights laws. With regard to cybercrime laws, section 251 of the Crimes Act 1961 makes it illegal for a person to make, sell, distribute or possess software or other information for committing a crime. This prohibition can apply to the development and distribution of encryption technologies if they are used to facilitate or hide criminal activities. However, it is only a crime if the sole or principal purpose of encryption is to commit an offence. Since the primary purposes of encryption are to preserve the confidentiality, integrity and authenticity of data, then the development, possession and use encryption should be deemed by default or at least prima facie legitimate.

With regard to law enforcement powers and measures, they are the most significant type of legal rules that apply to encryption. They are extremely pertinent to encryption because they provide the authority and means by which law enforcement officers can attempt to gain access to encrypted data, communications and devices. Encryption is generally impacted by the principle of lawful access. The general powers of search and seizure can and do apply to encryption and its various implementations and uses. Encrypted computers and devices can be physically seized and inspected, and encrypted data can be subject to a search and copied. However, being able to access and understand the encrypted data is another matter altogether. This is why law enforcement officers are granted additional powers to request reasonable assistance and require the

forced disclosure of passwords and other access information from third parties and possibly even from persons suspected of or charged with a crime. Under the law, a person who refuses to render reasonable assistance or disclose passwords or access information, without reasonable excuse and/or subject to the privilege against self-incrimination, can face imprisonment for a term not exceeding three months. With regard to the interception and collection of communications, the surveillance powers and associated duties under the Search and Surveillance Act 2012, the Telecommunications (Interception Capability and Security) Act 2013 (TICSA) and other laws apply to encryption and encrypted communications. Law enforcement officers generally have the power to use interception devices to intercept and collect communications, telecommunications and call associated data to investigate a crime pursuant to the surveillance device regime of the Search and Surveillance Act 2012. The interception may be done by the law enforcement officers themselves and/or with the assistance of the network operator or service provider. Under the TICSA, networks operators are required to make their networks interception capable to allow lawful access by law enforcement, and network operators and service providers have a duty to give reasonable assistance to intercept or collect the communications sought. But network operators and service providers are not required to decrypt any communications if they themselves have not provided the encryption. For the general public and users, they are free to use encryption and encrypt their communications. Under the TICSA, users are not prohibited from using encryption on telecommunications networks or services. In addition to the traditional search, seizure and surveillance powers, law enforcement officers may also avail of production orders in order to obtain encrypted data. Pursuant to a production order, law enforcement officers may be able to compel a third party or a user to produce existing encrypted documents and data and, specifically for service providers, non-content stored data such as traffic data, subscriber data, and other metadata that is being sought.

While law enforcement officers have at their disposal significant powers and measures in relation to encryption and encrypted data and communications, these powers and the manner by which they are exercised are not absolute and they must be consistent with certain human rights principles and protections. The human rights most relevant to encryption in this regard are the right against unreasonable search and seizure and the right against self-incrimination. The right against unreasonable search and seizure is

generally applicable to the powers and measures available under the Search and Surveillance Act 2012. Section 21 of the New Zealand Bill of Rights Act 1990 provides that "Everyone has the right to be secure against unreasonable search or seizure, whether of the person, property, or correspondence or otherwise". This means people have a reasonable expectation of privacy and any search, seizure or surveillance must comply with the overriding standard of reasonableness. In relation to the duty of reasonable assistance on the part of third-party providers, they may only be required to perform acts that are reasonable and necessary. This means that requiring providers to create a backdoor or intentionally weaken the security of their products or services could be deemed unreasonable. On its part, the right or privilege against self-incrimination is the general principle that the state cannot require a person to provide information that may expose that individual to criminal liability. This applies to compelled oral testimony and the production of documentary evidence. With regard to the provision of access information or passwords (e.g., a password to an encrypted file or device), there is a view that the right against self-incrimination only applies if the access information *itself* is incriminating. It should be noted though that section 4 of the Evidence Act 2006 interprets the word self-incrimination broadly as it encapsulates information "that could reasonably lead to, or increase the likelihood of, the prosecution of a person for a criminal offence". Therefore, if the provision of access information would reveal incriminating data or documents, then the access information would tend to incriminate the person as the information revealed would reasonable lead to and increase the likelihood of prosecution. The requirement to assist a law enforcement officer exercising a search power by providing access information is tempered by the applicability of the right against self-incrimination. This right is the strongest safeguard available in relation to encryption as it works to prevent a person from being punished for refusing to provide information that could lead to criminal liability.

Aside from the above human right protections, information security and data protection are important considerations as well as in relation to encryption. For instance, the security and protection of information systems and personal data are important concerns in both the public and private sectors. The use of encryption underpins information security and data protection. Therefore, information security and data protection issues and concerns should be seriously and carefully considered when

exercising any investigatory powers and measures. For instance, it may not be reasonable to compel a provider not to use encryption or to weaken the privacy protections of its products and services to enable or assist in the conduct of a search, surveillance or other investigatory measure. Ensuring information security and protecting personal data are legitimate reasons for using encryption and these can serve as reasonable excuses for a provider to lawfully refrain from rendering assistance as part of an investigation. Information security and data protection are critical principles and values that need to be protected for persons living in a networked information society.

Principles and values of encryption

Encryption involves a number of distinct legal, social and technical principles and values. Of these, 10 fundamental principles and values are clearly evident and most prominent, namely: *data protection*; *information security*; *law enforcement and lawful access*; *national security and public safety*; *privacy*; *right against self-incrimination (including right to silence and other rights of persons charged)*; *right against unreasonable search and seizure*; *right to property*; *secrecy of correspondence*; and *trust*. These 10 fundamental principles and values of encryption can be further grouped into two categories: (1) human rights and freedoms (i.e., data protection, privacy, right against self-incrimination (including right to silence and other rights of persons charged), right against unreasonable search and seizure, right to property, and secrecy of correspondence) and (2) law enforcement and public order (i.e., law enforcement and lawful access and national security and public safety). It should be noted that, because of their overarching character and importance, information security and trust sit across both categories.

Aside from the above categorisation, the principles and values of encryption conform to a certain hierarchy. Across the three groups of stakeholders (i.e., general public, business and government), there is a discernible ranking or prioritisation of principles and values. For all categories of stakeholders, privacy is deemed the topmost principle and value concerning encryption. Together with privacy, data protection, information security, trust, national security and public safety, and right to property make up the top tier. The second tier is comprised of secrecy of correspondence, law enforcement and lawful access, right against unreasonable search and seizure, and right against self-incrimination (including right to silence and other rights of persons charged).

The focus group participants as a whole are concerned most about the principles and values of privacy, data protection and information security. This comes as no surprise given that the principal objective of encryption is to provide information security, that is, to ensure the confidentiality, integrity and authenticity of data and communications. At the other end of the spectrum, the focus group participants regard the principles and values concerning crime and law enforcement as having the lowest priority. The most plausible reason for this is that focus group participants do not consider these crime-related principles and values pertinent to them on a personal level because they esteem themselves to be law-abiding people. Since they are not criminals and are not involved in criminal activities, such criminal procedure rights are not particularly relevant to them. In addition to their relative rankings, the relationships between and among the principles and values are complex and conflicting especially between those belonging to the two main categories (i.e., human rights and law enforcement). This is particularly evident in the long-running debate over privacy versus national security. Despite their perennial clashes, there are noteworthy connections and correspondences between and among the principles and values of encryption. The most significant of these involves trust, which is itself a paramount principle and value. Trust can act as an intermediary that intercedes between, balances and reconciles the other principles and values with each other.

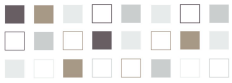
Conclusions and general policy directions

Based on the examination of the technical, legal and social dimensions of encryption, the following conclusions and recommendations can be made to inform and guide the development and improvement of laws and policies that affect encryption in New Zealand and possibly other jurisdictions as well. First, encryption is integral to information security. Because of this, the development and use of encryption should be encouraged. Moreover, laws and policies that undermine or weaken information security (whether intentionally or as an unintended effect) should be avoided. Second, encryption is necessary to protect privacy and data protection. Given the indispensability of encryption to privacy and data protection, individuals and entities should have the freedom to develop and use encryption and encryption technologies should be widely available and used by default. Any laws and policies that seek to curb the development and use of encryption or limit the choice or availability of encryption technologies should

not be pursued. Third, encryption involves law enforcement and public order values and concerns. This means that essential public interest and public order concerns must also be taken into account in relation to encryption. It is noteworthy though that there are already existing laws and rules in place in New Zealand that can be effectively used to gain access to encrypted data, communications and systems. The main issue is less about whether encryption can be regulated, but how can these powers and measures that apply to encryption be improved to better balance law enforcement and public order values vis-à-vis human rights and freedoms. Fourth, the right against unreasonable search and seizure and the right against self-incrimination are critical to encryption. These two rights represent the crux of the protection and preservation of human rights and freedoms with regard to access to and use of encryption. They represent the final or ultimate line of protection or defence against potential abuse or unreasonable outcomes. The right against unreasonable search and seizure is particularly relevant to the issue of reasonable assistance, while the right against self-incrimination is impacted by the forced disclosure of access information and passwords. Fifth, encryption requires balancing and reconciling competing principles, values and interests. A principles- and values-based approach is a useful starting point to examining the conflicts as well as possible correspondences between and among the different principles and values of encryption. In this way, areas of conflicts can also be viewed as points of connection. It is these correspondences that can potentially be developed or pursued in order to find the right balance between such apparently opposing principles, values and interests. For instance, information security is often set against national security and public safety. But information security can protect national security and public safety when it comes to preserving the integrity of public or government information systems. Sixth, encryption fundamentally relies on trust. Trust is a paramount principle and value of encryption and it plays an indispensable role in interceding between the other principles and values. Trust's mediating function is especially relevant when it comes to balancing and reconciling the competing interests and concerns surrounding encryption. It can therefore act as an essential standard or criterion for evaluating whether a balance can be or has been struck among the competing private and public issues and concerns. For example, if the principle and value of information security is diminished or sacrificed in the name of national security and public safety (e.g., requirement of mandatory backdoors in encryption), then such a

regulatory approach may be objected to on the ground that people would neither trust nor use encryption that did not provide an adequate level of security because it had a built-in weakness. Because of its fundamental importance to encryption, the maintenance and building of trust should be a principal focus when developing or proposing laws and policies on encryption.

In sum, a principles- and values-based approach can help provide guidance and direction to the development of encryption laws and policies in New Zealand. It can serve as an overarching framework for assessing the validity, legitimacy or utility of existing or proposed laws, powers and measures concerning encryption. The key is to recognise and understand the fundamental principles and values of encryption that are at play and strive to resolve or reconcile conflicts by finding connections or correspondences between them, especially with regard to maintaining or building trust. It is only then that a meaningful and workable balance between competing interests can be achieved.



Contents

1. Introduction: Encryption and the information society 1
   - 1.1 Encryption and cybersecurity 1
   - 1.2 Research objectives and questions 4
   - 1.3 Methodology 6
   - 1.4 Significance 8
   - 1.5 Research methods 9
   - 1.6 Overview of report 13

2. Technologies of encryption 14
   - 2.1 Significance of technical factors and dimensions 14
   - 2.2 Meaning of encryption 15
     - 2.2.1 Technology and science 15
     - 2.2.2 Process 17
     - 2.2.3 Kinds of encryption 18
     - 2.2.4 States and types of data 20
   - 2.3 Encryption architectures 21
     - 2.3.1 Encryption algorithms and primitives 22
       - 2.3.1.1 Block and stream ciphers 23
       - 2.3.1.2 Hash functions 23
       - 2.3.1.3 Key exchange 25
       - 2.3.1.4 Digital signatures 26
       - 2.3.1.5 Blockchain 26
     - 2.3.2 Encryption protocols 27
     - 2.3.3 Cryptosystems 27
   - 2.4 Key technical principles and rules 28
     - 2.4.1 Information security 28
       - 2.4.1.1 Confidentiality 29
       - 2.4.1.2 Integrity 29
       - 2.4.1.3 Authenticity 30
     - 2.4.2 Primacy of keys 32
       - 2.4.2.1 Secrecy 32
       - 2.4.2.2 Inviolability 33
     - 2.4.3 Openness of systems 34
     - 2.4.4 Adversarial nature 36
     - 2.4.5 Resistance to attacks 37
     - 2.4.6 Appropriate level of security 38
       - 2.4.6.1 Unconditional security – Perfect secrecy 38
       - 2.4.6.2 Computational or provable security – Impracticability and infeasibility of attacks 39
     - 2.4.7 Convenience, compatibility and other principles 41
   - 2.5 Impact and implications on law and society 42

3. Laws of encryption 46
3.1 Applicable laws 46
3.2 Export control laws 47
3.3 Cybercrime laws 50
3.4 Law enforcement powers and measures 51
3.4.1 Search and seizure 52
3.4.1.1 Grounds and scope 52
3.4.1.2 Access to computers and stored data 55
3.4.1.3 Reasonable assistance and forced disclosure of access information 61
3.4.1.4 Customs and border searches 66
3.4.1.5 Impact on stakeholders 68
3.4.2 Surveillance 69
3.4.2.1 Interception and collection of communications 69
3.4.2.2 Surveillance device regime 71
3.4.2.3 Interception capability and duty to assist 73
3.4.2.4 Content data and traffic data 75
3.4.2.5 In relation to national security 79
3.4.2.6 Effects on stakeholders 80
3.4.3 Production order 82
3.4.3.1 Nature and grounds 82
3.4.3.2 Documents and subscriber information 86
3.4.3.3 Encrypted documents and access information 89
3.4.4 Examination order 92
3.4.5 Declaratory orders 94
3.5 Human rights and other safeguards and protections 96
3.5.1 Right against unreasonable search and seizure 97
3.5.1.1 Reasonable expectation of privacy and reasonableness 97
3.5.1.2 Information held by third parties 101
3.5.1.3 Reasonable assistance 102
3.5.2 Right against self-incrimination 103
3.5.2.1 Oral and documentary evidence 103
3.5.2.2 Access information 105
3.5.2.3 Impact on sentencing 108
3.5.3 Information security and data protection 109
3.6 Tacit and implicit rules on encryption 113

4. Principles and values of encryption 115
4.1 Fundamental principles and values 115
4.1.1 Meanings 116
4.1.2 Categories 125
4.2 Hierarchy of principles and values 127
4.2.1 Ranking across and among stakeholders 127
4.2.2 Most important – those concerning privacy and information security 129
4.2.3 Least significant – those relating to crime and criminal investigations 133

4.3 Relationships between principles and values 138
4.3.1 According to different stakeholders 138
4.3.1.1 For businesses 138
4.3.1.2 For the general public 141
4.3.1.3 For government 144
4.3.2 Conflicts and connections between privacy and national security 147
4.3.3 Significance of trust 149
4.3.3.1 Mediating role 149
4.3.3.2 Trusting by nature 151
4.3.3.3 Levels of trust 152
4.3.3.4 (Dis)trust of businesses and government 155
4.4 Complex relations and possible connections 159

5. Conclusions and general policy directions 160
5.1 Encryption is integral to information security 160
5.2 Encryption is necessary to protect privacy and data protection 163
5.3 Encryption involves law enforcement and public order values and concerns 164
5.4 The right against unreasonable search and seizure and the right against self-incrimination are critical to encryption 165
5.5 Encryption requires balancing and reconciling competing principles, values and interests 168
5.6 Encryption fundamentally relies on trust 169
5.7 A principles- and values-based framework for encryption 172

Bibliography 176

Introduction: Encryption and the information society

1.1 Encryption and cybersecurity

The security of computer systems, networks and data is crucial for ensuring the safety and well-being of the general public, businesses, government, and the country as a whole. In an increasingly connected, information-dependent and technology-mediated world, private and public actors regularly use and rely on digital technologies and data in their day-to-day activities. For instance, ordinary users need safe and reliable systems and devices for everyday activities such as emailing, Web browsing, online shopping and internet banking. On their part, many companies, even those that are not part of the information technology industry (e.g., banks and retail establishments), depend on mission-critical information systems to conduct their businesses. Companies today also routinely deal with vast amounts of data (whether relating to their business, customers or employees) and they require robust technologies and processes to securely collect, process and store such data. Computer and data security is of paramount importance to government as well. Access to and use of secure information systems and tools are essential for government institutions, departments and agencies to operate efficiently and work effectively for the public interest and to perform their vital public service functions.

New Zealand has a reasonably comprehensive and well-grounded legal regime and strategy to deal with cybersecurity and other related matters.[1] Laws such as, among others, the Crimes Act 1961, the Harmful Digital Communications Act 2015, the Privacy Act 1993, the Search and Surveillance Act 2012, and the Telecommunications (Interception Capability and Security) Act 2013 are generally fit for purpose for tackling cybercrime and other cybersecurity threats. In addition, the country's Cyber Security

[1] See New Zealand's Cyber Security Strategy 2019; see New Zealand's Cyber Security Strategy 2015 Action Plan 2.

Strategy and corollary Action Plan are commendable and noteworthy for the following reasons: they rightly focus on both the technical and non-technical aspects of computer security (e.g., raising public awareness and investing in developing human resources); they emphasise the importance of public-private cooperation; they recognise the importance of having a stable and certain legal regime (particularly in relation to the prevention and prosecution of cybercrime); and they acknowledge the importance of international cooperation.[2]

There is one area of cybersecurity though that deserves further attention and research – encryption.[3] Encryption is a *technology that transforms information or data into ciphers or code for purposes of ensuring the confidentiality, integrity and authenticity of such data*.[4] It lies at the heart of and underpins many of the technologies and technical processes used for computer and network security.[5] Common and widely used technologies and techniques for securing computers, networks and data such as AES, RSA, SHA-3, TLS/SSL, digital signatures, PGP, and PKI are founded on encryption.[6] Encryption is clearly integral to cybersecurity from a technical standpoint as well as from the perspective of law and public policy.[7] A better understanding of and approach to encryption are essential to any cybersecurity strategy and can help strengthen a country's preparedness and resilience against actual or imminent cyberattacks and threats. This position is supported by the Organisation for Economic Co-operation and Development's (OECD) adoption of a Recommendation and Guidelines for cryptography policy as far back as 1997[8] and a United Nations Special Rapporteur report that recommends that countries adopt policies that support the use of encryption in digital communications.[9] It is notable that countries such as the Netherlands have started to come out with or are seriously considering

---

[2] New Zealand's Cyber Security Strategy 2019; New Zealand's Cyber Security Strategy 2015; New Zealand's Cyber Security Strategy 2015 Action Plan.
[3] Organisation for Economic Co-operation and Development, "Recommendation of the Council Concerning Guidelines for Cryptography Policy" (1997) (encryption is defined as "the transformation of data by the use of cryptography to produce unintelligible data (encrypted data) to ensure its confidentiality").
[4] See Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 4 and 11-12 (It should be noted that while availability is not an objective of encryption itself, the presence of encryption can determine whether a system can be made available or not).
[5] Organisation for Economic Co-operation and Development, "Recommendation of the Council Concerning Guidelines for Cryptography Policy" (1997).
[6] Jason Andress, *The Basics of Information Security* 71-75 and 77.
[7] Organisation for Economic Co-operation and Development, "Report on Background and Issues of Cryptography Policy".
[8] Organisation for Economic Co-operation and Development, "Recommendation of the Council Concerning Guidelines for Cryptography Policy" (1997).
[9] United Nations Human Rights Council, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression".

adopting their own official policies on encryption.[10] Despite the undeniable complexity of the topic of encryption, these countries see the importance of considering basic principles and approaches on how encryption is treated within their jurisdictions.

Given that New Zealand recognises the value of international cooperation in relation to cybersecurity matters and sees the importance of aligning cybersecurity laws and policies on a global level due to the transnational nature and effects of cybercrime and cyber threats,[11] it makes sense to similarly gain a better appreciation of how encryption is actually developed, used and accessed by various individuals, groups, entities and organisations in the country. In this way, it can keep pace with the rest of the world on how to deal with such a significant technology. With the growing application and use of encryption on data, communications, devices and systems, the legal problems and conflicts involving encryption have become increasingly acute and prominent. The *Apple v FBI case* in the United States that made global headlines in 2016 illustrates the legal dilemma faced by various stakeholders in the private and public sectors regarding lawful access to and use of encryption.[12] As part of its criminal investigation, the US Federal Bureau of Investigation (FBI) sought a court order to compel Apple's assistance in gaining access to an iPhone that was used by a person who shot and killed 14 people. The smartphone was locked and encrypted using the phone's built-in passcode system and it was set to automatically erase all of the phone's data after 10 failed unlock attempts. Apple formally objected and publicly stated that it would refuse to accede to the request on the grounds that it did not want to weaken the security of its devices and complying would be tantamount to creating a backdoor that could potentially undermine the security and privacy of millions of its customers around the world. The US court did not have a chance to resolve the thorny legal questions posed by this case because the FBI ultimately withdrew its request as it was able to unlock the iPhone with the help of a third party who knew how to break into the phone through other means. While external factors prevented a court of law from definitively ruling on this legal quandary, the problems and issues brought up by this case and many others like it remain unresolved.

---

[10] See Dutch Cabinet Position on Encryption <https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2016Z00009&did=2016D00015> accessed 13 July 2017; see also Daniel Severson, "The Encryption Debate in Europe" Hoover Institution Aegis Paper Series No. 1702.

[11] New Zealand's Cyber Security Strategy 2015 6.

[12] Michael Hack, "The implications of Apple's battle with the FBI" (2016) Network Security 8.

The recent spate of high-profile and widespread malware attacks and data breaches around the globe highlight the fact that cybersecurity is never static and is constantly evolving.[13] As such, it is essential for laws, policies and strategies concerning computer and data security to be continually updated, adapted and improved in light of technological, social and legal changes in society. This is especially true in relation to encryption. The legal, social and technical issues surrounding encryption continue to be relevant and are not going away.[14] Governments[15] (most recently Australia)[16] and private actors[17] have made known their views on encryption and its regulation, and it seems inevitable that their conflicting positions will soon come to a head.[18] The time is ripe to identify and discern the underlying principles and values of encryption for various stakeholders and actors in New Zealand so that the country can be better informed and prepared for how to potentially deal with this crucial technology.

1.2 Research objectives and questions

The principal objective of this study is to identify the principles and values of encryption in Aotearoa New Zealand with a view to informing future developments of encryption-related laws and policies. In order to achieve this aim, the research is centred on the overarching question: What fundamental principles and values apply to

---

[13] See Radio New Zealand, "NZ computers caught up in global cyberattack" <http://www.radionz.co.nz/news/world/330677/nz-computers-caught-up-in-global-cyberattack> accessed 13 July 2017; see also Jacob Brown, "NotPetya's impact on NZ firms" <http://www.newshub.co.nz/home/new-zealand/2017/06/notpetya-s-impact-on-nz-firms.html> accessed 13 July 2017.

[14] See Bruce Schneier "More Crypto Wars II" <https://www.schneier.com/blog/archives/2014/10/more_crypto_war.html> accessed 13 July 2017; see also Brian Barrett "The Apple-FBI Battle is Over, But the New Crypto Wars Has Just Begun" Wired <https://www.wired.com/2016/03/apple-fbi-battle-crypto-wars-just-begun/> accessed 13 July 2017.

[15] CNBC, "End-to-end encryption on messaging services is unacceptable: UK minister" <http://www.cnbc.com/2017/03/26/london-attack-whatsapp-encrypted-messaging-apps-khalid-masood.html> accessed 13 July 2017; Amar Toor, "France and Germany want Europe to crack down on encryption" The Verge <https://www.theverge.com/2016/8/24/12621834/france-germany-encryption-terorrism-eu-telegram> accessed 13 July 2017.

[16] See Australian Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018; see also Associated Press, "Australia plans law to force tech giants to decrypt messages" <https://apnews.com/621e0913072a4cb5a1a7f7338721b059/Australia-plans-law-to-force-tech-giants-to-decrypt-messages> accessed 15 July 2017.

[17] See InternetNZ, "Encryption: ways forward that protect the Internet's potential"; see Security For All <https://www.securetheinternet.org/> accessed 13 July 2017.

[18] See Radio New Zealand, "Calls for strong encryption in 'Five Eyes' countries" <http://www.radionz.co.nz/news/national/334256/calls-for-strong-encryption-in-five-eyes-countries> accessed 13 July 2017; See InternetNZ, "83 organisations send strong message to Five Eyes" <https://internetnz.nz/news/83-organisations-send-strong-message-five-eyes> accessed 13 July 2017.

encryption? In order to answer this question, the study further addresses the following research questions:

1. What is encryption? What technical principles and rules apply to this technology?
2. What New Zealand laws, policies and regulations apply to encryption? How do they impact the development, access to and use of encryption?
3. What are the perceptions, opinions and beliefs of the general public, businesses, and government about encryption? Which principles and values of encryption do these stakeholders consider most important and least significant? What are the relationships between the different principles and values?
4. Which fundamental principles and values should be considered when developing encryption-related laws and policies in New Zealand?

These research questions are purposely designed to tackle not only the legal but also the technical and social dimensions that need to be considered when examining such a complex and enigmatic technology such as encryption. The first research question focuses on the technical aspects on encryption. The second research question analyses the laws and regulations concerning encryption, while the third research question examines the social aspects and contexts surrounding encryption. The fourth research question aims to synthesise the collected and analysed legal, social and empirical materials and data and propose recommendations and conclusions.

Encryption is admittedly a complex and complicated matter.[19] This report does not intend nor aspire to resolve all of the problems related to encryption and its regulation. It does not intend to produce a formal, detailed or full-blown encryption law or regulation. Its chief aims are to conduct exploratory and foundational research and to discern the fundamental principles and values of encryption with the participation and contribution of relevant stakeholders (i.e., the general public, businesses, and government). Such encryption principles are inspired and guided by the OECD's

[19] Organisaton for Economic Co-operation and Development, "Report on Background and Issues of Cryptography Policy".

Guidelines for Cryptographic Policy.[20] As such, identifying and setting out the relevant encryption principles and values can be reasonably achieved through systemic and well-grounded research and open consultation and dialogue with the relevant stakeholders. This report does delve into more complex and controversial topics such as key disclosure, lawful access, and third party assistance[21] with the specific aim of discerning and enunciating the core principles and values that apply in these situations. Focusing on fundamental legal principles and attendant technical and social values can serve as ideal starting points for constructive dialogue and deliberation among various stakeholders on more specific rules and regulations.

The primary purpose of this study then is to set out the fundamental principles and values of encryption in New Zealand. To manage the scope of the research, the report intentionally does not propose detailed rules and regulation as these are better dealt with and addressed in larger research and law reform efforts. Nevertheless, the research and its outcomes complement and inform related legislative and policy activities in the areas of search and surveillance and privacy laws.[22]

1.3 Methodology

There are certain elements and features that distinguish this study from previous attempts to examine the laws and policies on encryption. First, the research is interdisciplinary. While many studies have focused solely on the legal or technical or social aspects of encryption, this research is cross disciplinary in its approach. This report examines the legal, technical and social dimensions of encryption and critically analyses how they interact and influence each other. It bears noting that the legal, social and technical issues concerning encryption cannot be solved through technology alone. While the prospects of using quantum computers to break present encryption technologies is an intriguing notion, the practical uses of quantum computers are years away and, by that time, people will have to face another problem – quantum cryptography. A purely technical solution cannot work because technological advancements lead to a never-

[20] Organisaton for Economic Co-operation and Development, "Recommendation of the Council Concerning Guidelines for Cryptography Policy" (1997).
[21] United National Human Rights Council, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression"15-16.
[22] Law Commission, *Review of the Search and Surveillance Act 2012*; Office of the Privacy Commissoner, "Privacy law reform resources" <https://www.privacy.org.nz/the-privacy-act-and-codes/privacy-law-reform-resources/> accessed 13 July 2017.

ending arms race. Similarly, an exclusively legal answer to encryption without proper consideration of its technical aspects and social context is also problematic. Former Australian Prime Minister Malcolm Turnbull's much-quoted statement about encryption, that "The laws of mathematics are very commendable, but the only laws that applies in Australia is the law of Australia"[23] is akin to lawmakers seeking to repeal the laws of supply and demand. Technology laws and policies do not exist in a vacuum. Thus, they must be grounded on a proper understanding of the subject technologies as well as the norms and values of the relevant stakeholders using these technologies. Otherwise, such laws and policies may prove ineffective or their legitimacy will be questioned.

Second, the research is principles- and values-based. A principle is essentially the core or foundational basis, rule or quality of something. On its part, a value is "a conception, explicit or implicit, distinctive of an individual or characteristic of a group, of the desirable which influences the selection of available modes, means, and ends of action".[24] Basically, it concerns a person's or group's ideas or beliefs about what are desirable goals and behaviours.[25] This study specifically focuses on principles and values because they both serve as the underlying bases for determining and guiding people's perceptions and actions. One of the primary aims of the research is to determine the principles and values of three groups of stakeholders through empirical research.[26] In so doing, it is possible to ascertain what these principles and values are, how they relate to each other, and possibly find shared or similar principles and values that can be constructively built on by the various stakeholders.

Third, the study involves a multi-stakeholder, collaborative process. The research is unique in that it is purposely designed to solicit and encourage the participation of and input from various stakeholders. It is also meant to bring the relevant stakeholders to the table, hear their views, and see the world through their eyes. The rationale behind this approach is that any potential law or regulation on encryption will only be adopted or deemed legitimate if it genuinely considers and takes into account the values and concerns of all relevant stakeholders. Such future encryption laws and policies must be founded on the values and promote the interests of those who will be most impacted by them – the

[23] The Guardian, "New law would force Facebook and Google to give police access to encrypted messages" <https://www.theguardian.com/technology/2017/jul/14/new-law-would-force-facebook-and-google-to-give-police-access-to-encrypted-messages> accessed 15 July 2017.
[24] Clyde Kluckholm and others, "Values and Value-Orientations in the Theory of Action" 395.
[25] Steven Hitlin and Jane Piliavin, "Values: Reviving a Dormant Concept" 362.
[26] See Clyde Kluckhohn and others, "Values and Value-Orientations in the Theory of Action" 404-405.

general public, business, and government itself. Many prior attempts to examine and recommend approaches to encryption around the world have not been successful because they were carried out by and for the benefit of a single group of stakeholders and merely espouse their own position without sufficiently or practically addressing the concerns of other stakeholders. Any attempt to develop laws and policies on encryption must be based on consensus and willingness to compromise.

Finally, given that the study is research-based and led by academics, it may help resolve the impasse among the different public and private stakeholders about how to best address the legal, social and technical issues surrounding encryption. The researchers can act as impartial mediators, facilitators or translators among the general public, businesses, and government. The presence and participation of an independent party can assist with the constructive deliberation and discussion of seemingly intractable issues. Furthermore, as the research is undertaken through a scholarly and systematic process and grounded on legal and empirical data, the validity of the study's outcomes and recommendations is assured.

1.4 Significance

The study is highly significant to the stakeholders who are both the participants and intended audiences of the research: the general public, businesses, and government.

From this report, ordinary users, consumers and members of the general public can have access to information that helps them gain a better understanding and awareness of encryption and their rights and responsibilities concerning the security and safety of their computer systems, data and communications. Having an express statement of the principles and values that apply to encryption can also assist the general public feel more confident and empowered to take control of their online identities and digital privacy.

New Zealand businesses can benefit from the research outcomes. Technology and non-technology companies can take advantage of the greater legal certainty and stability that a statement of encryption principles and values offers. Such principles on encryption provide legal and technical reassurances to New Zealand businesses and international companies wishing to do business in the country about the security of their computers

systems and data (including employee and customer personal data).[27] Furthermore, by having explicit principles on encryption, technology companies, global manufacturers, international businesses, cryptographers and information security professionals can see New Zealand as a more favourable place for developing and offering innovative products and services.

The New Zealand Government can also derive much value from this study. Police, law enforcement officers, intelligence agencies and courts can benefit from understanding the express principles and values of encryption that they can apply and implement as they carry out their public duties. These encryption principles and values can assist government officials, institutions and agencies take decisions and actions that are reasonable and consistent with human rights and other fundamental values, and yet at the same time help advance public goals and interests.[28] Clearly identifying and setting out the applicable principles and values of encryption can undoubtedly help improve New Zealand's digital competency, capability and preparedness.[29]

1.5 Research methods

In order to fully examine the legal, technical and social dimensions of encryption, the study utilised an interdisciplinary, mixed-methods approach. For data collection and analysis, the researchers conducted: (a) doctrinal legal research on existing and proposed encryption-related laws and policies in New Zealand and other jurisdictions; (b) focus group interviews with representatives of the relevant stakeholders about their perceptions, opinions, attitudes and beliefs about encryption; (c) secondary research on encryption; and (d) qualitative content analysis and values analysis of the empirical data.

Empirical data on individual and collective values, opinions and beliefs of stakeholders about encryption was principally collected through focus group interviews that were conducted from March to June 2018 in three major cities in the country (Auckland, Hamilton and Wellington). The focus group participants represented three categories of stakeholders:

- the general public (ordinary users, consumer groups, and civil society organisations);

[27] See New Zealand's Cyber Security Strategy 2015 7.
[28] See New Zealand's Cyber Security Strategy 2015 7.
[29] See New Zealand's Cyber Security Strategy 2015 5; see New Zealand's Cyber Security Strategy 2019.

- business (technology and non-technology companies, industry associations, and information security professionals); and
- government (police and law enforcement officers, government departments and other branches of government).

Out of the 10 total focus groups held, four involved representatives from the business sector, three were held with officials from different government branches, and the remaining three were attended by people who comprised the general public. It is common to hold around three to four focus groups for each category or type of group or participants.[30] For this study, upon conducting the last focus group for each category of stakeholder, data saturation was reached because conducting additional focus groups would no longer reveal or produce new information that was not already observed in previous focus groups.[31]

The focus group participants were representatives of the three stakeholder categories specifically selected because they were interested in or affected by encryption.[32] Using purposive non-probability sampling, names were collated on the basis of the following criteria: (a) being a member of the general public, the business sector or government agency; (b) having a role relating to encryption (e.g., as a developer, user or regulator); (c) having experience dealing with the legal, technical or social issues surrounding encryption; and/or (d) having been involved in or being knowledgeable about significant cases involving encryption. An initial list was drawn up from the network of contacts available to the study's principal researchers. This list was then expanded after an intensive review of newspaper articles, conference schedules, organisational charts of companies that offer encryption services or information security consultancy, membership lists of civil society organisations and other special-interest groups dealing with encryption-related issues, university records of faculty and researchers in the field of encryption and cybersecurity, and relevant government agencies. From a database of over 250 potential participants, more than 50 agreed to join the study and attended the focus group discussions. Although quota sampling was not the aim, the final list of participants sought some representativeness along the variables of gender and ethnicity with 15% of

[30] Richard A. Krueger and Mary Anne Casey, *Focus Groups: A Practical Guide for Applied Research* 21.
[31] See Maggie Walter, *Social Research Methods* 113; see also Richard A. Krueger and Mary Anne Casey, *Focus Groups: A Practical Guide for Applied Research* 21.
[32] See Richard A. Krueger and Mary Anne Casey, *Focus Groups: A Practical Guide for Applied Research* 66.

the participants being female and 14% coming from different non-European ethnic groups.

The focus group interviews were an hour and a half long and were held either at mid-morning or mid-afternoon. Each participant was provided an electronic copy of the participant information sheet during the recruitment process as well as a printed copy to read before the start of the focus group. Focus group participants were also requested to sign a consent form that confirmed that, among others: their participation was voluntary; they could withdraw at any time until the commencement of analysis of the data; the information they provided may be used in future publications and presentations of the researchers; they would not be named or identified in any publications; and they agreed to the recording of the interviews.

The focus group interviews were conducted using an interview guide. The interview guide had a list of general topics to be discussed, but each focus group interview was adapted based on whether the focus group was composed of representatives from the general public, business or government in order to capture their distinct approaches or perspectives on encryption. Despite these modifications to the interview guide, all focus group participants were asked questions about four main topic areas: their knowledge of and experience with encryption; their understanding and views on existing or proposed encryption laws and policies (e.g., encryption backdoors); their opinions and reflections about specific, high-profile cases involving encryption such as the *Apple v FBI* case; and their perceptions, attitudes and beliefs about the principles and values associated with encryption.

A central part of the focus group interviews involved a group exercise on the principles and values of encryption. The focus group participants were given cards and on each card was printed a particular principle and value (e.g., Privacy). The participants were then asked as a group to rank the principles and values from most important to least important. In addition, participants were asked to explain the relationships between and among the principles and values. The groups spread the cards across the table and started to rank and organise them. As they ranked and ordered the cards, the participants were asked to explain what the specific principle and value meant to them and what was the reason for ranking or ordering them in that way. By doing it in this way, the focus group participants were able to express how they understood each principle and value and their

understandings or definitions would be open to further elaboration, discussion and even contestation within the group. Any similarities or differences in meanings and conceptions of the focus group participants about the principles and values of encryption provided not only rich qualitative data that could be analysed, but also allowed for constructive and revealing discussions among the participants. Furthermore, through the ranking exercise, focus group participants were able to visualise and reflect on the priority or importance they gave to each principle and value, as well as the connections and relations between them. The primary benefit of the group ranking exercise was that it provided qualitative data that served as an empirical basis from which the researchers could compare the differing meanings, prioritisation and organisation of the principles and values of encryption between and across the different categories of stakeholders (the general public, businesses and government). In this way, it was possible compare and contrast the positions and views of various stakeholders with each other and investigate the conflicts as well as possible correspondences between them.

All 10 focus group interviews were audio recorded and transcribed. The transcripts of the interviews were coded and analysed using thematic analysis. Thematic analysis entails finding and identifying themes in the collected data through the process of coding.[33] Coding is essentially the process of applying descriptive and conceptual labels and categories to segments or parts of the interview transcripts (e.g., a participant's answer to the question of whether and why he or she uses encryption) and then observing connections and relations that arise from these codes.[34] The codes used in the analysis included a priori codes (which were based on the key concepts or topics from the research questions, interview guide and literature review),[35] in vivo codes (the terms used by the participants themselves),[36] and inductive codes (those that emerged or arose from a higher level conceptual analysis of the coded data).[37] The researchers used the qualitative data analysis programme ATLAS.ti for coding and analysis.[38]

[33] Maggie Walter, *Social Research Methods* 398.
[34] Kathy Charmaz, *Constructing Grounded Theory* 43.
[35] Maggie Walter, *Social Research Methods* 324-325.
[36] Alan Bryman, *Social Research Methods* 573.
[37] Maggie Walter, *Social Research Methods* 325.
[38] Susanne Friese, *Qualitative Data Analysis with ATLAS.ti*; see also Maggie Walter, *Social Research Methods* 398.

1.6 Overview of report

The aim of this report is to make salient the various technical, legal and social principles and values related to encryption and examine the conflicts and correspondences between them. Part 2 focuses on the technical dimension of encryption. It explains how encryption works and what elements make up its underlying architecture. From the examination of how encryption is designed and used, certain key technical principles and rules can be distilled. These technical principles and rules are important considerations, not only with respect to how encryption is developed and use, but also how this technology can be regulated. Part 3 examines the laws on encryption. This part describes how, contrary to common belief, encryption is already subject to legal control. The laws that apply to encryption include those that concern export control, cybercrime, search and surveillance, and human rights. These laws constitute a tacit and implicit legal framework that has a significant influence on how encryption is developed, accessed and used. Part 4 sets out the principles and values of encryption and how they are perceived and understood by the three categories of stakeholders. Based on the empirical data collected from the focus group interviews, this part analyses the similarities and differences between how the various stakeholders prioritise or rank the principles and values. In addition, this part explores the relationships between the different principles and values and the possibility of finding connections between them, particularly in relation to trust. Part 5 concludes the report by providing a synthesis of the research findings and analysis and coming up with statements of the principles and values of encryption that should be considered when developing relevant laws and policies. This part also provides recommendations on general policy directions that such laws and policies can take.

Technologies of encryption

2.1 Significance of technical factors and dimensions

Encryption is a key technology in a connected, information-driven and technologically-based world. It is an essential element of computer and information security.[1] In most situations, it would be difficult to securely and privately create, store, communicate and process data without encryption.[2] Whether people are aware of it or not, encryption plays an integral role in their everyday lives.[3] When a person uses a credit card in a physical shop or online, utilises internet banking services, browses the Web, saves photos on his or her smartphone, sends a private message, or uses public services online (e.g., health and social services), these and many other common activities involve and rely on encryption.[4] With encryption so pervasive and underpinning many aspects of living in an information society, it is important for people (whether they be developers, users and regulators) to comprehend how this technology works.

While a technical understanding of encryption is very useful, this study goes further and examines the core principles and values that influence how encryption is developed, implemented and used by various actors and stakeholders. This principles- and values-based approach is what distinguishes this study from other law and policy research on encryption. A premise of this report is that encryption is not a mere tool that is a simple or easy target of control and regulation. Far from it, based on the concepts and existing literature in the field of science and technology studies (STS), it is argued that, as with any technology, encryption inherently embodies and enacts particular principles and values and follows and conforms to specific and defined rules. These principles, values

[1] Jason Andress, *The Basics of Information Security* 63.
[2] See Jason Andress, *The Basics of Information Security* 79; see also Bert-Jaap Koops, *The Crypto Controversy* 33.
[3] See RL Rivest, "Foreword" in Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography*.
[4] Hans Delfs and Helmut Knebl, *Introduction to Cryptography* ix.

and rules play a significant role in determining and shaping what encryption is, how it is used, and how it affects law and society. Analysing these underlying technical standards and protocols and the inner workings of encryption as expounded in the fields of computer science, mathematics and other related areas is a requisite step to getting a better grasp of this technology. Moreover, contrary to what some people believe,[5] aside from law, there are non-legal rules such as social norms and technical protocols that similarly and significantly apply to how encryption is accessed and used.

2.2 Meaning of encryption

2.2.1 TECHNOLOGY AND SCIENCE

Given that encryption is a relatively complex technology both theoretically and in practice,[6] it is difficult to come up with a single or definitive definition for it. The Oxford Dictionary defines encryption as "the process of converting information or data into a code, especially to prevent unauthorized access".[7] According to Levy, it involves "the use of secret codes and ciphers to scramble information so that it's worthless to anyone but the intended recipients".[8] Technology law scholars such as Koops describes it as the "process of making data inaccessible to unauthorized people".[9] Technically speaking, encryption is "the transformation of unencrypted data, called plaintext or cleartext, into its encrypted form, called ciphertext".[10] It is basically a "process of encoding messages".[11] The reverse process is called decryption, which is "the process of recovering the plaintext message from the ciphertext. The plaintext and ciphertext… [are] generically referred to as the message".[12] Synthesising and refining the above definitions, for the purposes of this

[5] Associated Press, "Australia plans law to force tech giants to decrypt messages" <https://apnews.com/621e0913072a4cb5a1a7f7338721b059/Australia-plans-law-to-force-tech-giants-to-decrypt-messages> accessed 15 July 2017.
[6] RL Rivest, "Foreword" in Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography*.
[7] "Encryption", Oxford Dictionary <https://en.oxforddictionaries.com/definition/encryption> accessed 25 July 2018.
[8] Steven Levy, *Crypto* 1.
[9] Bert-Jaap Koops, *The Crypto Controversy* 269 and 35.
[10] Jason Andress, *The Basics of Information Security* 63.
[11] Simon Singh, *The Code Book* x.
[12] Jason Andress, *The Basics of Information Security* 63.

study, encryption is *a technology that transforms information or data into ciphers or code for purposes of ensuring the confidentiality, integrity and authenticity of such data.*[13]

Encryption and cryptography are often used synonymously or interchangeably with each other.[14] However, while they are intimately connected, they remain distinct concepts. Cryptography is described as "the *science* of keeping secrets secret"[15] or "the *science* of keeping information secure".[16] Practiced mostly by cryptographers,[17] it has also been called "the *art* of secret writing"[18] or the "*art* of secret communication".[19] More specifically, it is "the *study* of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication".[20] Cryptography then is the science, art or practice of secure and secret storage, communication and processing of information. Encryption may be said to be "a subset of cryptography"[21] and refers to the technology and technical process itself rather than the wider cryptographic field of study or area of practice. Since the aim of this report is to examine the meaning and impact of encryption for different stakeholders (i.e., providers, users and regulators), the primary focus of the research is the *technology of encryption* rather than the science of cryptography. Of course, cryptography remains an integral concept and relevant research and materials on this subject are used to inform the analysis.

It is worth noting that cryptography has a flipside called cryptanalysis. Cryptanalysis is "the science of studying attacks against cryptographic schemes".[22] Carried out by people called cryptanalysts and other "attackers",[23] it is the "science of breaking through the encryption used to create the ciphertext".[24] More specifically, it is "the study of mathematical techniques for attempting to defeat cryptographic techniques,

---

[13] See Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 4 and 11-12 (It should be noted that while availability is not a primary objective of encryption itself, the application of encryption can affect whether a system can be made available or not).
[14] Jason Andress, *The Basics of Information Security* 63.
[15] Hans Delfs and Helmut Knebl, *Introduction to Cryptography* 1 (emphasis added).
[16] Jason Andress, *The Basics of Information Security* 63 (emphasis added).
[17] Jason Andress, *The Basics of Information Security* 63.
[18] Bert-Jaap Koops, *The Crypto Controversy* 33 (emphasis added).
[19] Simon Singh, *The Code Book* xi (emphasis added).
[20] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 4 (emphasis added).
[21] Jason Andress, *The Basics of Information Security* 63.
[22] Hans Delfs and Helmut Knebl, *Introduction to Cryptography* 4.
[23] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 15.
[24] Jason Andress, *The Basics of Information Security* 64.

and, more generally, information security services".[25] So while cryptography is about "the making of crypto systems",[26] cryptanalysis is concerned with "breaking a crypto system or an encrypted message".[27] Together, cryptography and cryptanalysis constitute the broader field of cryptology.[28] Cryptology is the "science that studies the making and breaking of crypto systems"[29] and is performed by cryptologists.[30]

2.2.2 PROCESS

As explained in the previous section, in its most basic form, encryption is a method that transforms information or data into ciphers or code in a way that only an authorised party can access the meaningful content of the information in order to preserve its confidentiality, integrity, and authenticity. Decryption is the reverse process of transforming encrypted information, such that the original, unencrypted information is obtained. The original, unencrypted information is referred to as the plaintext, while the information encrypted using a cipher is called a ciphertext.

The transformation of information is based on an encryption algorithm. Every encryption algorithm has at least two inputs and at least one output. The algorithm is given the plaintext and a key. The key is a unique[31] string of information such as a very large random number. Using the key, an encryption algorithm transforms the plaintext into an apparently random ciphertext, while a different key would transform the same plaintext into a new ciphertext, which bears no resemblance to the first ciphertext. In this way, many independent parties can use the same encryption algorithm because they can use different keys in order to produce different outputs. Similarly, a decryption algorithm takes at least two inputs and produces at least one output. Given the ciphertext and a key, the apparently random information is transformed into the original, meaningful information.

---

[25] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 15.
[26] Bert-Jaap Koops, *The Crypto Controversy* 35 and 269.
[27] Bert-Jaap Koops, *The Crypto Controversy* 269.
[28] Hans Delfs and Helmut Knebl, *Introduction to Cryptography* 4; see also Jason Andress, *The Basics of Information Security* 64.
[29] Bert-Jaap Koops, *The Crypto Controversy* 269; see also Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 15.
[30] Jason Andress, *The Basics of Information Security* 64.
[31] True global uniqueness is yet another mathematical subject.

2.2.3 KINDS OF ENCRYPTION

Non-technical people generally tend to conceive or talk about encryption as if it was a singular monolithic technology. However, there are several kinds of encryption. Knowing the various forms of encryption is important because each has and adheres to differing underlying principles, assumptions and rules that affect how it is developed, implemented and used.

The two basic forms of encryption are symmetric and asymmetric.[32] Symmetric key cryptography is a system where the encryption key and decryption key are the same.[33] When used for communications, the single key "must be shared between the sender and the receiver" through key exchange.[34] Symmetric key cryptography is used to protect the confidentiality rather than the integrity or authenticity of data.[35] Examples of symmetric key algorithms include AES, DES, Blowfish, RC4 and SEAL.[36] Symmetric key cryptography is a much older technology that has been used for millennia while asymmetric key cryptography is a more recent development.[37] Asymmetric key cryptography or public-key cryptography is a system where the encryption key and decryption key are different.[38] With this system, the public (encryption) and private (decryption) keys could be held by different parties, enabling a variety of asymmetric communication possibilities, including digital signatures and key exchange. Asymmetric-key encryption has the benefit over symmetric-key encryption of not having to deal with the problem of key exchange for two parties to connect or communicate since the parties' public keys that will be used for encrypting the data are readily or widely available.[39] Public key encryption can be used to protect not just the confidentiality, but also the integrity and authenticity of data. RSA, ElGamal, DSS and PGP are well known examples of asymmetric-key algorithms.[40]

With respect to *where* the encryption process takes place, there is client-side encryption, which is the process of encrypting information before sending it to another party without providing a decryption key. For example, users can upload their encrypted

---

[32] Jason Andress, *The Basics of Information Security* 69.
[33] Hans Delfs and Helmut Knebl, *Introduction to Cryptography*.
[34] Jason Andress, *The Basics of Information Security* 69-70.
[35] Jason Andress, *The Basics of Information Security* 70.
[36] Jason Andress, *The Basics of Information Security* 70-71.
[37] See Simon Singh, *The Code Book*.
[38] Hans Delfs and Helmut Knebl, *Introduction to Cryptography*.
[39] Jason Andress, *The Basics of Information Security* 72.
[40] Jason Andress, *The Basics of Information Security* 72.

data to a cloud storage provider using client-side encryption to prevent the service provider from accessing the data as meaningful information. The service provider may be able to obtain or copy the users' data but it would be unintelligible. On the other hand, end-to-end encryption is the process whereby two parties encrypt information before sending it to each other either directly or through a third-party service.[41] However, only the two parties have access to the decryption keys. For example, two parties could use end-to-end encryption to send messages to each other over a communications service. In this case, neither the service provider nor any other party would be able to access the meaningful information.

Homomorphic encryption is a variant of encryption where it is possible to perform computation on ciphertexts.[42] To illustrate, a homomorphic cryptosystem could have an algorithm which takes two ciphertexts and produces a third ciphertext, which when decrypted gives the same result as if the original plaintexts were added together. With homomorphic encryption, some party could perform a computation service on behalf of another without knowing any meaningful information about the inputs or outputs for their service. This type of encryption is particularly relevant to processed data or data in use. In most cases, save for the case of a simple data transfer, data has to be unencrypted in order for it to be meaningfully processed. Homomorphic encryption can potentially resolve the issues of maintaining the confidentiality and integrity of data while it is being processed or used, but, at the time of writing, it is still too computationally intensive to be practically implemented as a generic solution for widespread use. For example, it would take at least 15 minutes to encrypt 1 megabyte of plaintext homomorphically.

Deniable encryption is the use of encryption to deny the existence of some information. This typically involves some intended information, along with decoy information, which should remain confidential but which is not the intended information. In this case, two separate keys are used. Using this decoy information, a party can create some volume of ciphertexts filled with random information with the first key, and then replace some of the volume with encrypted decoy information using the first key. Because the encrypted information would be indistinguishable from random information, the party can also replace some of the remaining volume with the intended information,

---

[41] Andy Greenberg, "Whatsapp just switched on end-to-end encryption for hundreds of millions of users" <https://www.wired.com/2014/11/ whatsapp-encrypted-messaging/> accessed 26 July 2018.
[42] Craig Gentry, *A fully homomorphic encryption scheme* [thesis].

encrypted with the second key. Depending on the implementation, and the plausibility of the decoys, the party could plausibly deny the existence of the intended information.[43] Deniable encryption is useful for preserving the secrecy or confidentiality of the data.

2.2.4 STATES AND TYPES OF DATA

Whichever kind of encryption used, it principally applies to data (whether as information or communication). Data can be in one of three distinct states: data at rest, data in motion, and data in use. Data is said to be at rest when it is stored physically and not currently being accessed. Specifically, 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".[44] Encryption is the primary method for protecting the confidentiality and integrity of data at rest.[45] Because an adversary or an unauthorised party can potentially access copious amounts of data multiple times over a long period when such data is at rest, it is considered good security practice to use encryption particularly for sensitive information.[46]

Data can also be in motion. It is in motion when it is transferred or sent over any medium, channel, network or other means of communication. The data can travel "over a network of some variety. This might be over a closed [wide area network] WAN or [local access network] LAN, over a wireless network, over the [i]nternet, or in other ways".[47] Data is especially susceptible to interception, collection or interference when it is in transit over an insecure channel or a public network. Special care needs to be taken to ensure that an eavesdropper or adversary cannot decipher, corrupt or spoof data between the parties.[48] The confidentiality, integrity and authenticity of such data and communications can be preserved in two ways: "by encrypting the data itself… or by protecting the entire connection".[49]

---

[43] Rein Canetti and others, "Deniable encryption".
[44] Jason Andress, *The Basics of Information Security* 75.
[45] Jason Andress, *The Basics of Information Security* 75.
[46] Stilgherrian, "Encrypting data at rest is vital, but it's just not happening" <https://www.zdnet.com/article/encrypting-data-at-rest-is-vital-but-its-just-not-happening/> accessed 17 August 2018.
[47] Jason Andress, *The Basics of Information Security* 76-77.
[48] IICS WG, "Interagency report on status of international cybersecurity standardization for the internet of things (IoT)".
[49] Jason Andress, *The Basics of Information Security* 77.

Finally, data can be in use. In this state, the data is currently being accessed, processed or put through some form of computation or operation. Protecting data while it is in use poses inevitable and unavoidable technical issues. Unless the data is homomorphically encrypted or is using some other form of secure computation, it is often the case that the data must be decrypted upon entering the system that is performing the computation. As Andress explains, "Although we can use encryption to protect data while it is stored or moving across a network, we are somewhat limited in our ability to protect data while it is being used by those who legitimately have access to it" [50] since the data has to be in plaintext. Some hardware can use memory encryption, whereby the system memory (RAM) is encrypted, but the data is decrypted upon arriving in the hardware's internal memory (cache).[51]

It is worth noting that the three data states are based on a technical categorisation of data. This can be compared with the classification of specific types of data under the Convention of Cybercrime and relevant national laws. Cybercrime investigations normally deal with the following data types: subscriber data, traffic data, metadata, content data, stored data, and communications.[52] While the states of data are distinct from the types of data, there is much overlap between them and it is useful to keep both categories of data in mind when analysing the legal, technical and social effects of encryption.

2.3 Encryption architectures

In terms of implementation and use, encryption can range from a simple manual system of secret writing to a full-blown computational cryptosystem. But whether its implementation is basic or complex, encryption adheres to an underlying architecture. This architecture can be conceived as being composed of different layers that build on top of each other. This structure comprises three main layers: (1) cryptographic primitives (including encryption algorithms) at the base; (2) cryptographic protocols in the middle; and (3) cryptosystems at the highest level. Focusing on the architecture of encryption is important because the design and structure of any technology inherently determines and controls how it is applied and used. Furthermore, as Lessig convincingly argues in his

[50] Jason Andress, *The Basics of Information Security* 78.
[51] Stephen Weis, "Protecting data in-use from firmware and physical attacks".
[52] See Council of Europe, Explanatory Report to the Convention on Cybercrime, para 136.

seminal book *Code and Other Laws of Cyberspace*, architecture is law or has normative or law-like effects.[53]

2.3.1 ENCRYPTION ALGORITHMS AND PRIMITIVES

At the core of any encryption system is the encryption algorithm. As discussed previously, it is "[t]he specifics of the process used to encrypt the plaintext or decrypt the" ciphertext.[54] Cryptographic algorithms generally use a key, or multiple keys, in order to encrypt or decrypt the message.[55] Encryption algorithms belong to a class of technologies called cryptographic primitives, which are the "basic building blocks" of encryption.[56] As Delfs and Knebl explain, "[e]ncryption and decryption algorithms, cryptographic hash functions, and pseudorandom generators [etc.]… are the basic building blocks… for solving problems involving secrecy, authentication or data integrity".[57] Primitives therefore serve as "basic cryptographic tools" that are "used to provide information security".[58]

The architecture of encryption or cryptosystems is generally composed of a mix of various primitives. As building blocks, primitives are modular and can be used and "applied in various ways and with various inputs".[59] A combination or amalgamation of various primitives is often necessary because "[i]n many cases a single building block is not sufficient to solve the given problem: different primitives must be combined".[60] Encryption primitives "need to be combined to meet various information security objectives. Which primitives are most effective for a given objective will be determined by [their] basic properties".[61] Each primitive is distinct and functions and interacts with others in unique yet complementary ways. The presence and use of primitives underscore the fact that encryption is heterogeneous. Knowing which cryptographic primitive is used in an encryption protocol or system is crucial to understanding how it was developed, how it operates, who exercises control over it, and who has access to the encrypted information.

---

[53] See Lawrence Lessig, *Code 2.0*.
[54] Jason Andress, *The Basics of Information Security* 64.
[55] Jason Andress, *The Basics of Information Security* 64.
[56] Hans Delfs and Helmut Knebl, *Introduction to Cryptography* 5.
[57] Hans Delfs and Helmut Knebl, *Introduction to Cryptography* 5.
[58] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 4.
[59] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 5.
[60] Hans Delfs and Helmut Knebl, *Introduction to Cryptography* 5.
[61] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 5.

2.3.1.1 Block and stream ciphers

Block ciphers are an encryption and decryption algorithm that use symmetric keys, which operate on message blocks of a fixed length. Each plaintext is encrypted to a ciphertext of the same length, and each ciphertext is decrypted to a plaintext of the same length. Block ciphers preserve the information security objectives of confidentiality and authenticity. On their own, these algorithms can only be used to encrypt and decrypt a single block securely. However, a mode of operation can be used to extend the block cipher in order to protect the confidentiality and authenticity across many blocks using a single key.[62]

Block ciphers are typically used as a building block for encryption systems and other cryptographic primitives. These include cryptographic hash functions, cryptographically secure pseudorandom number generators (PRNG), and stream ciphers. Block ciphers can also be used for Message Authentication Codes (MACs), which are similar to digital signatures but use symmetric keys.

Stream ciphers enable individual bits (in the case of a binary system, a single 0 (zero) or 1 (one)) of a message to be encoded in sequence using symmetric keys. Every plaintext bit of a message is combined with a cipher bit from a keystream allowing for messages of arbitrary length to be encrypted.[63] Keystreams can either be generated independently from the message (synchronous) or can be self-generated by some previous number of ciphertext bits (self-synchronizing). Stream ciphers are generally used to protect the confidentiality and integrity of data.

2.3.1.2 Hash functions

A cryptographic hash function transforms some information of an arbitrary length, into a hash (also known as a digest) of a fixed length.[64] Cryptographic hash functions have the following properties and characteristics. The same input information should always result in the same output hash. Further, any change to the input, no matter how small (even a single bit), should result in a completely different hash, which has no apparent correlation with the first hash. For example, an email is hashed. If a single letter is changed in the email, a different hash will be produced from this email compared to the

[62] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography*.
[63] Matthew Robshaw, "Stream ciphers".
[64] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography*.

original email. It should be infeasible to transform the hash back into the original information and the only viable method should be through hashing every possible input message and comparing these to the hash in question. This is so because a hash is meant to work one way (from plaintext to hash), unlike standard encryption where the transformation of plaintext to ciphertext can be reversed with the use of the appropriate key. Also, given one specific piece of information, it should be infeasible to find some other information which shares the same hash value. In any event, it should be infeasible to find any two different pieces of information that share the same hash value (known as a hash collision). Finally, the process of computing the hash should be relatively fast and efficient.

Cryptographic hash functions have a variety of uses such as assuring some information security objectives or providing an asymmetry of computational effort between two parties. For example, hash functions can verify the integrity of data. Cryptographic hashing can be used to determine whether some data has changed (whether at rest or in transit) by comparing the current hash to a hash at an earlier date or the hash before and after transit. In these cases, it is assumed that the first hash was not modified by an adversary. To prevent this, the hashes would need to be communicated over a secure channel. Hashes are also used for verifying passwords. A naive service can verify the identity of users by comparing the input password with a password stored locally in plaintext. However, this set-up is not secure because an adversary may obtain some or all of these passwords if he or she is able to access the data at rest. A more secure service would instead store the hash of a user's password and compare this with the hash of the input password. Cryptographic hash functions can also be implemented to verify proof-of-work. For instance, the challenging party can provide some random information and require that a responding party concatenates or links information onto the end such that the resulting hash has some easily-checked property. The responding party may have to hash and evaluate many different concatenated inputs, while the challenging party only has to hash and evaluate once to verify correctness. In this way, the responding party must perform more work than the challenging party.[65] This is the same process used in blockchains such as Bitcoin.

[65] Cynthia Dwork and Moni Naor, "Pricing via processing or combatting junk mail".

There are security issues with hash functions. Even if the only viable method to reverse a hash is through a brute-force search of all possible inputs, if the length of the input is small (for example, a password), it is possible to store the hashes for all inputs of a given length. A rainbow table, which is a table that efficiently stores these precomputed hashes, can be utilised to more efficiency and quickly resolve the search for the decryption key.[66] To counter this problem, a salt can be used. Salts are large, unique and random but known values which are concatenated onto a small input. Services can prevent a rainbow table attack on passwords by first salting and then hashing a user's password and storing both the hash and the salt. If every salt is unique, then an adversary would have to build a rainbow table for every individual password. This is more computationally and time consuming and would make an exhaustive search of the password impractical.[67]

2.3.1.3 Key exchange

Key exchange is a process whereby two parties obtain a shared symmetric key or each other's encryption keys.[68] Key exchange systems should have the following characteristics. The process must occur without any third party or other entity being able to obtain or derive the keys. The key exchange must be possible even if (a) an adversary is monitoring the communication or (b) an adversary can pretend to be the other party and alter the messages sent between parties (also known as a man-in-the-middle attack).

Key exchange is critical for modern encryption as it allows an end-to-end encryption channel to be established even on an insecure medium such as the internet without either party having to exchange private information beforehand. Key exchange can also be used to achieve forward secrecy. By exchanging new, ephemeral keys at the start of every communication sessions, two parties can ensure that even if any particular session is compromised, no other sessions are affected. Even if an adversary successfully pretends to be one of the parties and is able to perform a key exchange in place of the true party, only future sessions will be compromised since every previous session uses a different and unique key.[69]

---

[66] Philippe Oechslin, "Making a faster cryptanalytic time-memory trade- off".
[67] Poul-Henning Kamp and others, "Linkedin password leak: Salt their hide".
[68] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography*.
[69] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography*.

2.3.1.4 Digital signatures

Digital signatures ensure the authenticity, non-repudiation and integrity of data.[70] There are three basic steps for generating and using a verifiable digital signature. First, the encryption key should be kept private, but the decryption key can be made public. Then, a cryptographically secure hash of the message can be generated. Afterwards, the hash is encrypted with the private key.[71] The receiving party or other parties can then decrypt the hash using the public key and compare it with their own independently generated hash for the message. If the encryption key remains private and secure, then only the signing party could have produced the signature.

Situations that require ensuring the authenticity, non-repudiation and integrity of the data can take advantage of digital signatures. Digital signatures can be used to verify the identity of the creator of some software or the originator of a financial transaction. Further, they can be used to ensure the integrity of the data or message and that these were not altered or tampered with.

2.3.1.5 Blockchain

Blockchain technology that is used in cryptocurrencies such as bitcoin is based on encryption. A blockchain is basically a series of message blocks, each of which also contains a cryptographic hash of the previous message block.[72] By applying a proof-of-work requirement to every hash,[73] it becomes increasingly difficult to tamper with previous blocks in the chain as the hash of each subsequent block will also have to be modified and a proof-of-work applied to each block before the chain can be considered again.[74] By applying a number of additional systems, including message signing and a distributed majority consensus, a blockchain can enable public transaction ledgers (such as currency or digital identity management) with varying degrees of protection for their integrity, authentication and non-repudiation.

---

[70] Hans Delfs and Helmut Knebl, *Introduction to Cryptography* 3-4.
[71] Anna Lysyanskaya, *Signature schemes and applications to cryptographic protocol design*.
[72] It should be noted that blockchain is a particular form of distributed ledger technology. Not all distributed ledger technologies use blockchain.
[73] Some blockchains use proof-of-stake rather than proof-of-work.
[74] Satoshi Nakamoto, "Bitcoin: A peer-to-peer electronic cash system".

2.3.2 ENCRYPTION PROTOCOLS

Building on and combining primitives, encryption or cryptographic protocols constitute the second or middle layer of the encryption architecture. An encryption protocol is described as "a distributed algorithm defined by a sequence of steps precisely specifying the actions required of two or more entities to achieve a specific security objective".[75] Cryptographers and computer scientists agree that "[p]rotocols play a major role in cryptography and are essential in meeting cryptographic goals…. Encryption schemes, digital signatures, hash functions, and random number generation are among the primitives which may be utilized to build a protocol".[76]

What distinguishes a protocol from a basic encryption algorithm or a mere combination of primitives is that it involves at least two parties. For "a well-defined series of steps" that combine different primitives to be considered a protocol "at least two people are required to complete the task.".[77]

2.3.3 CRYPTOSYSTEMS

An encryption system or cryptosystem is the end of result of a combination and interoperation of varied and multiple cryptographic algorithms, primitives and protocols. A cryptosystem is a "general term… [that refers to] a set of cryptographic primitives used to provide information security services. Most often the term is used in conjunction with primitives providing confidentiality, i.e., encryption".[78] Essentially, it is the implementation of various algorithms, primitives and protocols that are needed to encrypt information and communications.[79] This generally includes elements of key generation, encryption and decryption algorithms, and "all possible keys, plaintexts, and ciphertexts".[80] In contrast to protocols, an encryption system is "a more general term encompassing protocols, algorithms (specifying the steps followed by a single entity), and

---

[75] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 33.
[76] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 34; Hans Delfs and Helmut Knebl, *Introduction to Cryptography* 5.
[77] Hans Delfs and Helmut Knebl, *Introduction to Cryptography* 5.
[78] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 15 (but cryptosystems are also used to protect the integrity and authenticity of data).
[79] Bert-Jaap Koops, *The Crypto Controversy* 269.
[80] Jason Andress, *The Basics of Information Security* 64; see also Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography*; see also Hans Delfs and Helmut Knebl, *Introduction to Cryptography* 1.

non-cryptographic techniques (e.g., hardware protection and procedural controls) to achieve specific security objectives".[81]

2.4 Key technical principles and rules

In the preceding discussion of the architecture of encryption, it is plain to see that the ways and manner by which encryption is designed, implemented and used subscribes and conforms to particular standards and objectives. An examination of encryption would only be complete if one recognises the significance and influence of these technical principles, values and rules.

2.4.1 INFORMATION SECURITY

Encryption is intrinsically connected to information security.[82] As it is currently practiced, cybersecurity would be difficult to ensure without encryption. This is why encryption shares some of the primary objectives of information security.[83] While information security focuses on the confidentiality, integrity and *availability* of computer data, systems and networks, encryption (as a necessary element of information security) is particularly concerned with the confidentiality, integrity and *authenticity* of data (whether in the form information or communications).[84] Encryption involves processes and "techniques for keeping information secret, for determining that information has not been tampered with, and for determining who authored [the] pieces of information".[85] As with information security, the "fundamental goal of cryptography is to adequately address these… areas in both theory and practice. Cryptography is about the prevention and detection of… [unauthorised] and other malicious activities".[86]

---

[81] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 34.
[82] See Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 2.
[83] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* xxiv and 14; Hans Delfs and Helmut Knebl, *Introduction to Cryptography* 2; see Bert-Jaap Koops, *The Crypto Controversy* 38-39 (who includes non-repudiation); see also Yulia Cherdantseva and Jeremy Hilton, "A reference model of information assurance & security".
[84] See Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* xxiv and 14; see also Hans Delfs and Helmut Knebl, *Introduction to Cryptography* 2; see also Bert-Jaap Koops, *The Crypto Controversy* 38-39 (who includes non-repudiation); see also Yulia Cherdantseva and Jeremy Hilton, "A reference model of information assurance & security".
[85] RL Rivest, "Foreword" in Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* xxi.
[86] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 4.

2.4.1.1 Confidentiality

Confidentiality has always been a primary goal of encryption. As Delfs and Knebl explain, "[t]he fundamental and classical task of cryptography is to provide *confidentiality* by *encryption methods*" [87] This basically means "keep[ing] the plaintext secret from eavesdroppers".[88] The practical aim is to ensure that information is not revealed to unauthorised persons or entities (i.e., "keep the content of information from all but those authorized to have it").[89] Confidentiality has also been described as "the property that data are kept secret from people who are not authorized to access them".[90] In the relation to communications, confidentiality requires a degree of anonymity whereby traffic data and other "information about who communicates with whom, when, how often, and from where is kept secret".[91]

In this study, the term confidentiality also covers the related and interconnected concepts of secrecy and privacy.[92] Secrecy and privacy are undoubtedly complex terms, but in the context of technical processes and systems, they can be viewed simply as keeping information unknown or unseen by others[93] and not disclosing personal data to others.[94]

2.4.1.2 Integrity

Integrity is the second objective of encryption. Integrity is "the property that data are unaltered and complete".[95] Encryption ensures that data remains unchanged by adversaries while at rest, in transit and in use.[96] Also known as data integrity, it concerns "the unauthorized alteration of data. To assure data integrity, one must have the ability to

---

[87] Hans Delfs and Helmut Knebl, *Introduction to Cryptography* 1.
[88] Hans Delfs and Helmut Knebl, *Introduction to Cryptography* 4.
[89] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 4; see also Jason Andress, *The Basics of Information Security* __.
[90] Bert-Jaap Koops, *The Crypto Controversy* 269 and 24 (notion of "exclusiveness").
[91] Bert-Jaap Koops, *The Crypto Controversy* 24.
[92] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 4.
[93] See "Secret", Oxford Dictionary <https://en.oxforddictionaries.com/definition/secret> accessed 7 August 2018.
[94] See "Private", Oxford Dictionary <https://en.oxforddictionaries.com/definition/private> accessed 7 August 2018; see also Daniel Weitzner and others, "Information accountability".
[95] Bert-Jaap Koops, *The Crypto Controversy* 269 and 24.
[96] Jason Andress, *The Basics of Information Security*.

detect data manipulation by unauthorized parties. Data manipulation includes such things as insertion, deletion, and substitution".[97]

Integrity also applies to messages and other forms of communication. An essential aspect of preserving the integrity of messages is providing the receiver with a means to "check whether the message was modified during transmission, either accidentally or deliberately. No one should be able to substitute a false message for the original message, or for parts of it".[98]

2.4.1.3 Authenticity

The third and final objective of encryption is authenticity.[99] Authenticity is "the property that a message was indeed sent by the purported sender",[100] whereas authentication is the corresponding process to achieve it. Authentication is generally concerned with identification and "applies to both entities and [the] information itself".[101] It permits the authorised parties to identify the author, sender and receiver of information. It also helps "guarantee that entities are who they claim to be, or that information has not been manipulated by unauthorized parties".[102] Authentication is crucial when communicating in online environments and across digital networks because "[t]wo parties entering into a communication should [be able] identify each other. Information delivered over a channel should be authenticated as to origin, date of origin, data content, time sent, etc.".[103] As a practical matter, "[t]he receiver of a message should be able to verify its origin. No one should be able to send a message to Bob and pretend to be Alice (data origin authentication). When initiating a communication, Alice and Bob should be able to identify each other (entity authentication)".[104]

Authentication thus involves two interrelated processes of entity authentication (identification) and data origin authentication (message authentication).[105] Entity authentication "assures one party (through acquisition of corroborative evidence) of both the identity of a second party involved, and that the second was active at the time the

---

[97] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 4.
[98] Hans Delfs and Helmut Knebl, *Introduction to Cryptography* 2 and 4.
[99] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 24.
[100] Bert-Jaap Koops, *The Crypto Controversy* 269.
[101] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 4.
[102] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 24.
[103] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 4.
[104] Hans Delfs and Helmut Knebl, *Introduction to Cryptography* 2.
[105] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 4 and 24-25.

evidence was created or acquired".[106] On its part, data origin authentication "provide[s] to one party which receives a message assurance (through corroborative evidence) of the identity of the party which originated the message".[107] Building on these two processes, authentication can also be used to achieve other "specific objectives [including] access control… data integrity, non-repudiation, and key authentication".[108] It should be noted that data origin authentication intrinsically involves data integrity because "if a message is modified [then] the source has [been effectively] changed".[109]

Some authors consider non-repudiation to be an additional and discrete objective of encryption.[110] Non-repudiation is "the property of a message which ensures that the sender or receiver cannot deny having sent or received it".[111] For the purposes of this report, however, it is deemed included in authentication because it is intimately linked to and is basically the natural consequence or inverse effect of the latter. In addition to non-repudiation (where adversaries should not be able to masquerade as the legitimate author, sender or receiver of information),[112] another objective covered by authenticity is accountability, which requires that it should not be possible for any party to deny that they performed their action during a transaction.[113]

Aside from the above three primary information security objectives, other ancillary processes and secondary goals of encryption include: authorisation, validation, access control, certification, timestamping, witnessing, receipt, confirmation, ownership, anonymity, revocation and auditability.[114] It should be noted that, together with confidentiality and integrity, availability is considered the third side of the information security triad. Availability requires that data must be accessible when needed and it should not be possible for an adversary to deny access to information.[115] Encryption though is concerned with and directly affects the secrecy, integrity and identification of data, but not its availability. In any event, encryption does play a vital role in realising the

---

[106] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 24.
[107] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 25.
[108] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 24.
[109] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 4; see also Hans Delfs and Helmut Knebl, *Introduction to Cryptography* 3 and 4)
[110] See Bert-Jaap Koops, *The Crypto Controversy* 38-39
[111] Bert-Jaap Koops, *The Crypto Controversy* 270 and 24; see also Hans Delfs and Helmut Knebl, *Introduction to Cryptography* 3.
[112] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 4.
[113] Adrian McCullagh and William Caelli, "Non-repudiation in the digital environment".
[114] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 3 and 4.
[115] Jason Andress, *The Basics of Information Security*.

overarching goal of information security. This means that encryption does protect the objective of availability albeit indirectly.

2.4.2 PRIMACY OF KEYS

2.4.2.1 Secrecy

Another paramount principle of encryption is the imperative of protecting the secrecy and inviolability of keys. For cryptologists and information security professionals, it is axiomatic that keys are kept secret and safe from unauthorised parties even though the design of the encryption algorithms, protocols and systems are publicly known.[116] It is "[a] fundamental premise in cryptography… that the sets… are public knowledge. When two parties wish to communicate securely using an encryption scheme, the only thing that they keep secret is the particular key pair" [117] – specifically, the private (decryption) key. This means that "the security of the system should reside only in the key chosen".[118] The key therefore is the linchpin of any encryption process or system. The implication is that "the objectives of information security [must] rely solely on digital information itself" – the key.[119]

The secrecy of keys is the second principle of Auguste Kerckhoffs' classic statement of the six principles of cryptography.[120] Based on this principle, a cryptosystem should be secure despite the fact that everything about it (save for the keys) is public knowledge.[121] It is also assumed that that adversaries "have complete access to the communication channel".[122] According to Delfs and Knebl,

> A fundamental assumption in cryptanalysis was first stated by A. Kerckhoffs in the nineteenth century. It is usually referred to as *Kerckhoffs' Principle*. It states that the adversary knows all the details of the cryptosystem, including its algorithms and their implementations. According to this principle, the security of a cryptosystem must be based entirely on the secret keys.[123]

Andress further explains that "cryptographic algorithms should be robust enough that, even though someone may know every bit of the system with the exception of the key

[116] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 14.
[117] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 14.
[118] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 14.
[119] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 3.
[120] Auguste Kerckhoffs, "La cryptographic militaire".
[121] Auguste Kerckhoffs, "La cryptographic militaire".
[122] Hans Delfs and Helmut Knebl, *Introduction to Cryptography* 4.
[123] Hans Delfs and Helmut Knebl, *Introduction to Cryptography* 4.

itself, he or she should still not be able to break the encryption". It considered "one of the underlying principles for many modern cryptographic systems".[124]

Kerckhoff's principles remain a good source and authority for precepts and rules about encryption even though some of them may appear at first to be outdated in the context of modern, computer-based and digital cryptography.[125] These principles are still relevant today and many cryptologists and information security professionals continue to refer and adhere to them.[126]

2.4.2.2 Inviolability

The inviolability or intrinsic security of the keys themselves depends on the notions of randomness and key length. As stated by Delfs and Knebl, "randomness is the key to security".[127] This so because "[r]andomness and the security of cryptographic schemes are closely related. There is no security without randomness. An encryption method provides secrecy only if the ciphertexts appear random to the adversary".[128]

Randomness is important for making an encryption algorithm's outputs unpredictable. Most of the software and hardware used today are deterministic, that is, they will produce the same outputs given the same inputs. A pseudorandom number generator will produce an apparently random sequence of numbers given an input seed number. But, if someone knows the generator algorithm and the seed number, they can consistently reproduce the same sequence of numbers.[129] True randomness must come from inputs outside of a deterministic system such as temperature, human typing patterns, radioactive decay or the quantum properties of light rays.[130] In practice though,

> Truly random functions cannot be implemented, nor even perfectly approximated in practice. Therefore, a proof in the random oracle model can never be a complete security proof. The hash functions used in practice are constructed to be good approximations to the ideal of random functions.[131]

Despite this limitation, randomness remains a crucial criterion for key generation and encryption as a whole. According to Levy, "those who devised cryptosystems had a

---

[124] Jason Andress, *The Basics of Information Security* 69.
[125] Auguste Kerckhoffs, "La cryptographic militaire"; see also Jason Andress, *The Basics of Information Security* 69.
[126] Jason Andress, *The Basics of Information Security* 69.
[127] Hans Delfs and Helmut Knebl, *Introduction to Cryptography* x.
[128] Hans Delfs and Helmut Knebl, *Introduction to Cryptography* 8.
[129] Jeffrey Schiller and Steve Crocker, "Randomness requirements for security".
[130] Bruno Sanguinetti and others, "Quantum random number generation on a mobile phone".
[131] Hans Delfs and Helmut Knebl, *Introduction to Cryptography* 9.

standard to live up to: randomness. The idea was to create ciphertext that appeared to be as close to a random string of characters as possible".[132]

Together with randomness, key length is an integral attribute of the inviolability of keys. The length of a key is determined by its keyspace, which is "the range of all possible values for the key".[133] The rule of thumb is: a longer key produces a greater number of possible key combinations and thus makes it harder to guess or break. An exhaustive search or brute force attack is a common attack against encryption whereby an attacker goes "through all the possible combinations of settings" or keys to see which one the parties used.[134] Therefore, "the number of keys (i.e., the size of the key space) should be large enough to make this approach [i.e., testing all possible keys] computationally infeasible".[135] It is considered good practice as well that an encryption or cryptosystem should be designed or implemented in such a way that "the best approach to breaking it is through exhaustive search of the key space. The key space must then be large enough to make an exhaustive search completely infeasible".[136]

2.4.3 OPENNESS OF SYSTEMS

A corollary to Kerckhoffs' second principle is the necessity for the architecture of a cryptosystem to be open, transparent and accessible to the public. Requiring openness seems counterintuitive but there is a rationale for this non-secretive approach to the design of cryptosystems. When developing encryption or implementing it in software, hardware or as part of a service, there are two general approaches: a proprietary and closed model versus an open source model. A proprietary model appears to benefit from the notion of security through obscurity. This is the belief that keeping the design and implementation of a system secret would make it more difficult for an adversary to understand and attack it. However, under the open source model, by openly disclosing how the system works, it can be more thoroughly analysed by many other parties (including third party experts like information security professionals and ethical

[132] Steven Levy, *Crypto* 12.
[133] Jason Andress, *The Basics of Information Security* 64.
[134] Steven Levy, *Crypto* 11; Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 14.
[135] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 14.
[136] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 44.

hackers).[137] As a result, the system benefits from quicker and continuous improvements from a wider and more diverse group of actors and thus becomes more robust and secure. A proprietary and closed system can be made more robust but it may take more time and effort.

Information security professionals generally agree that security through obscurity is neither a wise nor viable approach.[138] In contrast, the open source model to security testing is widely accepted and is encapsulated in Linus' Law, which states that "given enough eyeballs, all bugs are shallow".[139] The value of openness is closely associated with the four software freedoms advanced by free and open source software (FOSS), which are the freedoms to (1) study, (2) copy, (3) modify and (4) distribute copies of a computer program.[140] Underlying these freedoms is the indispensability of having access to the source code without which the freedoms to study and modify would be rendered nugatory. The logic behind the open source model is that, if the security of a system is not compromised after lengthy analysis and use by the public, it can hold a level of presumed security that cannot be matched by an obscure system that has not been robustly tested.

The openness, transparency and accessibility of an information system is particularly germane to encryption because users need to rely on the system with their private and sensitive data and communications, and trust that it is actually secure. For instance, users need to know whether the system has a known bug or an intentional backdoor. The underlying architecture of encryption ideally needs to be publicly accessible so that its security can be audited, vetted and verified. When it comes to information security, it is considered good practice to refrain from using, depending on or trusting a closed or secret system.

Openness is directly concerned with the issue of trust. Some people believe that the only completely secure encryption system is one where you "trust no one". They believe that one should not trust anyone else with the knowledge or possession of your keys or encrypted data.[141] Of course, trust can also exist outside of this extreme position so long as "all parties… have confidence that certain objectives associated with information

---

[137] See Jason Andress, *The Basics of Information Security* 69.
[138] See Jaap-Henk Hoepman and Bart Jacobs, "Increased security through open source" 2.
[139] Eric Raymond, *The Cathedral and the Bazaar*.
[140] Free Software Foundation, "What is free software?" <https://www.gnu.org/philosophy/free-sw.en.html> accessed 9 August 2018; see also Michael Dizon, *A Socio-Legal Study of Hacking* 31.
[141] Rohit Khare and Adam Rifkin, "Weaving a web of trust".

security have been met".[142] For example, encryption or cryptosystems can still be trustworthy and secure in cases where the desire to share keys and data is mutually beneficial, when the cryptosystem is open source and audited, or when the number of key-holders is as small as possible.

2.4.4 ADVERSARIAL NATURE

Another notable attribute of encryption is its inherently adversarial nature.[143] This arises from fact that, like Janus, the field of cryptology is composed of the dualities of: cryptography vs cryptanalysis, codemaking vs codebreaking, encipher vs decipher, and ciphertext vs plaintext. The history of encryption can be characterised as a race between those who seeks to preserve the secrecy and security of their information and communications and those who set out to crack it. It is a "centuries-old battle between codemakers and codebreakers".[144] The security of encryption therefore demands constantly anticipating and guarding against possible attacks. As Rivest states, "cryptographers must also consider all the ways an adversary might try to gain by breaking the rules or violating expectations".[145]

Aside from the sender or the receiver, an adversary is among the usual dramatis personae of encryption. In relation to a cryptosystem, parties are portrayed as either friends or adversaries.[146] Adversaries are individuals or entities who attempt to prevent the parties from securely and secretly communicating by discovering meaningful information, corrupting information in transit, masquerading as a legitimate party, or denying communications between parties.[147] An adversary (who can either be passive or active) is also referred to as an enemy, attacker or eavesdropper.[148]

---

[142] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 2.
[143] RL Rivest, "Foreword" in Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* xxi.
[144] Simon Singh, *The Code Book* ix.
[145] RL Rivest, "Foreword" in Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* xxi.
[146] Hans Delfs and Helmut Knebl, *Introduction to Cryptography* 6.
[147] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography*.
[148] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 13 and 14; see also Hans Delfs and Helmut Knebl, *Introduction to Cryptography* 1.

2.4.5 RESISTANCE TO ATTACKS

Due to the adversarial nature of encryption, attacks on it are expected and commonplace.[149] For example, "attacks may be directed against the underlying cryptographic algorithms [or primitives] or against the implementation of the algorithms and protocol. There may also be attacks against a protocol itself".[150] The confidentiality, integrity and authenticity of the encrypted data may be compromised by attacks to "recover the plaintext (or parts of the plaintext) from the ciphertext, substitute parts of the original message or forge digital signatures". [151]

Since the primary objective of encryption is information security, it must be able to resists various forms of attacks. For attacks against encryption algorithms, the main "objective… is to systematically recover plaintext from ciphertext, or even more drastically, to deduce the decryption key".[152] Ciphertext-only attack, known-plaintext attack and chosen-ciphertext attack are some of the ways to defeat an algorithm.[153] Encryption is considered "breakable if a third party, without prior knowledge of the key pair… can systematically recover plaintext from corresponding ciphertext within some appropriate time frame".[154] On the other hand, an encryption protocol is broken when "it fails to meet the goals for which it was intended, in a manner whereby an adversary gains advantage not by breaking an underlying primitive such as an encryption algorithm directly, but by manipulating the protocol or mechanism itself".[155] Many successful attacks on encryption such as known-key attack, replay, impersonation, dictionary, forward search and interleaving attack are a result of protocol failure.[156]

Attacks may also either be passive or active.[157] "A passive attack is one where the adversary only monitors the communication channel… [and] only threatens

---

[149] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 41.
[150] Hans Delfs and Helmut Knebl, *Introduction to Cryptography* 4; see also Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 41.
[151] Hans Delfs and Helmut Knebl, *Introduction to Cryptography* 4.
[152] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 41.
[153] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 41-42; see also Hans Delfs and Helmut Knebl, *Introduction to Cryptography* 4 and 6.
[154] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 14.
[155] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 34.
[156] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 42 and 47.
[157] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 41; see also Hans Delfs and Helmut Knebl, *Introduction to Cryptography* 4-5.

confidentiality of data".[158] With an active attack, "the adversary attempts to delete, add, or in some other way alter the transmission on the channel. An active attacker threatens data integrity and authentication as well as confidentiality".[159]

2.4.6 APPROPRIATE LEVEL OF SECURITY

The ability of encryption or a cryptosystem to resist different forms and magnitudes of attacks goes into the level of security that it provides. There are several ways to evaluate the level of security offered by an encryption primitive, protocol or system.[160]

2.4.6.1 Unconditional security – Perfect secrecy

At the highest level is unconditional security.[161] An unconditionally secure system means that it cannot be broken even if the adversary has unlimited computational resource.[162] Unconditional security is closely related to Claude Shannon's notion of perfect secrecy.[163] There is perfect secrecy when "if and only if an adversary cannot distinguish between two plaintexts, even if her computing resources are unlimited".[164] More specifically, "the uncertainty in the plaintext, after observing the ciphertext, must be equal to the a priori uncertainty about the plaintext – observation of the ciphertext provides no information whatsoever to an adversary".[165] Also known as semantic security, "[a] perfectly secret cipher perfectly resists all ciphertext-only attacks. An adversary gets no information at all about the plaintext, even if his [or her] resources in terms of computing power and time are unlimited".[166] A cryptosystem is semantically secure if, when given only a ciphertext, it is not feasible to extract any information besides the length of the ciphertext. For all intents and purposes, a ciphertext in a semantically secure

[158] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 41.
[159] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 41.
[160] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 42.
[161] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 42.
[162] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 42.
[163] Hans Delfs and Helmut Knebl, *Introduction to Cryptography* 8 (also known as ciphertext indistinguishability or semantic security).
[164] Hans Delfs and Helmut Knebl, *Introduction to Cryptography* 8.
[165] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 42.
[166] Hans Delfs and Helmut Knebl, *Introduction to Cryptography* 7.

cryptosystem will appear to be random content.[167] Perfect secrecy though requires that "the key [used must] be at least as long as the message".[168]

A one-time pad is an example of a "symmetric-key encryption scheme [that is] an unconditionally secure encryption algorithm".[169] While offering perfect secrecy, a one-time pad is extremely hard and impractical to use. Delfs and Knebl explain, "[u]nfortunately, Vernam's one-time pad and all perfectly secret ciphers are usually impractical. It is not practical in most situations to generate and handle truly random bit sequences of sufficient length as required for perfect secrecy".[170] Perfect secrecy is all but impossible to implement with symmetric or public key encryption since not one but a pair of keys are generated and used. Moreover, "[p]ublic-key encryption schemes cannot be unconditionally secure since, given a ciphertext… the plaintext can in principle be recovered by encrypting all possible plaintexts until [the ciphertext] is obtained".[171] Both in theory and in practice, most forms or implementations of encryption generally do "not offer perfect secrecy, and each ciphertext character observed decreases the theoretical uncertainty in the plaintext and the encryption key".[172]

2.4.6.2 Computational or provable security – Impracticability and infeasibility of attacks

Since the ideals of unconditional security and perfect secrecy are impractical and difficult to achieve, the next best level of security to aspire for is computational or provable security. Computation security is concerned with "the amount of computational effort required, by the best currently-known methods, to defeat a system".[173] An encryption or cryptosystem is deemed computationally secure "if the perceived level of computation required to defeat it (using the best attack known) exceeds, by a comfortable margin, the computational resources of the hypothesized adversary".[174] For example, "[t]he security of a public-key cryptosystem is based on the hardness of some

---

[167] Oded Goldreich, *Foundations of Cryptography*.
[168] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 42.
[169] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 42; see also Steven Levy, *Crypto* 12; Hans Delfs and Helmut Knebl, *Introduction to Cryptography* 7-10 (also called Vernam's one-time pad).
[170] Hans Delfs and Helmut Knebl, *Introduction to Cryptography* 7.
[171] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 43.
[172] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 42-43.
[173] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 43.
[174] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 43.

computational problem (there is no efficient algorithm for solving the problem)".[175] Computationally security is generally measured by work factor. Basically, the level of protection provided "is defined by an upper bound on the amount of work necessary to defeat" the system.[176] More specifically, work factor is "the minimum amount of work (measured in appropriate units such as elementary operations or clock cycles) required to compute the private key… given the public key…, or, in the case of symmetric-key schemes, to determine the secret key".[177]

One of the theoretical underpinnings of computational security is the notion of provable security.[178] Provable security is about using "mathematical proofs [to] show that the cryptosystem resists certain types of attacks".[179] In this way, an encryption or cryptosystem is regarded as provably secure "if the difficulty of defeating it can be shown to be essentially as difficult as solving a well-known and supposedly difficult (typically number-theoretic) problem, such as integer factorization or the computation of discrete logarithms".[180]

It should be noted though that, unlike unconditional security, computationally or provably secure systems do not provide absolute security. They are breakable. This is so because provable security is based on and subject to certain assumptions and conditions.[181] For example, common and widely used public-key systems can only at best achieve provable security because "[t]here are no mathematical proofs for the hardness of the computational problems used in public-key systems. Therefore, security proofs for public-key methods are always conditional: they depend on the validity of the underlying assumption".[182] In fact, "[t]he security proofs for public-key systems are always conditional and depend on *(*widely believed, but unproven) assumptions".[183]

Nonetheless, for cryptographers, computational or provable security offers a sufficient level of security for encryption or cryptosystems.[184] It complies with Kerckhoff's first principle of encryption.[185] As Delfs and Knebl explain,

---

[175] Hans Delfs and Helmut Knebl, *Introduction to Cryptography* 7.
[176] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 5.
[177] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 44.
[178] See Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 43 (on complexity-theoretic security).
[179] Hans Delfs and Helmut Knebl, *Introduction to Cryptography* 6.
[180] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 43.
[181] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 43.
[182] Hans Delfs and Helmut Knebl, *Introduction to Cryptography* 7.
[183] Hans Delfs and Helmut Knebl, *Introduction to Cryptography* 10.
[184] Hans Delfs and Helmut Knebl, *Introduction to Cryptography* 6.

> More recent approaches to provable security therefore abandon the ideal of perfect secrecy and the (unrealistic) assumption of unbounded computing power. The computational complexity of algorithms is taken into account. Only attacks that might be *feasible* in practice are considered. "Feasible" means that the attack can be performed by an efficient algorithm.[186]

Computational or provable security is good enough because possible or potential attacks are impractical or infeasible. The feasibility of an attack vis-à-vis the security of the system is typically assessed based on the time needed to break the system. In most cases, "[a]n appropriate time frame will be a function of the useful lifespan of the data being protected".[187] To illustrate, even though public-key encryption does not offer unconditional security or perfect secrecy, it is still widely used and relied on because the work factor required to defeat it is measured in years. If the number of years is "sufficiently large", then it is "for all practical purposes… a secure system".[188] In fact, "[t]o date no public-key system has been found where one can prove a sufficiently large lower bound on the work factor…. The best that is possible to date is to rely on the following as a basis for security".[189] Computational or provable security are said to provide an acceptable level of practical security.[190] Because of the difficulties of breaking the encryption itself, attackers normally focus on and exploit other aspects of an information system to gain access. For instance, attackers could target users to get them to disclose their passwords through a phishing attack. While encryption can offer an acceptable level of security, the security of a system can be compromised in various other ways.

2.4.7 CONVENIENCE, COMPATIBILITY AND OTHER PRINCIPLES

While Kerckhoff's second principle on the secrecy of keys is the one most referred to by cryptographers and information security professionals, his other principles on encryption remain relevant today. Kerckhoff's first principle is that the encryption system "should be, if not theoretically unbreakable, unbreakable in practice".[191] This is pertinent

---

[185] Auguste Kerckhoffs, "La cryptographic militaire".
[186] Hans Delfs and Helmut Knebl, *Introduction to Cryptography* 7.
[187] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 14.
[188] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 44.
[189] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 44.
[190] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 43.
[191] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 14; see also Jason Andress, *The Basics of Information Security* 68-69.

to the preceding topic on the appropriate level of security and the adequacy of computationally or provably secure encryption. As discussed above, the second principle on the primacy of keys is a fundamental tenet of encryption.[192] The third principle states that "the key should be [memorable] without notes and easily changed".[193] This goes into the importance of keeping keys (including passwords) secret by not writing them down or keeping a tangible record. Furthermore, the principle requires that the system should make it easy to change or modify keys. There is a practical reason behind this: "if some particular encryption/decryption transformation [ciphertext] is revealed then one does not have to redesign the entire scheme but simply change the key. It is sound cryptographic practice to change the key… frequently".[194]

Kerckhoff's fourth principle concerns the robustness, compatibility and interoperability of a cryptosystem that it can be used to send private and secure messages over an insecure channel, public network, or widely used medium. It says, "the cryptogram should be transmissible by telegraph".[195] Principle five is a rule on the physical attributes of the system itself and the need for mobility, practicality and usability. It states that "the encryption apparatus should be portable and operable by a single person".[196] The sixth principle is about convenience and ease of use. It provides that "the system should be easy, requiring neither the knowledge of a long list of rules nor mental strain".[197]

2.5 Impact and implications on law and society

It is evident that the technologies of encryption (especially its architecture and underlying principles, values and rules) act as parameters or guidelines that influence how the technology is developed, accessed and used. For example, businesses are creating systems that use client-side encryption so that only users possess the keys to unlock their data. Moreover, these technical principles and rules have a significant impact and broader

[192] Jason Andress, *The Basics of Information Security* 69.
[193] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 14; see also Jason Andress, *The Basics of Information Security* 68-69.
[194] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 12.
[195] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 14; see also Jason Andress, *The Basics of Information Security* 68-69.
[196] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 14; see also Jason Andress, *The Basics of Information Security* 68-69.
[197] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 14; see also Jason Andress, *The Basics of Information Security* 68-69.

implications on law and society, including how encryption is or ought to be regulated. For instance, whether as a technology, science or process, modern-day encryption at its core is mathematics, particularly when it comes to encryption algorithms and primitives. Mathematics per se is not normally the object or concern of law and regulation. Of course, the specific application, implementation and use of mathematics (e.g., as embodied in software or other technologies) can be the subject of regulation and there have been significant attempts by state actors to control encryption.[198]

As seen above, there are different kinds of encryption and they work in varied ways and involve multiple parties. From the perspective of law and policy, this means that encryption is not a simple and easy target of regulation because it involves a complex and dynamic network of diverse actors using specific technologies. For instance, the development and use of end-to-end encryption hinders the ability of law enforcement to gain access to communications even though interception or wiretapping is authorised under telecommunications laws.[199] However, in relation to homomorphic encryption, the meaningful processing of encrypted data remains impractical, which means that data has to be decrypted for processing. The consequence of this technical limitation is that data in use is ordinarily processed in plaintext and can thus be subject to a lawful access request. The use of deniable encryption may negate the effectivity of current and proposed laws that authorise the forced disclosure of password and keys since the data sought may be obfuscated through technical means.

The architecture of encryption also poses regulatory complications. It is essential to know which layer of encryption is involved and what specific primitive is used since they all have distinct objectives and outputs and function in various ways. Block and stream ciphers work differently from hash functions and digital signatures. Ciphers protect the information security objectives of confidentiality and integrity, hash functions primarily concern data integrity, and digital signatures deal with integrity and authenticity.

Because the specific technical principles and rules examined above go to the very essence of encryption, they have the greatest legal impact and broadest social implications. Encryption is integral to preserving information security and many common and widely used technologies and systems rely on it. This means that any attempt to

[198] See Steven Levy, *Crypto*.
[199] See Telecommunications (Interception Capability and Security) Act 2013.

completely ban the development and use of encryption would be impracticable and impossible to justify whether from a cybersecurity or a law and policy standpoint.[200] Furthermore, encryption is purposefully designed and used to realise the all-important information security objectives of confidentiality, integrity and authenticity. The general rule is that encryption should guard against all of these security threats and risks. From the perspective of information security, a backdoor would be considered a mechanism that intentionally compromises the security of encryption.[201] If encryption is designed to allow even an authorised party to undermine the security of the system, it can be assumed that eventually an adversary will be able to defeat the system using the same mechanism.[202] This means that a legislative proposal for mandatory backdoors for law enforcement and other purportedly legitimate purposes would effectively undercut and nullify the very nature and purpose of encryption to the point that for all intents and purposes it would not deserve to be called by that name. Encryption with a backdoor does not provide sufficient security and privacy protection.

The principle of the primacy of keys is another significant regulatory consideration. Both the secrecy and inviolability of keys are essential for the security of encryption and any related system that implements it. For law enforcement, the keys can be the principal target of a criminal investigation since whoever holds the keys has access to and control over the encrypted data or communication. But proposals for mandatory key escrow or similar systems whereby users' keys are stored with a trusted third party potentially contravene and weaken vital encryption principles. With regard to the inviolability of keys, developers and users need to use encryption with a sufficient key length to ensure its robustness. Prohibitions or restrictions against the use of strong cryptography are problematic.

The principle of openness requires that the underlying source code and architecture of encryption must be publicly accessible, transparent and auditable. Openness ensures that the encryption is actually safe and secure to use and it inspires trust among users. For these reasons, whether it is a de facto or de jure standard, the design and implementation of encryption should be open to scrutiny by the public.

---

[200] See Bert-Jaap Koops, *The Crypto Controversy* 131.
[201] Nicole Perlroth, Jeff Larson and Scott Shane, "NSA able to foil basic safeguards of privacy on web".
[202] Ronald Rivest, "The case against regulating encryption technology".

The adversarial nature of encryption has significant legal and social implications as well. Historically, encryption has always been a cat-and-mouse game between codemaking (cryptography) and codebreaking (cryptanalysis). In light of this, innovation in cybersecurity should be prioritised and continuous improvements to strengthen encryption should be encourage since these are essential to stay ahead of this never-ending technological competition and leapfrogging. Corollary to this, caution should be exercised when imposing or enforcing legal rules and obligations that have the unintended consequence of impeding, inhibiting and dissuading developers and providers from keeping their products and systems safe and resilient against known and future attacks.

An important takeaway from the examination of the levels of security of encryption is that, aside from one-time pads that are difficult and not widely used, the notion of encryption as unbreakable locks is more myth than reality. Based on the concepts of computational and provable security, most encryption or cryptosystems that are in use today are technically breakable. It is not a question of if but when they will be defeated. The upshot of this is, rather than lamenting the seeming infeasibility of deciphering encrypted data and communications, the time and resources of public and private actors alike would be better spent on innovating and producing new and cutting-edge technologies and techniques (e.g., quantum computing and post-quantum cryptography)[203] that improve the security of one's own and a friendly party's system and/or break or weaken those of adversaries.

The technologies of encryption have an unmistakable influence on law and society. But the converse is also true. Legal principles and social values similarly affect how encryption is developed, accessed and used. The interactions and conflicts between and among the technical, legal and social principles and values of encryption are further examined in the following parts of this report.

[203] Hans Delfs and Helmut Knebl, *Introduction to Cryptography* 10.

Laws of encryption

3.1 Applicable laws

There is a common belief that, aside from export control rules, encryption is largely unregulated in New Zealand. This is the perception as well with respect to most jurisdictions around the world.[1] This sentiment is unsurprising given that both public and private actors normally believe that new or emerging technologies are not subject to law and regulation at the initial stages of their development and before their widespread adoption, dissemination and use.[2] There is a persistent notion that existing laws do not or should not apply to novel technologies. This has been the case in relation to the internet, peer-to-peer file sharing, 3D printing, bitcoin and other technological innovations.[3] To illustrate, early writings about the internet likened it to a lawless place like the Wild West in the United States that was in a state of anarchy.[4] But research has shown that, like other information technologies, the internet was never immune to existing laws and other modes or regulation.[5] In fact, rather than being a chaotic space, the internet was subject to its own internal and external forms of control from the very start.[6] Early generations of internet users were guided by netiquette and other rules of acceptable behaviour and their online activities and actions were susceptible to internal techno-social sanctions or external real-world laws.[7] The internet was far from being a place without law and order.

The same can be said about encryption. While it is true that there are technically no special laws that explicitly or directly regulate encryption in New Zealand, in fact,

---

[1] See Nathan Saper, "International Cryptography Regulation and the Global Information Economy".
[2] See Llewellyn Joseph Gibbons, "No Regulation, Government Regulation, or Self-regulation".
[3] See David Johnson and David Post, "Law and Borders: The Rise of the Law in Cyberspace" (1996) 48 Stanford Law Review 1367.
[4] See David Johnson and David Post, "Law and Borders: The Rise of the Law in Cyberspace" (1996) 48 Stanford Law Review 1367.
[5] See Jack Goldsmith and Tim Wu, *Who Controls the Internet?: Illusions of a Borderless World*.
[6] See Lawrence Lessig, *Code and Other Laws of Cyberspace*.
[7] See Jack Goldsmith, "Regulation of the Internet: Three Persistent Fallacies".

there already exists a network of laws, regulations and rules that apply to and determine how encryption is accessed and used in the country. These laws and policies and their resulting intended and unintended effects and outcomes constitute a tacit and implicit framework that, to a certain and significant degree, controls and governs encryption.

This part of the study explains what these laws are and how they apply to and impact the development, implementation and availability of encryption. The discussion focuses primarily on New Zealand legislation and jurisprudence specifically those concerning criminal procedure and investigations including the search, seizure and surveillance of computers and data. A significant part of the analysis centres on the Search and Surveillance Act 2012. However, the overarching structure of the analysis is guided by the Convention on Cybercrime and pertinent human rights laws. This is so because the Convention on Cybercrime is considered the most influential and authoritative international legal regime on the substantive and procedural rules concerning crimes and other activities involving computers, computer data and systems. While New Zealand is not a signatory to the Convention, the country's cybercrime laws and policies are clearly inspired by and closely adhere to the Convention. As such, a discussion of the underlying policies and relevant articles of the Convention would be useful to understanding the equivalent legal rules in New Zealand on access to and use of encrypted data, communications, services and devices. In a similar vein, reference to and guidance from human rights laws and principles are necessary because they provide safeguards and protections that check, limit and counterbalance the investigatory powers available to law enforcement when investigating crimes.

3.2 Export control laws

Export control rules on dual-use goods and technologies are the main laws that expressly and specifically apply to encryption.[8] Dual-use goods and technologies are goods and technologies developed for commercial purposes but are capable of being used either as a military component or for the development or production of military systems.[9] Encryption is an example of dual-use technology.

[8] See Nathan Saper, "International Cryptography Regulation and the Global Information Economy" 677.
[9] MFAT, "Trading weapons and controlled chemicals: Which goods are controlled?" <mfat.govt.nz>.

The Wassenaar Arrangement is but one of several international instruments that require the implementation of export controls.[10] It arose out of a similar export control regime that governed the transfer of arms and dual-use technologies and had the specific aim of restricting transfers between the East and the West during the Cold War.[11] With the fall of the Soviet Union, the East/West focus was no longer appropriate and a more international export control regime was needed. The Wassenaar Arrangement was established in 1996 to contribute to international security and stability by promoting transparency and responsibility in transfers of conventional arms and dual-use technologies between states,[12] specifically by restricting transfers to "states of concern".[13] The Wassenaar Arrangement has been implemented domestically through Customs Export Prohibition Orders (CEPO).[14] Section 56 of the Customs and Excise Act 1996 authorised the Governor-General to prepare and publish such orders. The CEPOs allow for the publication of the New Zealand Strategic Goods List (NZSGL), which details the technologies whose export is restricted.[15] Following the full implementation of the Customs and Excise Act 2018,[16] authorisation to prepare and publish such orders are via sections 96 and 97.

As originally enacted, the wording of the Customs and Excise Act 1996 meant that export restrictions only applied to the tangible form of the good.[17] However, following the passing of the Films, Videos, and Publications Classification Amendment Act 2005 and the Customs and Excise Amendment Act 2007, the definitions of various words were changed so that this loophole no longer operated. Moreover, since CEPO 2008, the orders have explicitly referred to the fact that the electronic publication version of the good is included. In the Customs and Excise Act 2018, sections 96 and 97 specifically

---

[10] The others being the Missile Technology Control Regime; the Australia Group; and the Nuclear Suppliers Group. New Zealand is also a party to the Arms Trade Treaty. See MFAT "Trading weapons and controlled chemicals" <mfat.govt.nz>.
[11] The Wassenaar Arrangement, "Origins" <Wassenaar.org>.
[12] Wassenaar Arrangement Secretariat "Public Documents, Vol. 1 – Founding Documents" (WA-DOC (17) PUB 001, February 2017) at 4.
[13] Daryl Kimball, "The Wassenaar Arrangement at a Glance" <https://www.armscontrol.org/factsheets/wassenaar > accessed 22 August 2019.
[14] Currently, the Customs Export Prohibition Order 2017, which will be revoked at the close of 31st December 2018.
[15] Currently, MFAT "New Zealand Strategic Goods List" (October 2017).
[16] See Customs and Excise Act 2018, s 2.
[17] See R Amies and G Woollaston *Electronic Business and Technology Law (NZ)* (online looseleaf ed, LexisNexis NZ Limited) at [6.7.3].

define "goods" to include documents that are not otherwise goods and "document" is given a wide definition in section 5 of the 2018 Act.

The current 2017 version of the NZSGL effectively mirrors the Wassenaar Arrangement, which specifies that if the encryption product meets all of the following then it is not subject to export control: (a) generally available to the public by being sold, without restriction, from stock at retail selling points; (b) the cryptographic functionality cannot easily be changed by the user; (c) designed for installation by the user without further substantial support by the supplier; and (d) not used. Details of compliance with the above must be available to the appropriate authority so that they may ascertain that compliance.

Many everyday goods and services employ encryption technologies that are exempt from the Wassenaar Arrangement. For example, copy-protection mechanism for video streaming sites like Netflix, virtual private networks (VPNs), secure protocols (HTTPS), email encryption, end-to-end encryption apps such as WhatsApp, and digital rights management (DRM) on DVD players and e-books. Copy-protection measures use encryption and are implemented by copyright holders to prevent or inhibit the infringement of copyright in a work.[18] The only other statute to govern encryption specifically, the Copyright Act 1994, does so only insofar as it excuses a person from having committed an offence if a copy-protection mechanism is circumvented for the purposes of undertaking encryption research.[19] To make a device available that circumvents copy-protection mechanisms can be an offence.[20]

It is worth noting that the Wassenaar Arrangement and applicable New Zealand regulations only apply to the export of encryption.[21] There are no specific restrictions on the importation of encryption technologies into the country. This means that persons based in the country are generally free to access and use encryption technologies from abroad including widely used free and open source software that utilise encryption such as Signal and VeraCrypt. Because many encryption technologies are freely and publicly available online, access to and availability of encryption for domestic use is harder for governments to control.

---

[18] Copyright Act 1994, s 226.
[19] Copyright Act 1994, s 226E.
[20] Copyright Act 1994, ss 226E and 226A.
[21] See Nathan Saper, "International Cryptography Regulation and the Global Information Economy" 678.

3.3 Cybercrime laws

Aside from the act of importation, the development, possession and use of encryption is also generally not regulated or prohibited. The most relevant statutory provision in this case is section 251 of the Crimes Act 1961,[22] which is similar to Article 6 of the Convention on Cybercrime on the cybercrime of misuse of devices.[23] Under the Crimes Act, it is illegal for a person to make, sell, distribute or possess software or other information for committing a cybercrime such as unauthorised access.[24] The term software can cover many forms of modern encryption technologies. The law specifically states that it is illegal to provide "any software or other information that would enable another person to access a computer system without authorisation"[25] for either of the following reasons: (1) "the sole or principal use of which he or she knows to be the commission of an offence" or (2) "that he or she promotes as being useful for the commission of an offence (whether or not he or she also promotes it as being useful for any other purpose), knowing or being reckless as to whether it will be used for the commission of an offence".[26]

Encryption can be used to facilitate or hide criminal activities. However, it is only a crime if the sole or principal purpose of encryption is to commit an offence. Since the primary purposes of encryption are to preserve the confidentiality, integrity and authenticity of data, then 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 to commit illegal acts when a crime under section 251 is committed. This view is supported by the drafters of the Convention on Cybercrime who explain that the crime of misuse of devices is only committed in cases where the software "are objectively designed, or adapted, primarily for the purpose of committing an offence. This alone will usually exclude dual-use devices" (i.e., those can be used for both legitimate and illicit purposes).[27] For there to be a crime, "there must be the specific (i.e., direct) intent that the device is used for the purpose of committing" an offence.[28] Therefore, unless an encryption technology is primarily or specifically designed or promoted for the

[22] Crimes Act 1961, s 251.
[23] Convention on Cybercrime, art 6.
[24] Crimes Act 1961, s 251.
[25] Crimes Act 1961, s 251(1).
[26] Crimes Act 1961, s 251(1).
[27] Council of Europe, Explanatory Report to the Convention on Cybercrime, para 73.
[28] Council of Europe, Explanatory Report to the Convention on Cybercrime, para 76.

commission of a crime, people are generally free to develop, possess and use encryption without restrictions.

3.4 Law enforcement powers and measures

An examination of encryption-related laws would normally focus exclusively on export control laws discussed above. But they merely represent the tip of the proverbial iceberg. There are other relevant laws that have a profound impact on how encryption is developed, accessed and used. Law enforcement powers and measures make up a significant part of the body of legal rules that apply to encryption. They are highly pertinent to encryption because these are the very same rules that are utilised to gain lawful access to encrypted data, communications and devices by law enforcement. These procedural rules and investigatory powers mainly operate underneath the surface because they do not expressly refer to or mention encryption. The aim of this section is to make explicit the criminal procedure rules that actually albeit tacitly regulate encryption.

Encryption is generally impacted by the principle of lawful access. Lawful access entails that law enforcement officers including those from government regulatory agencies should have access to encrypted data if the proper process is followed to authorise such access. Such authorisation comes, typically, via search warrants and other investigatory procedures. New Zealand law enforcement officers already have powers and measures available to them that facilitate access to encrypted data. Aside from the police, law enforcement officers at regulatory agencies (i.e., public agencies granted powers to ensure compliance with regulatory regimes) are conferred search powers via their governing statute. For example, New Zealand Customs Officers are conferred search powers via the Customs and Excise Act 2018, Wine Officers via the Wine Act 2003, and Tax Commissioners via the Tax Administration Act 1994. There are over seventy such governing statutes.[29]

The Search and Surveillance Act represents a consolidation of New Zealand's search and surveillance framework into a singular statute. It outlines five investigatory regimes and contains a number of procedural provisions in Part Four that apply to, and frame, search, surveillance, and inspection powers generally. The purpose of the Search and Surveillance Act is to "facilitate the monitoring of compliance with the law and the

[29] See Law Commission, *Review of the Search and Surveillance Act 2012* (NZLC IP40, 2016) para 1.11.

investigation and prosecution of offences in a manner consistent with human rights values".[30]

It should be noted that the law enforcement powers and measures discussed below under the Search and Surveillance Act resemble the procedural rules and powers specifically provided for in the Convention on Cybercrime. The aim of the Convention on Cybercrime is to adapt

> traditional procedural measures, such as search and seizure, to the new technological environment. Additionally, new measures have been created… in order to ensure that traditional measures of collection, such as search and seizure, remain effective in the volatile technological environment.[31]

Similarly, the stated purpose of the Search and Surveillance Act is to modernise "the law of search, seizure, and surveillance to take into account advances in technologies and to regulate the use of those technologies".[32] Viewed in this light, the powers, procedures and measures in the Convention on Cybercrime and the Search and Surveillance Act embody and represent the current international and national approach to combating crime in a digital environment.

3.4.1 SEARCH AND SEIZURE

3.4.1.1 Grounds and scope

A law enforcement officer's search powers may be exercisable without a warrant, exercisable only with a warrant, or be a mixture of warranted and warrantless, depending on what the governing statute specifies. For example, a Fisheries Officer does not need a warrant to search any premise or thing if they believe on reasonable grounds that an offence against the Fisheries Act 1996 is being or has been committed and that evidential material will be found.[33] Alternatively, Wine Officers, operating under the Wine Act 2003,[34] and Tax Commissioners operating under the Tax Administration Act 1994,[35] may search any premise other than a dwelling house or marae without a warrant. To

[30] Search and Surveillance Act 2012, s 5.
[31] Council of Europe, Explanatory Report to the Convention on Cybercrime, para 134.
[32] Search and Surveillance Act 2012, s 5(a).
[33] Fisheries Act 1996, s 199A; see also, *Wikitera v Ministry for Primary Industries* [2018] NZCA 195.
[34] See Wine Act 2003, ss 62 and 63.
[35] See Tax Administration Act 1994, s 16.

search a dwelling house or marae a warrant is required.[36] The Police also have several warrantless powers of search available in certain situations.[37]

In the absence of provisions specifying when a warrantless search can be undertaken, the search of a place, vehicle or thing by a law enforcement officer should only take place after a warrant has been issued.[38] To obtain a search warrant, and to legitimately carry out a warrantless search, a law enforcement officer is required, in general, to satisfy two elements. First, that an offence against the relevant statute is being, has been, or will be committed, and, second, that the place or thing to be searched will result in evidential material being found.

The relevant statute against which an offence is, has been, or will be committed is, of course, the governing statute from which the law enforcement officers derive their search powers. As the Police enforce a broad range of statutes – such as the Crimes Act 1961 and the Misuse of Drugs Act 1975 – they are an exception to this and may enforce offences arising under a broad range of statutes.[39]

The law enforcement officer's governing statute specifies what threshold/s must be met for each of these elements to be considered satisfied. Some statutes require the same threshold be met for both elements. For example, the Films, Videos, and Publications Classification Act 1993,[40] the Animal Welfare Act 1999,[41] and the Fisheries Act 1996,[42] all require that the regulatory officer have "reasonable grounds to believe" that both elements are met. Others, such as the Search and Surveillance Act,[43] the National Animal Identification and Tracing Act 2012,[44] and the Immigration Act 2009,[45] specify that the first threshold is met if the officer has "reasonable grounds to suspect" and the second is met if the officer has "reasonable grounds to believe".

"Reasonable grounds to believe" is a higher threshold than "reasonable grounds to suspect".[46] However, neither phrase is defined in any statute. Rather, these phrases have

---

[36] The Wine Act 2003 also requires that a constable be present; see Wine Act 2003, s 66(3).
[37] See Search and Surveillance Act 2012, ss 7-29.
[38] *Adams on Criminal Law,* at [SS6.01].
[39] Search and Surveillance Act 2012, s 6(a); see also *Adams on Criminal Law,* at [SS6.03].
[40] Films, Videos, and Publications Classification Act 1993, ss 109, 109A, and 109B.
[41] Animal Welfare Act 1999, s 131.
[42] Fisheries Act 1996, s 199A.
[43] Search and Surveillance Act 2012, s 6.
[44] National Animal Identification and Tracing Act 2012, s 29.
[45] Immigration Act 2009, s 293A.
[46] Jacinda Funnell, *Response to Select Committee Questions raised on 13 March 2017* (New Zealand Customs Service, 15 March 2017) at [24].

been left to case law for interpretation as the circumstances have allowed. The following summaries of these phrases are taken from the New Zealand Customs Service because they are orientated towards searches of electronic devices. However, they are reflected more generally in the commentaries concerning the Search and Surveillance Act.[47]

> "Reasonable suspicion" means that a Customs officer has to have a particularised and objective basis for suspecting the person is committing an offence against [an] Act and that searching the e-device is a reasonable action in the circumstances to confirm or eliminate that suspicion.
>
> "Reasonable belief" … means that in light of all the surrounding facts, and circumstances, which are, known or which reasonably should be known, to the Customs officer at the time, that the Customs officer reasonably believes, under those facts and circumstances, that the e-device contains evidence of an offence against [an] Act."[48]

According to Young, Trendle and Mahoney, "[t]he distinction between the two lies in the strength of the conclusion reached, with belief requiring a higher threshold than suspicion".[49] While reasonable suspicion "requires more than idle speculation, but need amount to no more than an apprehension with some evidential basis that the state of affairs may exist", reasonable belief means

> the judicial officer issuing a warrant had to be satisfied that the state of affairs alleged by the applicant actually exists. That does not mean proof of the state of affairs is required; there must be an objective and credible basis for thinking a search will turn up the items identified in the warrant…. There must be more than surmise or suspicion that something is inherently likely.[50]

An application for a search warrant must specify several things. Among other things, these include the grounds on which the application is made, the address or description of place or thing to be searched, and a description of the evidential material sought.[51] These particulars must be described with enough specificity so that those conducting the search and the subject of the search can know the parameters of the

---

[47] See, for example, *Adams on Criminal Law,* at SS6.10.
[48] Jacinda Funnell, *Response to Select Committee Questions raised on 13 March 2017*, at [22-26].
[49] Warren Young, Neville Trendle and Richard Mahoney, *Search and Surveillance: Act and Analysis* 112.
[50] Warren Young, Neville Trendle and Richard Mahoney, *Search and Surveillance: Act and Analysis* 112.
[51] See Search and Surveillance Act 2012, s 98; see also National Animal Identification and Tracing Act 2012, s 30 and Trade Marks Act 2002, s 134G for further examples. Section 98 SSA is a provision in Part Four that is variously applicable to many other statutes as indicated in the Schedule. For example, see Films, Videos, and Publications Classifications Act 1993, s 110.

search.[52] To do otherwise is likely to render the search a "general" search and, therefore, invalid.[53]

3.4.1.2 Access to computers and stored data

The traditional or general powers of search and seizure can apply to encryption and its various implementations and uses. Under the Search and Surveillance Act, "search power" encompasses the authority of police and other law enforcement officers to enter, search, seize, inspect and examine "any place, vehicle, or other things, or to search a person".[54] It has been noted that search includes the "power of inspection or examination. Any items that may be inspected or examined may be seized".[55] To search includes specific powers to: *enter and search* ("enter and search the place, vehicle, or other thing that the person is authorised to enter and search, and any item or items found in that place or vehicle or thing");[56] *use reasonable force* ("use any force in respect of any property that is reasonable for the purposes of carrying out the search and any lawful seizure");[57] and *seize* ("seize anything that is the subject of the search or anything else that may be lawfully seized").[58]

The authority to search a particular place, vehicle or thing "*extends to the search of any computer system or data storage device* located *in whole or in part* at the place, vehicle or thing".[59] Law enforcement officers are allowed to "use a computer found on the premises to access evidential material".[60] Further, they have the authority under common law "to bring and to use equipment to assist in carrying out the search authorised by a warrant".[61] The Search and Surveillance Act expressly grants law enforcement officers specific authority to: *access a computer* ("use any reasonable measures to access a computer system or other data storage device located (in whole or in part) at the place, vehicle, or other

---

[52] *Trans Rail Ltd v Wellington District Court* [2002] 3 NZLR 780 at [41].
[53] *Trans Rail Ltd v Wellington District Court* [2002] 3 NZLR 780 at at [43].
[54] Search and Surveillance Act 2012, s 3(1); see also Warren Young, Neville Trendle and Richard Mahoney, *Search and Surveillance: Act and Analysis* 43.
[55] Warren Young, Neville Trendle and Richard Mahoney, *Search and Surveillance: Act and Analysis* 183.
[56] Search and Surveillance Act 2012, s 110(a).
[57] Search and Surveillance Act 2012, s 110(c).
[58] Search and Surveillance Act 2012, s 110(d); see also Warren Young, Neville Trendle and Richard Mahoney, *Search and Surveillance: Act and Analysis* 183; see also Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act: A Commentary* 908-909.
[59] Warren Young, Neville Trendle and Richard Mahoney, *Search and Surveillance: Act and Analysis* 183 (emphasis added).
[60] Warren Young, Neville Trendle and Richard Mahoney, *Search and Surveillance: Act and Analysis* 183.
[61] Warren Young, Neville Trendle and Richard Mahoney, *Search and Surveillance: Act and Analysis* 183.

thing if any intangible material that is the subject of the search may be in that computer system or other device")[62] and *copy intangible material* ("copy [any intangible] material (including by means of previewing, cloning, or other forensic methods either before or after removal for examination)… [that] is the subject of the search or may otherwise be lawfully seized".[63] In the context of computer systems and computer data, a search involves the ability to access, "seek, read, inspect or review data".[64] 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".[65] It is worth noting though that the making of a forensic copy of electronic data "does not constitute a 'seized thing'… and is therefore not subject to notice and inventory requirements".[66]

Electronic devices are not considered any different from any other receptacle, such as a filing cabinet, during a search.[67] The jurisprudence, however, may indicate a move away from this, as electronic devices are increasingly being considered substantively different due to the amount and range of data they may now store. For example, the Supreme Court in *Dotcom v AG*[68] emphasised that the search of computers raises special privacy concerns,[69] before endorsing the idea that the electronic device should, at the very least, be specified in the search warrant before it can be searched.[70] This case related to a search issued under legislation subsequently repealed by the Search and Surveillance Act. Therefore, there is some doubt as to whether this endorsement still stands in consideration that section 110(h) of the Search and Surveillance Act contemplates access to a computer system for any lawful search regardless of whether a computer is specified in the search warrant or not.[71] However, the passing of the Customs and Excise Act 2018 codified this substantive difference, as it singles out searches of electronic devices,[72] differentiates

---

[62] Search and Surveillance Act 2012, s 110(h).
[63] Search and Surveillance Act 2012, s 110(i) and (g); see also Warren Young, Neville Trendle and Richard Mahoney, *Search and Surveillance: Act and Analysis* 184; see also Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act: A Commentary* 908.
[64] Council of Europe, Explanatory Report to the Convention on Cybercrime, para 191.
[65] Council of Europe, Explanatory Report to the Convention on Cybercrime, para 197.
[66] Warren Young, Neville Trendle and Richard Mahoney, *Search and Surveillance: Act and Analysis* 184.
[67] See Law Commission, *Review of the Search and Surveillance Act 2012*, para 12.2 in relation to the Search and Surveillance Act 2012.
[68] *Dotcom v AG* [2014] NZSC 199.
[69] *Dotcom v AG* [2014] NZSC 199, at [191]
[70] *Dotcom v AG* [2014] NZSC 199, at [202-203] per McGrath and Arnold JJ for the majority. Elias CJ went further at [57] and held that although an electronic device can be seized under a search warrant, the search of the electronic device required specific warrant.
[71] See *Adams on Criminal Law,* at [SS110.12].
[72] Customs and Excise Act 2018, s 228.

between an initial and full search of such devices,[73] and requires a search warrant be obtained before a Customs officer can search material accessible from an electronic device but not stored on that electronic device. Additionally, in its review of the Search and Surveillance Act, the Law Commission considers that the endorsement in *Dotcom* should be adopted.[74]

The powers to access a computer system and to copy intangible material also apply in the searches of persons in cases where the computer or data storage device is carried or in the physical possession or immediate control of the person being searched.[75] Whether a law enforcement officer may search people is also determined by their governing statute. In general, the power to search people is limited to either specific offences or circumstances. For example, the Search and Surveillance Act allows the search of people if reasonable grounds to suspect an offence against the Arms Act 1983 exists,[76] or in relation to offences under the Misuse of Drugs Act 1975, or if a person has been arrested or detained;[77] the Customs and Excise Act 2018 allows for the search of persons entering or exiting New Zealand;[78] and the Courts Security Act 1999 allows for court security officers to search persons who want to enter or are in Court with,[79] or without,[80] a warrant. If a person is searched, the person exercising the power to search may search any item that is in the person's physical possession or immediate control,[81] and use any reasonable measures to access that item if it is a computer system or other data storage device.[82] Copies of any intangible material accessed on the computer system or other data storage device can also be made.[83]

The main objective of a search and seizure is to obtain evidential material, which, "in relation to an offence or a suspected offence, means evidence of the offence, or any other item, tangible or *intangible*, of relevance to the investigation of the offence".[84] Simply put, evidential material covers the evidence of the offence or any other item of relevance

---

[73] Customs and Excise Act 2018, s 228(2).
[74] Law Commission, *Review of the Search and Surveillance Act 2012*, para 12.53.
[75] Search and Surveillance Act 2012, s 125(l) and (m); see also Warren Young, Neville Trendle and Richard Mahoney, *Search and Surveillance: Act and Analysis* 206.
[76] Arms Act 1983, s 18.
[77] Misuse of Drugs Act 1975, s 88.
[78] Customs and Excise Act 2018, s 210.
[79] See Courts Security Act 1999, s 13.
[80] See Courts Security Act 1999, s 28(4).
[81] Search and Surveillance Act 2012, s 125(i).
[82] Section 125(l)
[83] Section 125(m).
[84] Search and Surveillance Act 2012, s 3(1) (emphasis added).

to the investigation of the offence, whether it exists physically or electronically.[85] A thing can be searched "whether it is tangible, such as a box or receptacle, or intangible".[86] As Young, Trendle and Mahoney explain:

> This term is central to the [Search and Surveillance] Act, as search and surveillance powers are directed to the collection of evidential material in respect of the suspected offence. It is widely defined to include both tangible and intangible items. The material does not have to be admissible; the critical element is its relevance to the investigation of a specific offence…. It covers items in *electronic, optical or other form*….[87]

It should be noted that one of the aims of the Search and Surveillance Act was to confirm that "searches can be for data in electronic form".[88]

In order to search and seize intangible evidential material such as electronic evidence, law enforcement officers often need to first gain access to a computer system or device on which the data is stored. Under the Search and Surveillance Act, the term computer system covers a single computer, interconnected computers and devices, and "all related input, output, processing, storage, software, or communication facilities, and stored data".[89] The definition of computer system contemplates both stand-alone personal computers and any other computer or facility connected to that computer.[90] This has the potential to be wide-ranging, as it could include any data stored on a computer in an integrated network such as all the computers associated with a business that has centres of operation throughout New Zealand. It also has the possibility to encompass international centres if there is no break in the legal personality of the subject business, and any third-parties offering cloud-based storage that the subject business leases. This is because the definition of computer system also includes "any communication links between computers or to remote terminals or another device",[91] and a computer is considered "interconnected with another computer if it can be lawfully used to provide access to that other computer".[92] If a person executing a search is uncertain whether any item found

---

[85] Search and Surveillance Act 2012, s 3; see also *Adams on Criminal Law* at [ss3.17.01].
[86] Warren Young, Neville Trendle and Richard Mahoney, *Search and Surveillance: Act and Analysis* 162.
[87] Warren Young, Neville Trendle and Richard Mahoney, *Search and Surveillance: Act and Analysis* 36 (emphasis added).
[88] Warren Young, Neville Trendle and Richard Mahoney, *Search and Surveillance: Act and Analysis* 162.
[89] Search and Surveillance Act 2012, s 3(1); see also Convention on Cybercrime, art 1(a); see also Warren Young, Neville Trendle and Richard Mahoney, *Search and Surveillance: Act and Analysis* 34.
[90] See Search and Surveillance Act 2012, s 3 (definition of "computer system") and *Adams on Criminal Law*, at [SS3.09.01].
[91] Search and Surveillance Act 2012, s 3 (definition of "computer system" (a)(iii))
[92] Section 3(2).

may be seized or not, because, for example, an electronic device was not specified in the warrant, they are able to remove that item in order to determine whether it can be seized.[93]

With regard to access, it means to "instruct, communicate with, store data in, receive data from, or otherwise make use of any of the resources of the computer system".[94] According to Young, Trendle and Mahoney, the term access may be also understood in a number of senses including "to gain access to a computer system for intangible material", "to require a specified person to assist in enabling the officer to access data in a computer system", and "the powers of enforcement officers to gain remote access to a computer system".[95] A specific type of data that is particularly crucial to gaining access to computers and computer data is called access information. Access information is defined as including "codes, *passwords*, and *encryption keys*, and any related information that enables access to a computer system or any other data storage device".[96] It is a "type of information that an enforcement officer may need to gain access to a computer or computer system when exercising a search power. Access information falls with the definition of a 'thing' that may be the subject of a search warrant".[97] As clarified in the Search and Surveillance Act, a thing to be searched or seized includes "an intangible thing (for example, an email address or *access information* to an Internet data storage facility)".[98] Consequently, if the access information has been noted down or saved in a non-encrypted computer file, it may be seized or copied during a search.

The above powers to search and seize computer systems and data in the Search and Surveillance Act closely mirror Article 19 of the Convention on Cybercrime, which provides law enforcement specific powers for the "search and seizure of stored computer data".[99] "Computer data" is defined under the Convention as "any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function".[100] According to drafters of the Convention, "[t]he definition of computer data builds upon

---

[93] Search and Surveillance Act 2012, s 112.
[94] Search and Surveillance Act 2012, s 3(1).
[95] Warren Young, Neville Trendle and Richard Mahoney, *Search and Surveillance: Act and Analysis* 31.
[96] Search and Surveillance Act 2012, s 3(1) (emphasis added).
[97] Warren Young, Neville Trendle and Richard Mahoney, *Search and Surveillance: Act and Analysis* 32; see also *Adams on Criminal Law*, at [SS3.02.01].
[98] Search and Surveillance Act 2012, s 97 (emphasis added).
[99] Convention on Cybercrime, art 19.
[100] Convention on Cybercrime, art 1(b).

the ISO-definition of data. This definition contains the terms 'suitable for processing'. This means that data is put in such a form that it can be directly processed by the computer".[101]

Article 19 of the Convention on Cybercrime authorises law enforcement to "search and or similarly access… a computer system or part of it and computer data stored therein; and… a computer-data storage medium in which computer data may be stored in its territory".[102] The power to search and seize computer data includes the authority to resort to the following measures: (a) "seize or similarly secure a computer system or part of it or a computer-data storage medium"; (b) "make and retain a copy of those computer data"; (c) "maintain the integrity of the relevant stored computer data"; and (d) "render inaccessible or remove those computer data in the accessed computer system".[103]

The drafters of the Convention explain the rationale behind these updated and expanded search and seizure powers, which is pertinent as well to those in the Search and Surveillance Act:

> [Article 19] aims at modernising and harmonising domestic laws on search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law includes powers for search and seizure of tangible objects. However, in a number of jurisdictions stored computer data per se will not be considered as a tangible object and therefore cannot be secured on behalf of criminal investigations and proceedings in a parallel manner as tangible objects, other than by securing the data medium upon which it is stored. The aim of Article 19 of this Convention is to establish an equivalent power relating to stored data.[104]

To summarise, a search warrant authorises a law enforcement officer to enter a place and search for and seize any evidential material. A warrantless search, and/or a search of a person, authorises the same thing. Evidential material may be located on a computer system or other storage device. There is some debate as to whether it should be specified in the warrant that an electronic device found at the premises forms a part of the search before it can be searched. This does not prevent the electronic device from being removed, however, and then examined to determine whether it may be seized.

---

[101] Council of Europe, Explanatory Report to the Convention on Cybercrime, para 25.
[102] Convention on Cybercrime, art 19(1).
[103] Convention on Cybercrime, art 19(3).
[104] Council of Europe, Explanatory Report to the Convention on Cybercrime, para 184.

It is clear that the powers of search and seizure (whether under the Search and Surveillance Act or the Convention on Cybercrime) can and do apply to encryption. Encrypted computers and devices can be physically seized and inspected and encrypted data can be searched and copied. However, being able to access and understand the encrypted data is another matter altogether. Because encryption protects the confidentiality, integrity and authenticity of computer systems and data as well as prevent their unauthorised access, encryption can serve as a hindrance to law enforcement gaining access to computers or data that are subject to a search and seizure. The impact of encryption technologies on the execution of a search warrant is that the use of encryption prevents law enforcement officers from accessing any encrypted information on the electronic device or accessing the electronic device itself. In light of these issues of gaining access to encrypted computer systems and data and making such encrypted data searched for intelligible, the Search and Surveillance Act imposes additional duties on users, owners, developers and providers of computer systems.

3.4.1.3 Reasonable assistance and forced disclosure of access information

In addition to the specific search and seizure powers discussed above, law enforcement officers have the authority "to request any person to assist with the entry and search".[105] Moreover, they have a specific power under Section 130 to require the user, owner, or provider of a computer system to offer reasonable assistance to law enforcement officers conducting a search and seizure including providing access information. Section 130 of the Search and Surveillance Act explicitly provides:

> 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*.[106]

The Convention on Cybercrime also has a provision on the duty of reasonable assistance that states that law enforcement authorities have the power "to order any person who has knowledge about the functioning of the computer system or measures applied to protect

[105] Search and Surveillance Act 2012, s 110(b).
[106] Search and Surveillance Act 2012, s 130(1) (emphasis added)

the computer data therein to provide, *as is reasonable*, the necessary information, to enable the undertaking of the measures" to search and seize stored computer data.[107]

The definition of a "specified person" who is required to provide access information or reasonable assistance appears to be much broader in the Search and Surveillance Act compared to the Convention on Cybercrime. Section 130 of Search and Surveillance Act covers both the user ("a user of a computer system or other data storage device or an Internet site who has relevant knowledge of that system, device, or site;**"**) and provider of the computer system ("a person who provides an Internet service or maintains an Internet site and who holds access information").[108] With regard to the user, this includes any person who:

> (a) owns, leases, possesses, or controls the system, device, or site; or
> (b) is entitled, by reason of an account or other arrangement, to access data on an Internet site; or
> (c) is an employee of a person described in paragraph (a) or (b).[109]

Section 130 not only captures an individual who is the subject of the search, but also any third party such as an IT company providing cloud-based and/or other computing services or the website operator.

Section 130 though impacts users and providers in different ways. For users, the requirement to provide access information under section 130 appears to have wide applicability as the definition is broad and can cover even those who are suspected of or charged with the commission of an offence. Under subsection (1) of Section 130, a suspect or an accused person can be ordered to divulge his or her password, encryption keys and other access information as part of a search. Subsection (2) of Section 130 though provides an exception pursuant to the right of self-incrimination that "a specified person may not be required… to give any information tending to incriminate the person".[110] But subsection (2) is subject to a further qualification in subsection (3), which states that:

> Subsection (2) does not prevent a person exercising a search power from requiring a specified person to provide information or providing assistance that is reasonable and necessary to allow the person exercising the search power to access data held in, or accessible from, a computer system or other

[107] Convention on Cybercrime, art 19(4) (emphasis added).
[108] Search and Surveillance Act 2012, s 130(5).
[109] Search and Surveillance Act 2012, s 130(5).
[110] Search and Surveillance Act 2012, s 130(2).

> data storage device that contains or may contain information tending to incriminate the specified person.[111]

Subsection (3) seems to contradict or nullify the express objective of Subsection (2). To make matters more confusing, subsection (4) of Section 130 also explicitly states that the preceding "Subsections (2) and (3) are subject to subpart 5 of this Part (which relates to privilege and confidentiality)", which confusingly reaffirms the protection of the privilege against self-incrimination.[112] The Law Commission and legal scholars also find the provisions of Section 130 confusing.[113] In its review of the Search and Surveillance Act, the Law Commission is of the view that "the privilege against self-incrimination should only be available under section 130 of the Act if it is the *content* of the access information that is incriminating. In such cases, the Act should permit a privilege claim to be made".[114] The example given by Law Commission is a specified person's password is "I murdered Joe Bloggs".[115] Short of this, which would be a truly rare or exceptional situation,[116] any user, owner or provider of a computer system and other electronic device, including a criminal suspect or accused, can be made to provide, under threat of criminal penalty, their passwords, decryption keys and any other access information. The Law Commissions explains the reasoning behind its interpretation:

> the privilege against self-incrimination should not be available simply because the assistance will lead to the discovery of incriminating evidence. Nor should it be available to protect a person from having to disclose the fact that they know what the access information is. That fact is an inference drawn from the provision of existing information as opposed to an oral statement or document created in response to a request for information. Therefore, the privilege against self-incrimination as recognised by section 60 of the Evidence Act does not apply in this situation. Given that, we do not think there is any reason to place restrictions on the use of that fact as evidence at trial.[117]

Following this narrow interpretation of Section 130 vis-à-vis the right against self-incrimination, virtually everyone who is subject to a search pursuant to a search warrant or a lawful warrantless search can be compelled under pain of criminal prosecution to provide their passwords and other access information that may lead to incriminating or

---

[111] Search and Surveillance Act 2012, s 130(3).
[112] Search and Surveillance Act 2012, s 130(4).
[113] Law Commission, *Review of the Search and Surveillance Act 2012*, paras 12.160-12.162.
[114] Law Commission, *Review of the Search and Surveillance Act 2012*, para 12.169.
[115] Law Commission, *Review of the Search and Surveillance Act 2012*, para 12.163.
[116] See Law Commission, *Review of the Search and Surveillance Act 2012*, para 12.169.
[117] Law Commission, *Review of the Search and Surveillance Act 2012*, para 12.168.

inculpatory evidence about them. Young, Trendle and Mahoney appear to agree with the Law Commission's interpretation. They say

> Subsection (1) only requires information or assistance that would enable access to a computer system or data storage device. If the existence of incriminating information on the system or device does not invoke the privilege (because *the access information itself* does not do so), it is difficult to see when subs (2) could apply".[118]

Section 130 must also be read together with section 178 of the Search and Surveillance Act. Section 178 is the provision that makes it an offence to fail, without reasonable excuse, to assist a person exercising a search power to access a computer system.[119] If convicted, a person faces imprisonment for a term not exceeding three months.[120] While the offence contained in section 178 is a stand-alone offence, there does not appear to be a case where any person has been tried solely for failing to assist access. Rather, prosecutions for breaching section 178 only appear when offenders are being prosecuted for other crimes, such as offences against the Films, Videos, and Publications Act 1993. Refusals to provide access information can prematurely end investigations.[121] In part, this is because the punishment for offending against section 178 is an imprisonment term of no more than three months. The offences typically hidden behind encrypted access to computers and data carry imprisonment terms of, at least, 14 years or more.[122] Consequently, it is rational for a person suspected or accused of a crime to refuse to comply with a section 130(1) demand for assistance if incriminating files are contained behind encrypted access. The Law Commission has recommended increasing the sentence for breaching section 178 to a term of imprisonment not exceeding six months.[123] The apparent authority of law enforcement officers to compel users (even those who are suspected or charged with a crime) to disclose access information and passwords is a complex and controversial issue, which is analysed further in a succeeding section on the right against self-incrimination.

---

[118] Warren Young, Neville Trendle and Richard Mahoney, *Search and Surveillance: Act and Analysis* 211 (emphasis added).
[119] Search and Surveillance Act 2012, s 178.
[120] Search and Surveillance Act 2012, s 178.
[121] Law Commission, *Review of the Search and Surveillance Act 2012*, para 12.173.
[122] For example, a breach against the Films, Videos, and Publications Classification Act 1993, s 124 (regarding objectionable material) faces an imprisonment term not exceeding 14 years. Breaching the Terrorism Suppression Act 2002, s 6A (intending to carry out a terrorist act) carries a life imprisonment term while breaching s 8 (financing of terrorism) carries an imprisonment term of not more than 14 years.
[123] Law Commission, *Review of the Search and Surveillance Act 2012*, para 12.179.

With respect to providers, the drafters of the Convention on Cybercrime explain the reasoning behind the imposition of this duty. According to the drafters:

> It addresses the practical problem that it may be difficult to access and identify the data sought as evidence, given the quantity of data that can be processed and stored, the deployment of security measures, as well as the nature of computer operations. It recognises that system administrators, who have particular knowledge of the computer system, may need to be consulted concerning the technical modalities about how best the search should be conducted.[124]

They further explain:

> This power is not only of benefit to the investigating authorities. Without such co-operation, investigative authorities could remain on the searched premises and prevent access to the computer system for long periods of time while undertaking the search. This could be an economic burden on legitimate businesses or customers and subscribers that are denied access to data during this time. A means to order the co-operation of knowledgeable persons would help in making searches more effective and cost efficient, both for law enforcement and innocent individuals affected. Legally compelling a system administrator to assist may also relieve the administrator of any contractual or other obligations not to disclose the data.[125]

While these are sensible reasons, the duty on the part of providers to provide reasonable assistance in the search of a computer system and data remains unclear and potentially problematic. Providers of computer systems normally act as third parties, which means that they are not themselves involved in the crime being investigated and the right against self-incrimination is generally not relevant or available to them. However, as seen in the *Apple v FBI* case,[126] the extent and manner by which a provider can be required to provide reasonable assistance in the search of a computer system it developed, owns or controls is unsettled. There is as of yet no case law that sufficiently clarifies or explains what "reasonable and necessary assistance" actually means or entails on the part of a provider. According to Young, Trendle and Mahoney, a specified person does "not commit an offence… if he or she has a *reasonable excuse* for failing to provide the assistance requested".[127] But what is reasonable assistance or what amounts to a reasonable excuse are uncertain and depend on the particular circumstances of the case. The drafters of the

[124] Council of Europe, Explanatory Report to the Convention on Cybercrime, para 200.
[125] Council of Europe, Explanatory Report to the Convention on Cybercrime, para 201.
[126] See Michael Hack, "The implications of Apple's battle with the FBI".
[127] Warren Young, Neville Trendle and Richard Mahoney, *Search and Surveillance: Act and Analysis* 271 (emphasis added).

Convention on Cybercrime offer some guidance and examples of what amounts to reasonable assistance. They note that "[t]he provision of this information, however, is restricted to that which is 'reasonable'".[128] Reasonableness depends on the context or circumstances. They explain,

> 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.[129]

As explained in Part 2, ordering a company to give up its encryption keys may not be fair or just given that the secrecy and inviolability of encryption keys are essential to preserving the security and integrity of any information system. The disclosure of encryption keys, passwords and other access information may also result in compromising the security of a computer system, weakening its ability to resist an attack, or endangering the privacy and security of all of its users and not just the one who is subject to a search.

3.4.1.4 Customs and border searches

The problems and issues surrounding searching and gaining access to electronic devices and data is particularly relevant in relation to customs and border searches. The security of New Zealand's borders is the purview of the New Zealand Customs Service. Their governing statute is the Customs and Excise Act 2018, which recently replaced the Customs and Excise Act 1996.[130]

Encryption and its corresponding issue of access did not appear in the 1996 Act. Rather, provisions from the 1996 Act had been co-opted to deal with the issue of access. These co-opted provisions broadly regarded search and seizure (sections 151, 152, 175C, and 175D) and assistance (sections 29, 39, and 145). Section 151 was the lynchpin provision, as goods were defined in the 1996 Act very broadly and section 151 authorised their examination.[131] Other search and seizure provisions either triggered section 151's examination powers,[132] or assumed the prior valid exercise of section 151.[133] The courts

[128] Council of Europe, Explanatory Report to the Convention on Cybercrime, para 202.
[129] Council of Europe, Explanatory Report to the Convention on Cybercrime, para 202.
[130] The Customs and Excise Act 2018 commenced on 1 October 2018. See Customs and Excise Act 2018, s 2.
[131] Customs and Excise Act 1996, s 2 (definition of "goods").
[132] Section 152(3)

have agreed, holding that section 151 unambiguously permitted the search of electronic devices as goods.[134]

Under the previous law, there was no legal obligation to provide access to an electronic device.[135] Rather, the requirements in the 1996 Act to make baggage available for examination and to answer a Customs officer's question had been co-opted.[136] If such requirements were not followed, then Customs considered that import formalities had not been complied with and would retain the device until access information was provided or Customs was able to manually access the device's contents.[137]

Conversely, encryption and its related issue of access does feature explicitly in the 2018 Act. A user must provide access to an electronic device for that device to be searched if required by a Customs officer.[138] "User" is defined more narrowly than in the Search and Surveillance Act as it only refers to "a person who owns, leases, possesses, or controls a device (or an employee of such a person) and who has relevant knowledge of the device."[139] If the user has no reasonable excuse for failing to provide access information, then the person becomes liable to a fine not exceeding $5,000.[140] Customs may retain the device to arrange access to that device,[141] and the device may be condemned to the Crown, destroyed, or returned to the user at the court's discretion.[142]

This contrasts with the 1996 Act where there was no legal obligation to provide access information. Therefore, no fine could be imposed for failing to provide such information. Customs could still retain and possibly destroy the device, although this was Customs' operating procedure rather than a legislative requirement. The liability for not providing access information when required also contrasts with the liability imposed by section 178 of the Search and Surveillance Act. Not providing access information when requested under section 130 of the Search and Surveillance Act can result in

---

[133] Such as Customs and Excise Act 1996, ss 175C and 175D. See also *S v R* [2016] NZCA 448 at [36].
[134] *S v R*, at [32]. This case was appealed. However, the Supreme Court declined to reconsider Customs' approach due to the progress of the then Customs and Excise Bill. See *S v R* [2016] NZSC 172 at [7].
[135] See New Zealand Customs Service, *Customs and Excise Act 1996 Review: Discussion Paper 2015* (March 2015) at 133.
[136] Jacinda Funnell, *E-Devices: Supplementary Briefing for Foreign Affairs, Defence and Trade Committee* (New Zealand Customs Service, 21 February 2017) at [4] and [11].
[137] Jacinda Funnell, *E-Devices: Supplementary Briefing for Foreign Affairs, Defence and Trade Committee*, at [21].
[138] Customs and Excise Act 2018, s 228(3)(c) and (d).
[139] Section 228(5) (definition of "user").
[140] Section 228(8).
[141] Section 228(9).
[142] Section 228(11).

imprisonment for a term not exceeding three months.[143] However, no fine can be imposed.

Customs' operating procedure when it came to searching electronic devices has been curtailed by the 2018 Act.[144] Electronic devices are explicitly excluded from the 2018 Act's equivalent to the 1996 Act's section 151,[145] and remotely accessible stored data now requires a search warrant to access.[146] The new lynchpin provision for the search of an electronic device is section 228. This provision differentiates between an initial search and a full search, with both requiring thresholds to be met before they can be conducted.

3.4.1.5 Impact on stakeholders

To summarise, the powers of search and seizure impact the three groups of stakeholders (government, businesses and the general public) differently. Government actors such as law enforcement officers have significant search and seizure powers in relation to encryption. They can search and seize encrypted data and the computers, systems and devices on which such data are stored. To gain access to encrypted data and protected computers, law enforcement officers also have the authority to compel the disclosure of passwords and other access information possibly even from people who are suspected or charged with a crime. Similarly, in relation to border searches, Customs can also conduct searches and seizures of electronic devices and demand access information under certain conditions.

Businesses who develop or provide encrypted products and services are generally considered third parties in relation to a search as they are not the ones suspected or charged with a crime. This means that the right of self-incrimination is not available to them and they may be compelled to disclose access information or provide reasonable assistance to allow law enforcement to gain access to the encrypted data or computer sought to be searched or seized. There is the essential condition though that the provider has knowledge of or control over how to access the encrypted data or computer. If a provider holds the encryption key, knows the password to unlock a computer being

[143] Search and Surveillance Act 2012, s 178.
[144] See, for background, New Zealand Customs Service, *Customs and Excise Act 1996. Summary of Submissions* (March 2016) and "Customs and Excise Bill – First Reading" (6 December 2016) 7719 NZPD 15546, particularly the comments of the Hon. Nicky Wagner.
[145] Customs and Excise Act 2018, s 227(5).
[146] Customs and Excise Act 2018, ss 227(5) and 228(3).

searched, or has general control over the means to gain access to the encrypted data or system, then the provider may be compelled to render the necessary assistance or provide access information. However, if the provider's product or service uses client-side encryption where it is the user alone who knows or holds the encryption keys, then the provider would not be in a position to provide the assistance required. If the provider's use of encryption is for a legitimate purpose such as to protect information security or privacy, it would be unreasonable to require a provider to render assistance that would result in weakening of the security and privacy protections of its products and services.

Ordinary users and members of the general public are free to use encryption to protect and secure their stored data. Pursuant to a search warrant or a lawful warrantless search, law enforcement officers appear to have the power to order users to provide access information or render reasonable assistance to gain access to the encrypted data. However, this is subject to the important qualification that such required information or assistance should not infringe users' right against self-incrimination. There is ambiguity and uncertainty though in the law as to what type of information and what kind assistance is considered incriminating or not. It is still unclear whether the forced disclosure of passwords or the compelled production of encryption keys on the part of suspects or persons charged with a crime are covered by the right against self-incrimination.

3.4.2 SURVEILLANCE

3.4.2.1 Interception and collection of communications

While the powers of search and seizure are concerned with gaining access to stored data or data at rest, surveillance is principally focused on intercepting and collecting communications or data in motion. The state of the data being sought determines which investigatory power or measure is appropriate. For surveillance to be apropos, the "temporal quality" of the data is key because a communication "is 'intercepted' only if it is captured (eg, through listening, eavesdropping, or recording) at the time it is occurring."[147] Young, Trendle and Mahoney further explain that a "written or electronic communication (eg, a letter or an email) is 'intercepted' only if it is acquired while it is in the process of being physically or electronically transmitted from sender to

[147] Warren Young, Neville Trendle and Richard Mahoney, *Search and Surveillance: Act and Analysis* 37.

recipient".[148] Thus, before or after any data or communication is sent, transmitted or received, it is classified as stored data that may be subject to a search and seizure.

Surveillance of data normally involves the act of interception. To intercept is specifically defined under the Search and Surveillance Act as including to "hear, listen to, record, monitor, acquire, or receive the communication either[:] (a) while it is taking place; or (b) while it is in transit".[149] Given the stated objective of the Search and Surveillance Act to apply to new technologies and forms of communication, the power of surveillance is "not confined to listening or hearing a conversation. It includes recording, monitoring, acquiring or receiving other forms of communication, such as one sent in a *digital format*, or in Morse Code".[150] Surveillance can apply to "any form of communication over a distance, however conveyed, such as *electronic communications* or communications by Morse code or other signals. Examples include email or facsimile transmissions and text messaging".[151]

Surveillance is specifically targeted at intercepting "private communications", which the law defines as

> (a)… a communication (whether in oral or written form, or in the form of a telecommunication, or otherwise) made under circumstances that may reasonably be taken to indicate that any party to the communication desires it to be confined to the parties to the communication; but
>
> (b) does not include a communication of that kind occurring in circumstances in which any party to the communication ought reasonably to expect that the communication may be intercepted by some other person without having the express or implied consent of any party to do so.[152]

It is the intention and/or the reasonable expectation of the parties involved that determines the character of a communication as being private and not the network on which it is sent or transmitted. For example, an email sent over a public network like the internet or a call made on a traditional public switched telephone network remain private

---

[148] Warren Young, Neville Trendle and Richard Mahoney, *Search and Surveillance: Act and Analysis* 37.
[149] Search and Surveillance Act 2012, s 3(1).
[150] Warren Young, Neville Trendle and Richard Mahoney, *Search and Surveillance: Act and Analysis* 37 (emphasis added).
[151] Warren Young, Neville Trendle and Richard Mahoney, *Search and Surveillance: Act and Analysis* 41 (emphasis added).
[152] Search and Surveillance Act 2012, s 3(1).

communications if the intent or expectation of the communicating parties is that their communications are private or confidential.[153]

3.4.2.2 Surveillance device regime

Surveillance powers are subject to a surveillance device regime, which is governed by sections 45 to 64 of the Search and Surveillance Act.[154] This regime only authorises three types of surveillance because the definition of "surveillance device" is expressly limited to three types of devices: (a) an interception device; (b) a tracking device: and (c) a visual surveillance device.[155] Additionally, only the New Zealand Police (and the New Zealand Customs Service and Department of Internal Affairs if approval has been granted by the Governor-General by Order in Council,[156] which has not yet occurred)[157] can apply for a surveillance device warrant involving visual surveillance that requires trespass to utilise an interception device.[158]

A warrant is not available for surveillance that does not fall within one of these three types of devices.[159] Additionally, the Law Commission opines that although the word "device" is not defined in the Search and Surveillance Act, the definitions of all three types of surveillance device refer to "instruments, apparatus, equipment, or other device".[160] This implies that "device" is to carry its ordinary meaning of a tangible thing.[161] Therefore, intangible things, such as computer programs, are not thought by the Law Commission to be encompassed by the surveillance device regime of the Search and Surveillance Act.[162] It is uncertain whether methods of surveillance falling outside of the Search and Surveillance Act's surveillance device regime may be in breach of the law and would, therefore, be invalid.[163]

---

[153] See Warren Young, Neville Trendle and Richard Mahoney, *Search and Surveillance: Act and Analysis* 105.
[154] Search and Surveillance Act 2012, s 49(1).
[155] Section 3; see also Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act: A Commentary* 911-912.
[156] Section 50; see also Warren Young, Neville Trendle and Richard Mahoney, *Search and Surveillance: Act and Analysis* 7
[157] Law Commission, *Review of the Search and Surveillance Act 2012*, para 7.7.
[158] Search and Surveillance Act 2012, s 49(5).
[159] Law Commission, *Review of the Search and Surveillance Act 2012*, para 7.5.
[160] Law Commission, *Review of the Search and Surveillance Act 2012*, para 7.11.
[161] Law Commission, *Review of the Search and Surveillance Act 2012*, para 7.11.
[162] Law Commission, *Review of the Search and Surveillance Act 2012*, para 7.2.
[163] Law Commission, *Review of the Search and Surveillance Act 2012*, para 7.5 and further para 7.14. A search that is unlawful is almost always considered unreasonable in terms of s 21 of the New Zealand Bill of Rights Act 1990. See *Hamed v R* [2011] NZSC 101 at [174].

A surveillance device warrant must be obtained to use any of the three types of surveillance devices or conduct specific forms of surveillance.[164] Surveillance involving trespass, or the use of an interception device, can only be issued in relation to offences that carry imprisonment sentences of seven years or more or for other specified offences.[165] Use of a surveillance device without a warrant is permitted in situations of urgency if the circumstances would otherwise support the application for a surveillance device warrant but for the urgency of the situation.[166] Only a Judge may issue a surveillance device warrant,[167] and only if they are satisfied that there are reasonable grounds:

> i) to suspect that an offence has been, is being, or will be committed in respect of which this Act or any enactment specified in column 2 of the Schedule authorises the enforcement officer to apply for a warrant to enter premises for the purpose of obtaining evidence about the suspected offence; and
>
> ii) to believe that the proposed use of the surveillance device will obtain information that is evidential material in respect of the offence.[168]

Of the three types of surveillance devices available under the surveillance device regime, an interception device is the most pertinent to encryption. This is because interception devices are devices capable of being used to intercept or record encrypted communications. An interception device is defined under the law as "any electronic, mechanical, electromagnetic, optical, or electro-optical instrument, apparatus, equipment, or other device that is used or is capable of being used to intercept or record a private communication (including a telecommunication)".[169] Aside from being able to intercept communications using an interception device, a surveillance device warrant further authorises law enforcement officers to: "use any assistance that is reasonable in the circumstances"; use "any force that is reasonable in the circumstances to do so, in order to install, maintain, or remove the surveillance device, or to access and use electricity to power the surveillance device"; and obtain "the content of a telecommunication" and

[164] Search and Surveillance Act 2012, s 46.
[165] See Search and Surveillance Act 2012, ss 45(1)(b) and (c); and s 45(2)(b) and (c).
[166] Search and Surveillance Act 2012, s 48.
[167] Search and Surveillance Act 2012, s 53.
[168] Search and Surveillance Act 2012, s 51.
[169] Search and Surveillance Act 2012, s 3(1).

"direct the relevant network operator to provide call associated data (as defined in section 3(1) of the Telecommunications (Interception Capability and Security) Act 2013)".[170]

3.4.2.3 Interception capability and duty to assist

The word "telecommunication" as opposed to "private communication" is not defined in the Search and Surveillance Act. However, the Telecommunications Act 2001 defines telecommunications as "the conveyance by electromagnetic means from one device to another of any *encrypted or non-encrypted* sign, signal, impulse, writing, image, sound, instruction, information, or intelligence of any nature, whether for the information of any person using the device or not".[171] Telecommunications are facilitated or enabled by those who the Telecommunications (Interception Capability and Security) Act 2013 (TICSA) defines as providers of a telecommunications service.[172] Providers of a telecommunications service have their capability to do so supplied by what the TICSA defines as network operators,[173] and the same business may, in fact, be both a network operator and a provider of telecommunications services. Network operators are also defined as owners, controllers, or operators of a public telecommunications network,[174] making them the ultimate suppliers of internet and email access,[175] and the dial-up telephone network,[176] in New Zealand. All network operators are required to register with the Police.[177]

The TICSA imposes two kinds of obligations on network operators. A duty pursuant to section 9 to ensure that their public telecommunications networks and telecommunications service has full interception capability, and a duty pursuant to section 24 to assist a surveillance agency. Surveillance agency is defined to mean either a law enforcement agency or an intelligence and security agency,[178] which are specified as being

[170] Search and Surveillance Act 2012, s 55(3)(f-h).
[171] Telecommunications Act 2001, s 5 (emphasis added).
[172] Telecommunications (Interception Capability and Security) Act 2013, s 3 (definition of "telecommunications service").
[173] Section 3 (definition of "network operator").
[174] Section 3 (definition of "network operator").
[175] Section 3 (definition of "public data network").
[176] Section 3 (definition of "public switched telephone network").
[177] Section 60.
[178] Section 3 (definition of "surveillance agency").

the New Zealand Police,[179] the New Zealand Security Intelligence Service or the Government Communications Security Bureau.[180]

The duty imposed by section 9 is outlined in section 10 of the TICSA and is known as having full interception capability. Effectively, compliance entails that the surveillance agency be able to obtain the call associated data of a telecommunication and the contents of the telecommunication in a useable format.[181] Call associated data is defined as the metadata associated with a telecommunication.[182] A useable format means either a format determined by notice or a format mutually acceptable to the network operator and surveillance agency.[183] Network operators with fewer than 4,000 customers and network operators offering wholesale network services have reduced duties, as outlined in sections 11 and 12 respectively. Infrastructure-level services are not subject to any duty.[184] Wholesale network services are telecommunications services provided by one network operator to another,[185] while infrastructure-level service "means any service that provides the physical medium over which telecommunications are transmitted.[186]

The duty to assist is imposed on both network operators and service providers,[187] which are defined as meaning "any person who, from within our outside New Zealand, provides or makes available in New Zealand a telecommunications service to an end-user".[188] The duty requires that the network operator and/or service provider provide "reasonable" assistance to the surveillance agency. This entails assisting the surveillance agency to identify, intercept and obtain both the contents of the telecommunication and the metadata associated with the telecommunication, at the time of the transmission of the telecommunication or as close to that time as is practicable, and without unduly interfering with any telecommunication not authorised to be intercepted.[189] There are no cases available to indicate what may be considered reasonable assistance. It is standard

---

[179] Section 3 (definition of "law enforcement agency"). It may also encompass the New Zealand Customs Service and the Department of Internal Affairs if Search and Surveillance Act 2012, section 50(4).
[180] Section 3 (definition of "intelligence and security agency").
[181] Section 10(1)(b) and (c), and (5).
[182] Section 3 (definition of "call associated data")
[183] Section 10(5). This notice consists of the "Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic" ETSI TS 101 671 v3.12.1 (2013-10), applicable via "Telecommunications (Interception Capability and Security) Useable Format Notice 2017" 83 *New Zealand Gazette*.
[184] Section 14.
[185] Section 3 (definition of "wholesale network service")
[186] Section 3 (definition of "infrastructure-level service").
[187] Telecommunications (Interception Capability and Security) Act 2013, s 24(2)(b).
[188] Section 3 (definition of "service provider").
[189] Section 24(3).

practise of the telecommunications industry to encrypt communications by its users.[190] Moreover, email and other communications apps also encrypt by default or offer end-to-end encryption where the app provider is unable to decrypt the encryption process. Moreover, a network operator or service provider must only decrypt the content of a telecommunications if it has provided that encryption.[191] Furthermore, a network operator or service provider does not have to ensure that a surveillance agency has the capability to decrypt a telecommunication that is has not provided.[192]

In sum, surveillance device warrants authorise the use of three types of surveillance device: interception devices, tracking devices, and visual surveillance devices. Interception devices are the most pertinent to encryption technologies as they enable the interception of telecommunications, which are virtually all encrypted if sent digitally. Providers of the networks that form the medium by which telecommunications are sent are statutorily obliged to assist surveillance agencies to decrypt encrypted telecommunications only if that encryption has been provided by them. Third-party app providers, like WhatsApp, Telegram, Facebook Messenger, Gmail, or Outlook for example, would be caught by TICSA, as they fit the definition of a service provider and, therefore, fall within the ambit of section 24 of the TICSA. Consequently, pursuant to a surveillance device warrant for an interception device, they may be required to assist in the decryption of telecommunications sent using their applications. However, whether it is reasonable for an app provider to assist if the application makes use of end-to-end encryption, such as WhatsApp and Telegram for example, is, ultimately, unclear as no case law exists to offer guidance on this matter. As in the case of providers being required to disclose their encryption keys and other access information as part of a search and seizure, the same problems are present when they are required to do so under a surveillance warrant.

3.4.2.4 Content data and traffic data

It is noteworthy that, while the powers of search and seizures have been significantly updated in light of the greater use of computers and other information

---

[190] See Privacy Commissioner, "Privacy on the line: A resource document in relation to Privacy in Telecommunications" (June 2010) <www.privacy.org.nz> at 20.
[191] Section 24(3)(vi). A network operator does not need to be able to decrypt a telecommunication if it is supplied by that network operator as an agent for that product or supplied by another and is available to the public to be fully compliant with section 9. See Telecommunications (Interception Capability and Security) Act 2013, s 10(4).
[192] Section 24(4)(b).

technologies (e.g., Section 130 on computer system searches), surveillance powers have not received the same robust treatment. It can be argued that such updated surveillance powers can be found in the TICSA. However, even the interception powers under TICSA do not appear to completely embrace the growing use of digital communications and the inevitable convergence between traditional telecommunications networks and information systems. As explained by the drafters of the Convention on Cybercrime, "[t]he distinction between telecommunications and computer communications, and the distinctiveness between their infrastructures, is blurring with the convergence of telecommunication and information technologies".[193]

While the surveillance powers under the Search and Surveillance Act and TICSA are generally aligned with those of the Convention on Cybercrime, the former does not appear to be as extensive when it comes to dealing with computer data and communications. For instance, the Convention on Cybercrime makes an important distinction between two types of data in motion or communications that may subject to surveillance, namely: content data and traffic data.[194] Content data is not specifically defined in the Convention on Cybercrime but it has been described as referring to "the communication content of the communication; i.e., the meaning or purport of the communication, or the message or information being conveyed by the communication. It is everything transmitted as part of the communication that is not traffic data".[195] In contrast, traffic data is explicitly defined as

> 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.[196]

Traffic data, which also includes metadata, is further described as being "generated by computers in the chain of communication in order to route a communication from its origin to its destination. It is therefore auxiliary to the communication itself".[197]

In light of these two types of communications data that can be intercepted or collected, the Convention on Cybercrime provides for two kinds of surveillance powers: (a) interception of content data and (b) real-time collection of traffic data. Article 21 of the

[193] Council of Europe, Explanatory Report to the Convention on Cybercrime, para 206.
[194] Council of Europe, Explanatory Report to the Convention on Cybercrime, para 209.
[195] Council of Europe, Explanatory Report to the Convention on Cybercrime, paras 229 and 209.
[196] Convention on Cybercrime, art 1(d).
[197] Council of Europe, Explanatory Report to the Convention on Cybercrime, para 28.

Convention specifically empowers law enforcement authorities to "collect or record… content data, in real-time, of specified communications in its territory transmitted by means of a computer system".[198] The act of interception of communications (i.e., "to collect or record through the application of technical means")[199] may be done by a competent authority itself (e.g., a law enforcement agency) or it may "compel a service provider, within its existing technical capability" to either (a) "collect or record through the application of technical means" or (b) "co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system".[200] Article 21 also imposes an obligation of confidentiality because in order not to defeat the purpose of surveillance it "may be necessary to oblige a service provider to keep confidential the fact of the execution of [such] power… and any information relating to it".[201] Confidentiality is required because part of the effectivness of the powers of interception and collection for criminal investigations is that the persons subject to surveillance are unaware that their communications are being monitored and recorded.

Article 20 of the Convention on Cybercrime further authorises law enforcement authorities to collect "traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system".[202] As with the interception of content data, the collection of traffic data may be done either by the law enforcement authority itself ("collect or record through the application of technical means")[203] or it may "compel a service provider, within its existing technical capability" to "collect or record through the application of technical means" or to "co-operate and assist the competent authorities in the collection or recording of" traffic data.[204] Article 20 also imposes the obligation of confidentiality on the service provider not to disclose "the fact of the execution of [collection of traffic data]… and any information relating to it".[205]

The above examination of the Convention on Cybercrime provides interesting insights and possible guidance to the interpretation and application of the surveillance

[198] Convention on Cybercrime, art 21(1)(b).
[199] Convention on Cybercrime, art 21(1)(a).
[200] Convention on Cybercrime, art 21(1)(b)
[201] Convention on Cybercrime, art 21(3).
[202] Convention on Cybercrime, art 20(1)(b).
[203] Convention on Cybercrime, art 20(1)(a).
[204] Convention on Cybercrime, art 20(1)(b).
[205] Convention on Cybercrime, art 20(3).

powers and procedures under the Search and Surveillance Act and the TICSA. First, a service provider (as opposed to a network operator) may only be compelled to collect or record content data or traffic data if this is "within its existing technical capability".[206] There is no positive obligation on the part of service providers to make their products and services interception capable or ready if they do not wish to do so. This aligns with the TICSA where only network operators are specifically required to ensure that their telecommunications networks have interception capability to allow lawful access by law enforcement. Second, the concept of computer data (including content data and traffic data) under the Convention on Cybercrime are more specific and in accord with how communications are actually conducted today compared to the traditional notions of private communications, telecommunications and call associated data under the Search and Surveillance Act and TICSA. Computer data can cover transfers of information that may not necessarily be telecommunications in the traditional sense. Third, the Convention on Cybercrime makes a clear distinction between content data and traffic data and this has significant legal implications and effects. The interception of content data is generally considered more serious and invasive than the collection of traffic data. As the drafter of the Convention explain, "the collection of [traffic] data is regarded in principle to be less intrusive since as such it doesn't reveal the content of the communication which is regarded to be more sensitive".[207] This means that the legal conditions and protections to authorise the collection of traffic data are lower than those required for the interception of content data. The drafters of the Convention note that "many States consider that the privacy interests in respect of content data are greater due to the nature of the communication content or message. Greater limitations may be imposed with respect to the real-time collection of content data than traffic data".[208] Furthermore, because of their very intrusive character, "the law often prescribes that [the interception of content data] is only available in relation to the investigation of serious offences or categories of serious offences",[209] whereas the collection of traffic data may "in principle [apply] to any criminal offence".[210] It is worth considering having a similar distinction between content data and traffic data under the Search and Surveillance Act.

[206] Convention on Cybercrime, arts 20(1)(b) and 21(1)(b).
[207] Council of Europe, Explanatory Report to the Convention on Cybercrime, para 29.
[208] Council of Europe, Explanatory Report to the Convention on Cybercrime, para 210.
[209] Council of Europe, Explanatory Report to the Convention on Cybercrime, para 212.
[210] Council of Europe, Explanatory Report to the Convention on Cybercrime, para 213.

Finally, under the Convention on Cybercrime, the powers and procedures for conducting surveillance are not limited to physical interception devices. Interception of content data or collection traffic can be accomplished "through the application of technical means",[211] which permits the use by law enforcement of different kinds and forms of technologies including computer programs and software-based techniques and not just physical hardware and devices. This is the reason why the Law Commission has recommended giving law enforcement officers the authority to use "data surveillance technology" as part of their surveillance and interception powers.[212] This would make the country's surveillance rules more in line with international procedures as contained in the Convention on Cybercrime and those practiced in other jurisdictions.

3.4.2.5 In relation to national security

The use of surveillance powers is also relevant to national security matters. National security, international relations, and the well-being of New Zealand is the purview of New Zealand's intelligence and security agencies. These are defined as being either the New Zealand Security Intelligence Services or the Government Communications Security Bureau.[213] Their powers are derived solely from their governing statute, the Intelligence and Security Act 2017 – Part Four of the Search and Surveillance Act has no applicability to their investigatory powers.

The Intelligence and Security Act arose out of a review of the collection of statutes that governed intelligence activities,[214] and the Act was designed to replace this disparate collection;[215] setting out clearly the functions, powers, and oversight of New Zealand's intelligence and security agencies.[216]

Interestingly, the Act does not mention encryption or cryptography at all. Furthermore, there is no duty to assist with access like that contained in the Search and Surveillance Act. Potentially, these apparent oversights may reflect the fact that the

---

[211] Convention on Cybercrime, arts 20(1)(a) and 21(1)(a).
[212] Law Commission, *Review of the Search and Surveillance Act 2012*, para 7.49.
[213] Intelligence and Security Act 2017, s 4 (definition of "intelligence and security agency").
[214] Michael Cullen and Patsy Reddy, *Intelligence and Security in a Free Society: Report of the first Independent Review of Intelligence and Security in New Zealand* (Independent Review of Intelligence and Security, 29 February 2016).
[215] This collection consisted of: New Zealand Security Intelligence Act 1969; Government Communications Security Bureau Act 2003; Inspector-General of Intelligence and Security Act 1996; and Intelligence and Security Committee Act 1996.
[216] See (18 August 2016) 716 NZPD 2680, particularly the introductory comments of his Hon Christopher Finlayson.

activities an intelligence agency may be authorised to do are largely geared towards the gathering of evidence *ex ante*, which is in contrast to the New Zealand Police and other law enforcement officers who do a substantial amount of evidence gathering *ex post facto*.

An intelligence agency must seek authorisation to carry out any activity that would otherwise be unlawful;[217] except in a "situation of urgency" or when a very urgent situation arises.[218] If granted, an intelligence warrant is issued, which is differentiated into two types. A type 1 warrant is required to carry out powers in relation to New Zealand citizens or permanent residents.[219] Type 2 warrants cover any other situation where a type 1 warrant is not required.[220] Several criteria is required to be met before an intelligence warrant can be authorised.[221]

A broad range of activities become authorised following the granting of an intelligence warrant.[222] The NZSIS and GSCB have further specific activities that become authorised to give effect to an intelligence warrant.[223] For example, both agencies become authorised to access an information infrastructure, or class of information infrastructures.[224] Information infrastructure is defined broadly in section 4 to include, inter alia, communications systems and networks, information technology systems and networks, and any communications carried on, contained in, or relating to those systems or networks. Effectively then, New Zealand's intelligence agencies can receive authorisation to lawfully compromise, crack or attack a protected information system or encrypted data. An intelligence warrant though cannot authorise any activity whose purpose is to obtain privileged communication or privileged information of a New Zealand citizen or permanent resident.[225]

3.4.2.6 Effects on stakeholders

It is clear from the above discussion that the surveillance powers and associated duties under the Search and Surveillance Act, the TICSA and other laws can and do

[217] Intelligence and Security Act 2017, s 49.
[218] Section 71 and 72, and 78 respectively.
[219] Section 53. A type 1 warrant differentiates an individual from a class of persons and allows an intelligence agency to carry out powers against both.
[220] Section 54.
[221] See, generally, sections 55-66.
[222] Section 67.
[223] Sections 68 and 69, respectively.
[224] Section 68(1)(c) and 69(1)(a), respectively.
[225] Section 70.

apply to encryption and encrypted communications. For government stakeholders, law enforcement officers generally have the power to use interception devices to intercept and collect communications, telecommunications and call associated data (whether they are encrypted or not) in order to investigate a crime pursuant to the surveillance device regime of the Search and Surveillance Act. The interception may be done by the law enforcement themselves and/or with the assistance of the network operator or service provider. Under the TICSA, networks operators are required to make their networks interception capable to allow lawful access by law enforcement, and network operators and service providers have a duty to give reasonable assistance to intercept or collect the communications sought. A company like WhatsApp that is providing end-to-end encryption would be subject to the duty of reasonable assistance but not the requirement of making their service interceptable as it is not a network operator. As with the reasonable assistance duty under computer system searches, there is some ambiguity as to what constitutes reasonable assistance. It appears that requiring or requesting a service provider such as WhatsApp to explain how their service works, including how the encryption and security systems function, is reasonable. However, it would not be reasonable to require providers to intentionally weaken the security of their systems or potentially compromise the privacy of their users, which what was Apple was being required to do by the FBI. The use of encryption for purposes of preserving information security and protecting user privacy are a legitimate business reasons and goals. Therefore, providers should be able to lawfully decline any request for assistance from law enforcement that negatively impacts or compromises the security of its systems and the privacy of its users. To require otherwise may be unfair or unjust.

For business stakeholders, network operators and service providers are not required to decrypt any communications if they themselves have not provided the encryption. While networks operators are required to make their networks interception capable, they have no general duty to decrypt and make those intercepted encrypted communications intelligible when they have no control over the encryption process.[226] This makes sense because while lawful access legislation have always required that telephone calls be tappable by law enforcement, there is no corresponding duty on the part of network operators to ensure that any recorded telephone conversations are

[226] Telecommunications (Interception Capability and Reprinted as at Security) Act 2013, s 24(4).

understandable or intelligible since they cannot control or prevent the conversing parties from speaking in codes or ciphers (e.g., in a language only understood by them). It should be noted that the above duties and obligations under the TICSA are only applicable to network operators and service providers involved in telecommunications and communications.

For the general public and users, they are free to use encryption and encrypt their communications. While the TICSA imposes duties on telecommunications network and services, there is no prohibition against users from using their own encryption on such telecommunications networks or services. Furthermore, the surveillance powers under the Search and Seizure Act do not have a provision similar to Section 130 on computer system searches that authorises the forced disclosure of access information on the part of the person under surveillance. There is no express authority in the Search and Surveillance Act to compel a person subject to surveillance warrant to decrypt or provide access information to communications that are being intercepted. This is reasonable given that the essence of surveillance is confidentiality and discreteness in order to capture people's communications (including incriminating statements) as they are being made in real time. However, if the communication is no longer in transit and is stored in some form (e.g., an encrypted email has already been sent or received), then it may be subject to search and seizure measures including duties of reasonable assistance and forced disclosure of access information under Section 130 of the Search and Surveillance Act. However, as explained previously, such search and seizure powers are subject to a person's right against self-incrimination.

3.4.3 PRODUCTION ORDER

3.4.3.1 Nature and grounds

Production orders are a new investigatory regime introduced by the Search and Surveillance Act.[227] Pursuant to a production order, a person must provide "any documents described in the order that are in his or her possession or control, and to disclose to the best of his or her knowledge or belief the location of any documents not in his or her possession of control".[228] Productions orders may be issued in relation to any

[227] Law Commission, *Review of the Search and Surveillance Act 2012*, para 14.1.
[228] Warren Young, Neville Trendle and Richard Mahoney, *Search and Surveillance: Act and Analysis* 10.

offence "for which a search warrant is available. The order is issued in respect of a person rather than premises".[229] They are intended to be a less intrusive alternative to search warrants,[230] and largely represents a formalisation of the voluntary request procedure utilised by regulatory agencies to obtain relevant documents regarding persons of interest from third parties.[231] Productions order are mainly applicable to documents,[232] and are mostly useful for officially requesting documents about individuals from businesses that collect such data, such as customer records for example.[233] The use of productions orders is

> a suitable means of evidence-gathering only in circumstances where the subject (such as a bank or professional adviser) is likely to be co-operative, but because of fiduciary obligations is unwilling to provide financial or other business records relating to a client without a judicial order.[234]

The introduction of the production order regime was not intended to limit the ability of law enforcement officers to unofficially obtain information from third parties, as long as they did so lawfully and the parties could comply voluntarily.[235] This is the same rationale underlying production orders under the Convention on Cybercrime. According to the drafters of the Convention, 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.[236] Production orders are also considered

> beneficial to third party custodians of data, such as ISPs, who are often prepared to assist law enforcement authorities on a voluntary basis by providing data under their control, but who prefer an appropriate legal basis for such assistance, relieving them of any contractual or non-contractual liability.[237]

In relation to a production order, an enforcement officer must have reasonable grounds to suspect that an offence has been, is being, or will be committed and that this offence would also allow for an application for a search warrant.[238] Additionally, an enforcement officer must have reasonable grounds to believe that the documents sought

---

[229] Warren Young, Neville Trendle and Richard Mahoney, *Search and Surveillance: Act and Analysis* 139.
[230] Law Commission, *Review of the Search and Surveillance Act 2012*, para 14.10.
[231] Law Commission, *Review of the Search and Surveillance Act 2012*, para 14.11.
[232] Search and Surveillance Act 2012, s 71(1).
[233] Law Commission, *Review of the Search and Surveillance Act 2012*, para 14.1.
[234] Warren Young, Neville Trendle and Richard Mahoney, *Search and Surveillance: Act and Analysis* 137.
[235] See *R v Alsford* [2017] NZSC 42 at [29].
[236] Council of Europe, Explanatory Report to the Convention on Cybercrime, para 171.
[237] Council of Europe, Explanatory Report to the Convention on Cybercrime, para 171.
[238] Search and Surveillance Act 2012, s 72(a).

constitute evidential material for the offence and that these documents are in the possession or control of the person who is the subject of the order or will come into their possession while the order is in force.[239] "Possession or control" carries its ordinary meaning of being located at the place. Other than only applying to documents, the conditions for obtaining a production order are essentially the same as those pertaining to search warrants.[240]

In fact, being otherwise able to apply for a search warrant in respect of the documents sought is a prerequisite for an enforcement officer to be able to use the production order regime.[241] For example, if a regulatory agency's governing legislation provides for a search warrant to be obtained only in a limited number of circumstances, then a production order is only available to that enforcement officer in those specific circumstances. Furthermore, if a regulatory agency's warrantless powers of search contained in their governing legislation would facilitate the warrantless search for documents, then the regulatory agency does not need to make use of the production order regime in order to acquire those documents.

For example, in November 2014, a regulatory officer enforcing the Fisheries Act 1996 wrote to a telecommunications company requesting the provision of call data and text messages in relation to some cell phone numbers.[242] This information was supplied and led to charges being laid against three people. On appeal from the District Court decision, the appellants argued that the regulatory officer should have obtained a production order to get that information because of the interference in privacy rights that provision of the information entailed.[243] The High Court held that, apart from some limited circumstances, the Fisheries Act 1996 did not provide its regulatory officers with the power to obtain a search warrant,[244] and in order to obtain a production order a regulatory officer must first have the ability to obtain a search warrant.[245] Therefore, it was not possible for the regulatory officer to obtain a production order in the

---

[239] Section 72(b).
[240] See *R v Alsford*, at [18]. Many of the provisions governing the production order regime refer to provisions that specifically govern the search warrant regime, incorporating their strictures. See, for example, the references in Search and Surveillance Act 2012, ss 71(2)(b), 72(a), and 77.
[241] Search and Surveillance Act 2012, s 71(1).
[242] See *Wikitera v Ministry for Primary Industries*.
[243] *Wikitera v Ministry for Primary Industries*, at [15].
[244] *Wikitera v Ministry for Primary Industries*, at [17].
[245] *Wikitera v Ministry for Primary Industries*, at [23].

circumstances of this case.[246] The powers of warrantless search conferred by the Fisheries Act 1996, however, is "clear and unambiguous",[247] and would have permitted the warrantless search of a telecommunications company's place of business.[248] Therefore, the call data and text messages were obtained lawfully, and somewhat less intrusively than an actual search would have entailed.

An order can remain in force for up to 30 days.[249] Therefore, an order can relate to documents that do not yet exist but will come into existence while the order is in force.[250] A production order is required to specify whether the documents are required to be produced on one occasion only or on an ongoing basis.[251] It appears that call associated data and the content of telecommunications cannot be brought into existence, i.e. stored specifically for meeting the requirements of an ongoing production order if such data and content is not ordinarily stored "in the normal course of its business", due to the definition of the word "document" in the Search and Surveillance Act.[252] It is this distinction that also differentiates production orders from surveillance as production orders do not authorise interception.[253] An interesting matter arises when considering the ongoing nature of production orders, as there is overlap between the production order regime and an interception warrant obtained under the surveillance device regime. Both allow for the handing over of the content of telecommunications that have not been created and sent yet but will come to be created and sent within the time frame of the order/warrant to an enforcement agency. The key distinction is that production orders are only applicable to documents that are normally stored during the course of a business' operations whereas interception warrants allow for the business to now intercept and store these telecommunications for handover to the enforcement agency regardless of whether they would store the telecommunications during the ordinary course of its business or not. Therefore, it seems that a business' data retention policy is foundational to which regime may be appropriate to use by an enforcement agency. How long each regime may remain

[246] *Wikitera v Ministry for Primary Industries*, at [15].
[247] *Wikitera v Ministry for Primary Industries*, at [36].
[248] *Wikitera v Ministry for Primary Industries*, at [40].
[249] Search and Surveillance Act 2012, s 76.
[250] Law Commission, *Review of the Search and Surveillance Act 2012*, para 14.9.
[251] Search and Surveillance Act 2012, ss 71(2)(g) and 75(2)(d).
[252] See Law Commission, *Review of the Search and Surveillance Act 2012*, para 14.9.
[253] Law Commission, *Review of the Search and Surveillance Act 2012*, para 14.20.

in force is another consideration. Production orders only remain in force for a period of 30 days,[254] whereas an interception warrant can remain in force for a period of 60 days.[255]

The production order regime largely represents a codification of the voluntary request procedure regulatory agencies utilised prior to the Search and Surveillance Act being enacted. As such, it is mostly used when requesting information from third parties about the person of interest in an investigation. However, there is no reason why a production order cannot be used directly against persons or entities of interest, such as a business for example. It is only applicable against documents, both physical and digital, and includes metadata and the content of telecommunications. Upon meeting the relevant thresholds and being issued, it requires that the person being served with the production order provide the documents stated in the order to the officer who applied for the order. A production order cannot be used to require the production of documents that would not have otherwise existed. Failure to comply with a production order can result in imprisonment for a term not exceeding one year or, in the case of a body corporate, to a fine not exceeding $40,000.[256]

3.4.3.2 Documents and subscriber information

The principal object of production orders are documents. Under the Search and Surveillance Act, "document" is specifically defined as including call associated data and the content of telecommunications that a network operator has the storage capability for, and does in fact store that data during the normal course of its business.[257] "Call associated data" and "network operator" have the same meaning as provided in section 3(1) of the TICSA.[258] In contrast to surveillance and interception powers, production orders pertain to "stored or existing data, and do not include data that has not yet come into existence such as traffic data or content data related to future communications".[259] The term document includes both physical and digital versions of information and encompasses the rendering of one into the other – for example, when a customer's power consumption data is stored electronically but provided to the requesting officer in a

[254] Search and Surveillance Act 2012, s 76.
[255] Search and Surveillance Act 2012, s 55.
[256] Search and Surveillance Act 2012, s 174.
[257] Search and Surveillance Act 2012, s 70.
[258] Search and Surveillance Act 2012, s 70.
[259] Council of Europe, Explanatory Report to the Convention on Cybercrime, para 170.

physical format. This is because the wide definition given to the term document in section 217 of the Crimes Act 1961 is likely to be applicable:

> document means a document, or part of a document, in any form; and includes, without limitation, –
> (a) any paper or other material used for writing or printing that is marked with matter capable of being read; or
> (b) any photograph, or any photographic negative, plate, slide, film, or microfilm, or any photostatic negative; or
> (c) any disc, tape, wire, sound track, card, or other material or device in or on which information, sounds, or other data are recorded, stored (whether temporarily or permanently), or embodied so as to be capable, with or without the aid of some other equipment, of being reproduced; or
> (d) any material by means of which information is supplied, whether directly or by means of any equipment, to any device used for recording or storing processing information; or
> (e) any material derived, whether directly or by means of any equipment, from information recorded or stored or processed by any device used for recording or storing or processing information.[260]

The meaning of documents that may be subject to a production order is quite expansive and covers "disks and data storage devices, and any material by means of which information is supplied to a device used for recording, storing or processing information".[261]

Production orders under the Search and Surveillance are similar to those in the Convention on Cybercrime although the latter explicitly refers to stored computer data rather than the generic term documents. Article 18 of the Convention on Cybercrime gives law enforcement authorities the power to order any 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".[262] Further, "a service provider offering its services" may be required "to submit subscriber information relating to such services in that service provider's possession or control."[263] The meaning of service provider under the Convention is broader and is not limited to those providing telecommunications services.

One specific type of data that is the ideal target of a production order is subscriber information. The Convention on Cybercrime places much emphasis on the usefulness of production orders to get subscriber information in criminal investigations. While the

---

[260] See *Adams on Criminal Law*, at [SS70.02].
[261] Warren Young, Neville Trendle and Richard Mahoney, *Search and Surveillance: Act and Analysis* 135.
[262] Convention on Cybercrime, art 18(1).
[263] Convention on Cybercrime, art 18(1).

Search and Surveillance Act does not expressly mention the term subscriber information (as opposed to call associated data), documents that may subject to a production order can include those that contain subscriber information. Under Article 18 of the Convention on Cybercrime, subscriber information is "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*" that 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".[264] Subscriber information basically covers information about the identity of a subscriber and any information about him or her that is normally recorded and stored by the service provider that is not traffic or content data. Subscriber information may be kept by the service provider in the form of computer data or paper records.[265] The term subscriber can be understood as encompassing "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".[266]

Subscriber information is extremely relevant and useful in criminal investigations because they provide valuable data about the subscriber and the services being used. As explained in the Explanatory Report to the Convention on Cybercrime:

> subscriber information may be needed primarily in two specific situations. First, subscriber information is needed to identify which services and related technical measures have been used or are being used by a subscriber…. Second, when a technical address is known, subscriber information is needed in order to assist in establishing the identity of the person concerned. Other subscriber information, such as commercial information about billing and payment records of the subscriber may also be relevant to criminal investigations, especially where the crime under investigation involves computer fraud or other economic crimes.[267]

[264] Convention on Cybercrime, art 18(3) (emphasis added).
[265] Council of Europe, Explanatory Report to the Convention on Cybercrime, para 177.
[266] Council of Europe, Explanatory Report to the Convention on Cybercrime, para 177.
[267] Council of Europe, Explanatory Report to the Convention on Cybercrime, para 178.

Under the Convention on Cybercrime, a service provider is only required to provide "computer data or subscriber information that are in [its] possession or control".[268] Absent data retention laws or other similar rules, there is no generally duty on the part of service providers to keep records of the identities of their subscribers or to monitor or record how their subscribers use their services.[269] Based on the Convention on Cybercrime, production orders do not

> impose an obligation on service providers to keep records of their subscribers, nor would it require service providers to ensure the correctness of such information. Thus, a service provider is not obliged to register identity information of users of so-called prepaid cards for mobile telephone services. Nor is it obliged to verify the identity of the subscribers or to resist the use of pseudonyms by users of its services.[270]

Service providers may therefore choose not to keep records about its subscribers as part of their ordinary course of business and, as result, cannot be compelled to do otherwise by means of a production order. In cases where a service provider does not keep records about its subscribers, law enforcement officers may, as an alternative, resort to the use of surveillance or interception powers to gather content, traffic and other data and communications about the subscriber in real-time either on its own or with the assistance of the service provider if the latter has the technical means to do so.

3.4.3.3 Encrypted documents and access information

The use of encryption may diminish the efficacy of production orders. While law enforcement officers may be able to demand encrypted documents and data from a person or service provider, since the documents are in an unintelligible form they offer very little in evidentiary usefulness or value. With production orders, persons and service providers are only required to give documents and data (whether encrypted or not) in their possession or control and there is no legal obligation to decrypt. Consequently, for a business offering a service that is end-to-end encrypted, there is no onus to subvert their technology to comply with a production order as the unencrypted "documents" are not stored "in the normal course of its business". They may still be required to produce the unintelligible encrypted data, however. Section 78(c) of the Search and Surveillance Act

[268] Council of Europe, Explanatory Report to the Convention on Cybercrime, para 172.
[269] Council of Europe, Explanatory Report to the Convention on Cybercrime, para 172.
[270] Council of Europe, Explanatory Report to the Convention on Cybercrime, para 181.

states that the person producing the document may be required to reproduce, or assist in the reproduction, of the document – in this case, the encrypted data – in a "usable form". "Usable form" is not defined in the Search and Surveillance and no case law exists specifically regarding its interpretation. However, the phrase is readily used in many other statutes.[271] Though no clear definition arises from the case law, the phrase seems to imply that usable form is whatever is reasonable and functional in the circumstances.[272] Furthermore, and as mentioned above, what constitutes useable form for the purposes of TICSA has been specified by the Governor-General by Order in Council. This is likely to be persuasive within the production order context should the matter ever go to court. It appears though that usable form pertains to the format of the document rather the content of the document itself. For example, an encrypted email that is printed on paper is in a usable form or format even though the content is undecipherable. Further, based on the above discussion on surveillance powers, usable does not appear to mean intelligible. Recall that network operators and service providers under the TICSA are not required to decrypt communications when they have no control over the means of encryption.

Encryption though is less of a hindrance when it comes to non-content data such as traffic data, subscriber data, and other metadata. The latter forms of data are much harder to conceal or keep private even with the use of encryption since they are mainly in the possession or control of the service provider rather than the end user. Encrypted communications are known for leaking metadata. For instance, while the content of an email is encrypted, the relevant service providers or network operators (e.g., the user's email provider and ISP) could be in a position know which email addresses sent and received the email and at what time. Even an end-to-end encryption service like WhatsApp can produce metadata that can provide information about its users and could be the subject of a production order. The metadata associated with the content of a telecommunication are producible.[273]

Whether access information is producible pursuant to a production order depends on the circumstances. A production order normally applies to documents that are in

[271] Across 25 statutes according to a search of legislation.govt.nz. For example, see, Reserve Bank of New Zealand Act 1989; Corporations (Investigation and Management) Act 1989; Animal Products Act 1999; and Wine Act 2003.
[272] See, generally, *Houghton v Saunders* [2014] NZHC 2229 at [419 – 423].
[273] Any encryption of this metadata would likely be company provided. Therefore, decryptable pursuant to Search and Surveillance Act 2012, s 130.

existence at the time a production order is served.[274] It cannot be used to compel a person to create or prepare a document in response to a production order.[275] With respect to ongoing production orders, the Law Commission opines that, due to the passive wording of the relevant provision in the Search and Surveillance Act, a production order cannot be used to require a person to create documents that would not have otherwise existed.[276] There is an important distinction though 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 saved or stored digitally as computer files but can also be printed out 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. It should be noted as well that a production order "may also require the provision of oral information: if any of those documents are not, or are no longer, in the person's possession or under his or her control, he or she must disclose the whereabouts of those documents to the best of his or her knowledge or belief".[277] A person or service provider may be compelled to produce their encryption keys as documents or disclose the location of those keys. However, 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 a certain situations. For example, requiring Apple to give up the encryption keys that it uses to sign, authenticate or secure its products and service would not appear reasonable.

In contrast, passwords do not have to be written down or saved in a document or file and can be stored in a person's mind. Unless the passwords are stored or written down in some form, a person or service provider cannot be compelled to produce or write down their passwords pursuant to a production order. As with Section 130, production orders are subject to right against self-incrimination under Section 138 of the Search and Surveillance Act.[278] As noted by Young, Trendle and Mahoney, a production order "is generally subject to the privilege regime… of the Act. If the person refuses to produce a document on the grounds that it is privileged, the enforcement officer may apply to a

[274] See Search and Surveillance Act 2012, s 71(2)(g)(i).
[275] See *Adams on Criminal Law,* at [SS136.11].
[276] Law Commission, *Review of the Search and Surveillance Act 2012*, para 14.9.
[277] Warren Young, Neville Trendle and Richard Mahoney, *Search and Surveillance: Act and Analysis* 141.
[278] Search and Surveillance Act 2012, s 138(1).

judge under s 139 for an order determining whether the claim is valid".[279] They further explain, "s 51(3) of the Evidence Act defines the class of 'information' that is subject to such privilege as including documents only when they are prepare or created 'after and in response to a requirement'".[280] A request to produce or write down passwords not already in existence would be "after and in response" to a production order and thus covered under the privilege. This situation may however be subject to the duties under Section 130 of the Search and Surveillance Act on computer system searches discussed above.

3.4.4 EXAMINATION ORDER

An examination order requires a specified person to attend compulsory questioning when they have previously refused to do so.[281] One of the main rationales for the introduction of an examination order regime was to assist in situations where people are unable to cooperate on grounds of professional confidentiality.[282] The specified person must have been given a reasonable opportunity to provide the information and has not done so.[283] It can only be sought by a constable who is of or above the level of inspector and comes in the form of a court order. The regime is governed by Sections 33 to 43 of the Search and Surveillance Act and are available in business and non-business contexts:

> In a business context, it is directed to those who may hold information in a professional capacity (such as an officer of a financial institution or an accountant) that they do not wish to disclose voluntarily – for example, on account of their fiduciary duty to the client. In the non-business context, it is directed to those (including suspects) who may hold information that they are not willing to disclose voluntarily.[284]

While examination orders do require a person to attend compulsory questioning, the privilege against self-incrimination is available.[285] Furthermore, examination orders can only be made in relation to persons where there are reasonable grounds to believe that the person has information that constitutes evidential material in respect of the offence.[286] A judge must also be satisfied that "it is reasonable to subject the person to

---

[279] Warren Young, Neville Trendle and Richard Mahoney, *Search and Surveillance: Act and Analysis* 11.
[280] Warren Young, Neville Trendle and Richard Mahoney, *Search and Surveillance: Act and Analysis* 140.
[281] See Law Commission, *Review of the Search and Surveillance Act 2012*, para 16.2.
[282] At [16.6].
[283] Search and Surveillance Act 2012, ss 34(d) and 36(d).
[284] Warren Young, Neville Trendle and Richard Mahoney, *Search and Surveillance: Act and Analysis* 7.
[285] Search and Surveillance Act 2012, s 138; see also Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act: A Commentary* 911.
[286] See Search and Surveillance Act 2012, s 34(b) and s 36(b).

compulsory examination" after taking into consideration several factors before making an examination order.[287] Failing to comply with an examination order renders an individual liable for an imprisonment term not exceeding one year or, in the case of a body corporate, a fine not exceeding $40,000.[288]

Examination orders have limited applicability to the issue of encryption and lawful access to encrypted data. Although evidential material may be understood in the broad sense of "evidence of the offence, or any other item, tangible or intangible, of relevance to the investigation of the offence" provided for in the definition of those words,[289] it would be a stretch to consider access information such as passwords as evidence of an offence. And even if they are considered evidential material, there would a stronger claim that providing them would infringe on a person's right against self-incrimination.[290] In addition, any request for "access information" is likely to be by way of Section 130 of the Search and Surveillance Act because encrypted electronic devices and encrypted data storage devices are only likely to come into evidence following the exercise of a search power thereby triggering the provisions in Part Four of the SSA, rather than by way of a person of interest not being given a reasonable opportunity to provide the information and not having done so, which is a condition to be met before an examination order can be made.[291] Lastly, at minimum, an examination order can only be made in respect of an offence carrying a minimum imprisonment term of five years. Consequently, a police officer could not meet the requirements for an examination order if they wished to follow up a person of interest's refusal to comply with a request under Section 130 with an examination order to obtain the access information because a violation of Section 130 in relation Section 178 of the Search and Surveillance Act only carries a maximum penalty of imprisonment for a term not exceeding three months.[292] It can also be argued that the examination order should be sought in relation to an investigation of the main crime and not the refusal to provide the access information. It is also worth noting that in a non-business context, examination orders can only be used in cases of serious or complex

[287] Section 38(b).
[288] Section 173.
[289] See Search and Surveillance Act 2012, s 3 (definition of "evidentiary material").
[290] Search and Surveillance Act 2012, s 138.
[291] Section 34(d) and s 36(d).
[292] Search and Surveillance Act 2012, s 178.

fraud and those committed by organised criminal groups, which significant limits that applicability of examination orders to members of the general public.[293]

Whether a provider of encrypted messaging service such as WhatsApp or Facebook Messenger for example, could be required to explain how their system works pursuant to an examination order would depend on the interpretation of the phrase "of relevance to the investigation of the offence" in the definition of "evidentiary material". However, the alleged offence is the lynchpin around which the evidence must refer and the examination order should relate to that. The workings of a provider's system are only obliquely connected to that offence because it simply provides the medium by which the alleged offenders communicate. Consequently, an examination order is unlikely to be successful if used in such a manner. Examination orders have not been used by the Police since the commencement of the Search and Surveillance Act.[294] There is, therefore, no case law regarding the interpretation of this phrase in the context of an examination order.

3.4.5 DECLARATORY ORDERS

Only a judge may make a declaratory order,[295] as a declaratory order is a statement by a judge that they are satisfied that the use of a device, technique, or procedure, or the carrying out of an activity is, in the circumstances, reasonable and lawful.[296] It is advisory in nature and does not bind any future court to make the same determination.[297] Declaratory orders are available to any enforcement officer.

Declaratory orders provide a way for a law enforcement authority to test their reasoning for an activity that may intrude on reasonable expectations of privacy,[298] thereby preventing unreasonable searches from happening and encouraging public confidence in the justice system.[299] This is particularly useful considering the rapid

[293] Search and Surveillance Act 2012, s 36(a).
[294] See the individual New Zealand Police *Annual Reports,* ranging from the 2011/2012 to the most recent 2016/2017.
[295] Search and Surveillance Act 2012, s 68.
[296] Section 65.
[297] Section 65(2).
[298] Law Commission, *Review of the Search and Surveillance Act 2012*, para 6.37.
[299] Law Commission, *Review of the Search and Surveillance Act 2012*, para 6.38.

development of technology,[300] and the principle that intrusions into individual's private lives should be pursuant to some form of authorisation.[301]

Since the Search and Surveillance Act's commencement, a declaratory order has only been applied for, and issued, once.[302] This application sought a statement regarding the reasonable and lawful use of drug detection dogs at consenting domestic courier depots.[303] Because declaratory orders can only be made in relation to uses or activities that a judge considers to be reasonable and lawful, they cannot be used to authorise otherwise unlawful activity.

For example, the installation of a keystroke logger, spyware, or remote access software would invariably entail the unauthorised access to a computer system, which would contravene section 252 of the Crimes Act 1961.[304] This does not mean that a law enforcement officer cannot use any form of penetration tools or cracking techniques to access an electronic device or other data storage device that has been seized pursuant to a search power, as they are able to: "use any reasonable measures to access a computer system or other data storage device (in whole or in part) located at the place, vehicle, or other thing if any intangible material that is the subject of the search may be in that computer system or device."[305] It appears the law enforcement officer could legitimately use password cracking tools, decryption software and other techniques to gain access to encrypted data or protected computers pursuant to a valid search and seizure. Such instances of law enforcement hacking would generally not be considered unauthorised or illegal access under the Crimes Act 1961 since it would be done with legal authorisation.[306] A declaratory order is a suitable way for law enforcement to get formal confirmation from the courts that the use of such tools and techniques for carrying a digital search and seizure is reasonable and lawful. However, law enforcement officers are unable to use such methods or measures in order to conduct surveillance or a remote access search as no methods of cracking fall within the scope of either the surveillance device regime or a remote access search.

---

[300] Law Commission, *Review of the Search and Surveillance Act 2012*, para 6.36.
[301] Law Commission, *Review of the Search and Surveillance Act* 2012, para 6.40. See also *Adams on Criminal Law,* at [SS6.01].
[302] See the individual New Zealand Police *Annual Reports*.
[303] New Zealand Police *Annual Report 2015/2016* (online pdf version) at 152.
[304] See Law Commission, *Review of the Search and Surveillance Act 2012*, para 6.7.
[305] Search and Surveillance Act 2012, s 110(h).
[306] Crimes Act 1961, ss 249 and 252.

3.5 Human rights and other safeguards and protections

As seen in the preceding sections, there are quite a number of existing laws and rules that already regulate and control how encryption is developed, implemented and used. The Search and Surveillance Act is not explicitly called or characterised as an encryption law but, as shown above, the investigatory powers and measures contained therein can and do affect access to and use of encryption. Law enforcement powers though only represent one albeit major part of the tacit and implicit legal framework that regulates encryption. An integral aspect of law enforcement and criminal investigations requires the consideration and protection of the rights of persons. Human rights therefore constitute the other major part of the laws and legal principles that are relevant to encryption. This is confirmed by the purpose of the Search and Surveillance Act, which expressly states that "the investigation and prosecution of offences" must be done "in a manner that is consistent with human rights values".[307] It is necessary then to balance the goal of effective and adequate law enforcement with human rights principles and considerations.

Gaining access to encrypted data and communications as part of a criminal investigation involves the issue of lawful access. As the principle of lawful access manifests itself in New Zealand's legislation, a corollary manifestation in New Zealand's jurisprudence can be seen regarding the applicability of existing human rights protections and other safeguards. The most significant protections, and those that will be discussed more fully below, are security from unreasonable searches and seizures and the right against self-incrimination. Other human rights protections, such as the minimum standards of criminal procedure contained in section 25 of the New Zealand Bill of Rights Act 1990 (NZBORA), find expression insofar as they are evidenced in the application of the more significant protections. Safeguards may also be contained in the wording of a provision itself (e.g., the use of the words "reasonable" and "necessary" in section 130 of the Search and Surveillance Act and section 228 of the Customs and Excise Act 2018).

Lastly, two considerations should always be kept in mind when determining how existing human rights protections and other safeguards are being applied to frame or limit the principle of lawful access as it operates in practise. First, that these human rights

[307] Search and Surveillance Act 2012, s 5.

protections and other safeguards are only enforceable against state action.[308] It is not possible to allege that a business has undertaken an unreasonable search of an individual's personal information. Second, that NZBORA is not overriding legislation. While an interpretation of a provision in a statute that is consistent with NZBORA is preferred,[309] if a provision states in clear terms something that is inconsistent with a right contained in NZBORA, then that provision cannot be struck down.

3.5.1 RIGHT AGAINST UNREASONABLE SEARCH AND SEIZURE

3.5.1.1 Reasonable expectation of privacy and reasonableness

In the same way that the powers of search and seizure are critical for law enforcement officers to gain access to encrypted data and communications, the right against unreasonable search and seizure provides an essential counterbalance for protecting the rights of both members of the general public and businesses.

Section 21 of the NZBORA states "Everyone has the right to be secure against unreasonable search or seizure, whether of the person, property, or correspondence or otherwise".[310] The right against unreasonable search and seizure is generally applicable to the powers and measures available under the Search and Surveillance Act. The 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".[311] It includes "not only to the interception of mail… but also to the electronic interception of private conversations and other forms of surveillance".[312] In addition, reference to "correspondence" under section 21 means that secrecy of correspondence is also protected under this broad right.

Frequently, challenges to the admissibility of evidence allege that it has been improperly obtained because the evidence was gathered in contravention of section 21 of the NZBORA. Because the word "unreasonable" requires interpretation, how the protection against unreasonable search and seizure applies has been expounded in case law. A search and seizure warrant issued in accordance with the governing statute and executed in compliance with any applicable provisions of the Search and Surveillance Act and best practise will be generally considered reasonable.

---

[308] New Zealand Bill of Rights Act 1990, s 3.
[309] Section 6.
[310] New Zealand Bill of Rights Act 1990, s 21.
[311] Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act: A Commentary* 904.
[312] Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act: A Commentary* 904.

"Search" and "seizure" are not defined in NZBORA. In many decisions, they have been used interchangeably.[313] Search can be understood in "its ordinary sense of consciously looking for something or somebody, whether or not through the use of technology".[314] An investigation would be considered a search "to the extent that it intrudes significantly on personal privacy, seeks an object or information traditionally considered private, and/or occurs in a place closely associated with traditional privacy rights".[315] The word "surveillance" does not appear in NZBORA at all. However, in the Supreme Court decision of *Hamed v R,*[316] which concerned the unreasonableness of a police surveillance operation, the words "search" and "surveillance" were conflated for the purposes of the section 21 of NZBORA analysis that the Court undertook. Therefore, the principles arising from the case law pertaining to what constitutes an unreasonable search is applicable to searches, seizures, and surveillance. Consequently, section 21 of the NZBORA is directly applicable to warranted and warrantless searches, surveillance device warrants, and production orders. Section 21 is also relevant to declaratory orders because declaratory orders require a judge to determine the reasonableness of a specified use of a device, technique, procedure, or activity.

New Zealand formally adopted the definition of a search as being a police activity that invades a reasonable expectation of privacy in the 2011 *Hamed v R* decision.[317] In the more recent 2017 decision of *R v Alsford,*[318] the Supreme Court considered that the protection afforded by a reasonable expectation of privacy is:

> directed at protecting a "biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination by the state" and includes information "which tends to reveal intimate details of the lifestyle and personal choices of the individual".[319]

The reasonable expectation of privacy is twofold. First, the person complaining of a breach must have a subjective expectation in the place or thing being searched, or time of the police activity. Second, that expectation must be one that society is prepared to

[313] *Henderson v AG* [2017] NZHC 606 at [38].
[314] Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act: A Commentary* 937.
[315] Paul Rishworth and others, *The New Zealand Bill of Rights* 425.
[316] *Hamed v R* [2011] NZSC 101.
[317] At [163]. Adopted from the Canadian Supreme Court decision of *R v Wise* [1992] 1 SCR 527.
[318] *R v Alsford* [2017] NZSC 42.
[319] At [63].

recognise as reasonable.[320] If both these limbs are met, then the conduct of a regulatory agency will be a search for the purposes of section 21 of NZBORA. It should be noted that there is no formal or distinct right to privacy in the country. While other countries have interpreted the existence of an independent, separate or standalone right to privacy based on or as an essential part of the right against unreasonable search and seizure, this has not been done in New Zealand. Therefore, claims for privacy protections must be based on the application of section 21 of the NZBORA, the Privacy Act 1993 and other relevant laws and legal rules.

Searches of computers and other electronic devices though "raise special privacy concerns, because of the nature and extent of the information that they hold."[321] When assessing the significance of privacy interests, outward signs of an increased subjective expectation of privacy is to be taken into account. For example, a PIN locked electronic device indicates a slightly higher subjective expectation of privacy.[322] The focus of the second limb is on the inherent privacy of the area or thing being searched or observed – the search or surveillance happening to reveal unlawful activity cannot be used to justify what would otherwise be an unlawful search.[323] The second limb is also "a contextual one, requiring consideration of the particular circumstances of the case".[324]

It is relatively straightforward to obtain information contained in a PIN locked device that is not also encrypted. However, encrypting a device makes the information only obtainable to those who hold the access information. Therefore, encrypted information is only supposed to be seen by those who hold the access information. An encrypted electronic device, other data storage device, or folder/file in that device is likely to be taken to indicate that there is an increased subjective expectation of privacy in that – especially if it is a feature that must be enabled. It is also likely that this heightened subjective expectation would be reasonable; society would be prepared to recognise the inherent privacy exhibited in encrypted information.

---

[320] See Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act: A Commentary* 936.
[321] *Dotcom v AG*, at [191]. Indeed, the Law Commission recommends that a warrant should be required before an electronic device can be searched if an electronic device has been found during a warrantless search. Only certain urgent circumstances would provide exceptions. See Law Commission, *Review of the Search and Surveillance Act 2012*, para 12.9.
[322] *W v R* [2017] NZCA 522 at [30].
[323] At [38].
[324] *R v Alsford,* at [63].

Once it is established that a search has taken place – i.e. a reasonable subjective expectation exists in a thing or place and it is an expectation society recognises – the question then becomes whether that search itself was unreasonable.[325] There is a reasonableness standard that must be complied with.[326] The requirement of reasonableness though is "an elastic concept not entirely susceptible of close definition".[327] Depending on the circumstances, a search can be unreasonable if "the search itself [is] unreasonable or if… [it] is carried out in an unreasonable manner".[328] To determine reasonableness, "a court will look at the nature of the place or object being searched, the degree of intrusiveness into the privacy of the person affected and the reason why the search was occurring".[329] This "situation-specific assessment of reasonableness" means that "reasonableness can only be assessed in light of the facts and circumstances of a particular case".[330] As legal commentators further explain,

> The powers and obligations [under the Search and Surveillance Act] codify many aspects of the common law on reasonableness under s 21 of the New Zealand Bill of Rights Act 1990 prior to the passage of this Act. If a search is carried out in conformity with this and subsequent actions, it is *likely* to be reasonable under s 21. But there is still an overriding requirement of reasonableness; if the search is carried out in a manner that is unreasonable in the particular circumstances, it will be in breach of s 21 even if authorised under these provisions.[331]

Depending on the particular context or facts of the situation, it is possible for a search or surveillance that is conducted pursuant to a warrant to be considered unreasonable "if it constitutes an unjustified intrusion on a reasonable expectation of privacy".[332] It is standard for courts to first consider whether the search was lawful, because an unlawful search is almost always unreasonable.[333] The party advocating that an unlawful search is not unreasonable has a "significant persuasive burden".[334] If the breaches are only of a technical or minor nature, or the police had a reasonable yet erroneous belief that they

---

[325] *Henderson v AG,* at [47].
[326] Paul Rishworth and others, *The New Zealand Bill of Rights* 423.
[327] Paul Rishworth and others, *The New Zealand Bill of Rights* 434.
[328] Paul Rishworth and others, *The New Zealand Bill of Rights* 434.
[329] Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act: A Commentary* 937.
[330] Paul Rishworth and others, *The New Zealand Bill of Rights* 434 and 435.
[331] Warren Young, Neville Trendle and Richard Mahoney, *Search and Surveillance: Act and Analysis* 182.
[332] Warren Young, Neville Trendle and Richard Mahoney, *Search and Surveillance: Act and Analysis* 7.
[333] *Hamed v R*, at [174] per Blanchard J. Elias CJ, in a dissenting judgment, considers that an unlawful police search is unreasonable by definition, at [50]. Moreover, Elias CJ would consider that the police would always be acting unlawfully if they did not have specific statutory authority for intruding upon personal freedom, at [38].
[334] At [71] per Elias CJ.

were acting lawfully, then the search can be reasonable.[335] If a regulatory agency relies on evidence that was obtained improperly in a future application for a search warrant, production order, or surveillance device warrant, then this may taint that future application so as to render any evidence obtained from it inadmissible.[336]

3.5.1.2 Information held by third parties

Whether the provision of personal information or other data by a third party to a law enforcement officer or regulatory agency constitutes a search requires the same analysis of what is the reasonable expectation of privacy in that personal information.[337] The Supreme Court has identified the following circumstances that could be included in any such determination:

> (a) the nature of the information at issue;
> (b) the nature of the relationship between the party releasing the information and the party claiming confidentiality in the information;
> (c) the place where the information was obtained; and
> (d) the way the information was obtained.[338]

If it is determinable that the personal information or data held by a third party has the circumstances necessary for a reasonable expectation of privacy to reside in that personal information, then it would have been obtained unreasonably if the third party divulged that information voluntarily.[339] This does not foreclose a regulatory agency from obtaining that information at all; rather, they are required to obtain appropriate statutory authority for that information. For example, by exercising the appropriate warrantless power,[340] or by obtaining a search warrant or a production order.

Access information held by a third party (for example, an IT data service provider) is likely to have a reasonable expectation of privacy reside in that access information. After all, the nature of the information is that it governs access to information and the IT data service provider would have been contracted to provide data security services.

---

[335] At [174] per Blanchard J.
[336] *R v Alsford,* at [92-96].
[337] See *R v Alsford*.
[338] At [63].
[339] At [64]. Contrast this with the position in the United States of America, which holds that information divulged to a third party has no privacy interest; known as the third-party doctrine. However, there are indications that this doctrine may be softening. See *Carpenter v United States of America* 585 US (2018). Of course, the United States of America does not have an equivalent to New Zealand's Privacy Act 1993, which imposes a duty on all New Zealand government agencies and businesses to safeguard an individual's personal information.
[340] See *Wikitera v Ministry for Primary Industries*.

Therefore, if a regulatory agency was to call an IT company inquiring after the access information they held for a business they provided data security for, the IT company would be remiss if they divulged that information without seeing appropriate statutory authority from the regulatory agency.

If a court holds that a search has been unreasonable, then that search produces evidence that has been improperly obtained.[341] Whether the evidence obtained by that unreasonable search is admissible in court is determined under section 30 of the Evidence Act 2006. Both the defendant and the Judge in a criminal proceeding may raise the issue of whether the evidence has been improperly obtained.[342] If such an issue is raised, the Judge is required to find, on the balance of probabilities, whether the evidence has been improperly obtained and then determine whether exclusion of that evidence is proportionate to the impropriety.[343] A number of matters are specified by the Evidence Act 2006 as matters that the court may have regard to when determining whether evidence should be excluded or not.[344]

3.5.1.3 Reasonable assistance

The right against unreasonable search and seizure also touches on the issue of reasonable assistance during the conduct of a search. The "[c]ompulsory provision of information (for example, requirement to produce/supply information)" amounts to a search and seizure and is covered by section 21 of NZBORA.[345] As discussed above, Section 130 of the Search and Surveillance Act and section 228 of the Customs and Excise Act 2018 require a user to only provide information and assistance that is reasonable and necessary to access a device. To date, there is very little case law regarding what is "reasonable and necessary" within the context of section 130 of the Search and Surveillance Act. There is no case law with respect to the Customs and Excise Act 2018.

Not providing access information when requested to do so under section 130 of the Search and Surveillance Act because of advice from legal counsel does not provide a defence to a charge laid under section 178.[346] Whether a claim to have forgotten the

[341] Evidence Act 2006, s 30(5)(a).
[342] Section 30(1).
[343] Section 30(2).
[344] Section 30(3).
[345] Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act: A Commentary* 949.
[346] See *R v Darroch* [2016] NZDC 11893.

access information would be successful as a defence is dependent on whether the accompanying factual matrix independently verifies such a claim.[347] For example, if the encrypted files/folders have recently been used or created, the defendant is familiar with computers, and/or the files/folders exhibit a high level of organisation then it is open to the judge to question the defendant's veracity in claiming that they have forgotten the access information.[348]

It is unlikely that section 130 of the Search and Surveillance Act would require a third party service provider to rewrite their application to allow backdoor access. The phrasing of the provision requires that any assistance or information be both "reasonable and necessary to allow the person exercising the search power to access that data".[349] Changing the nature of an application, such as a messaging app employing end-to-end encryption, might be necessary to allow a person excising a search power to access that data, but it would not be reasonable – the change is likely to make all users data accessible. Arguably, it might not be necessary either if other avenues to gain access have not been attempted. It is likely that what constitutes "reasonable and necessary" will be highly dependent on the context. Requirements to assist with access via the Customs and Excise Act 2018 is unlikely to encompass a third party, as the definition of "user" is narrower under the Act.

3.5.2 RIGHT AGAINST SELF-INCRIMINATION

3.5.2.1 Oral and documentary evidence

Generally, the state cannot require an individual to provide information which may expose them to criminal liability.[350] This is known as the right or privilege against self-incrimination, which must be claimed as it does not automatically apply.[351] This is closely related to but distinct from the right to silence.[352] The latter applies exclusively to criminal procedure whereas the privilege against self-incrimination is claimable in a variety of contexts.[353] The right against self-incrimination "presupposes that the

[347] See *Cooper v DIA* HC Wellington CRI 2008-485-86, 18 September 2008 at [11].
[348] At [11].
[349] Search and Surveillance Act 2012, s 130(1).
[350] Law Commission, *The Privilege against Self-Incrimination* (NZLC PP25, 1996), para 1.
[351] Law Commission, *The Privilege against Self-Incrimination,* para 21.
[352] See New Zealand Bill of Rights Act 1990, s 25(d).
[353] Law Commission, *The Privilege against Self-Incrimination*, paras 4-5.

prosecution in a criminal case seek to prove their case against the accused without resort to evidence obtained through methods of coercion or oppression in defiance of the will of the accused".[354] 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".[355] The underlying premise for 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".[356] Under common law, it is a rule that "no person can be forced to make an incriminating statement against his or her will".[357]

It is worth noting that "at common law the right to refuse to answer incriminatory questions embraces not just answers to *oral* interrogation, but also requests for the production of *documentation* (including pre-existing documents) and any other incriminating evidence".[358] This includes the right "to decline to produce pre-existing documentary material", which may be interpreted to include access information.[359] This is similar to the rules in other jurisdictions. 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".[360] In Canada, "the *act* of producing pre-existing documents may be inadmissible if that *act* provides an incriminating link to incriminating evidence".[361] The right against self-incrimination has been construed as pertaining to testimonial evidence. Under US law, "the privilege has been confined to essentially testimonial (oral or documentary) evidence" but does not include real evidence.[362] Similar to the rules in Europe, "the right against self-incrimination does not extend to evidence which has *an existence independent of the will of the suspect* (such as… 'documents acquired pursuant to a search warrant, breath, blood and urine samples and bodily tissue for purposes of DNA testing')".[363]

---

[354] Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act: A Commentary* 1436.
[355] Paul Rishworth and others, *The New Zealand Bill of Rights* 647.
[356] Paul Rishworth and others, *The New Zealand Bill of Rights* 647.
[357] Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act: A Commentary* 1437.
[358] Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act: A Commentary* 1437.
[359] Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act: A Commentary* 1439.
[360] Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act: A Commentary* 1440.
[361] Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act: A Commentary* 1441.
[362] Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act: A Commentary* 1442.
[363] Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act: A Commentary* 1441 (emphasis added).

3.5.2.2 Access information

However, legislation can impose obligations on an individual to provide information, while expressly retaining the privilege against self-incrimination.[364] Section 130(1) of the Search and Surveillance Act is an example of such a provision in legislation. This section imposes an obligation on an individual to provide access information if required to do so. Subsection (2), however, expressly retains the privilege against self-incrimination.

Whether access information could be subject to a claim of privilege because the access information tends to incriminate the person was first discussed in the 2008 New Zealand Court of Appeal judgment in *R v Spark*.[365] This case appears to be the only time this issue has been discussed in New Zealand case law and predates the Search and Surveillance Act. Furthermore, the discussion was obiter, as the point was not required to be determined. The Court distinguished between passwords being incriminating in themselves and passwords providing access to incriminating files.[366] The Court considered that the first type would trigger the privilege against self-incrimination whereas the second may not, as it simply provides access to content that the person acknowledges as theirs. However, the point was raised that passwords which provide access to incriminating files but are not incriminating in themselves may fall within the ambit of the definition of self-incrimination contained in section 4 of the Evidence Act 2006. This is because section 4 defines "self-incrimination" to mean "the provision of information that could reasonably lead to, or increase the likelihood of, the prosecution of that person for a criminal office". The Court states that "[i]t may be that Parliament should clarify the position."[367]

Subsections (2), (3) and (4) of section 130 of the Search and Surveillance Act represent Parliament's attempt to clarify the position. Subsection 2 states that a "specified person may not be required under subsection (1) to give any information tending to incriminate the person".[368] However, subsection (3) states that:

> Subsection (2) does not prevent a person exercising a search power from requiring a specified person to provide information or providing assistance that is reasonable and necessary to allow the person exercising the search

[364] Law Commission, *The Privilege against Self-Incrimination*, para 6.
[365] *R v Spark* [2008] NZCA 561.
[366] At [23].
[367] At [32].
[368] Search and Surveillance Act 2012, s 130(2).

> power to access data held in, or accessible from, a computer system or other data storage device that contains or may contain information tending to incriminate the specified person.[369]

Subsection (4) states that subsections (2) and (3) are subject to the subpart of Part 4 of the Search and Surveillance that relates to privilege and confidentiality. The only relevant provision is section 138,[370] which concerns the privilege against self-incrimination in the context of examination orders and production orders and states that "any assertion of a privilege against self-incrimination must be based on section 60 of the Evidence Act 2006."[371] The Law Commission considers that subsections (2), (3), and (4) of section 130 of the Search and Surveillance Act can cause confusion.[372] The Law Commission prefers an interpretation that would only allow a user to claim the privilege against self-incrimination if the access information *itself* was incriminating.[373] It should not be available if the information contained behind the access information is incriminating.[374] The Law Commission believes that the privilege against self-incrimination should only be available in situations where it is reasonable and necessary for the access information to be provided orally or in writing.[375] It should not prevent a requirement to provide that information through other means.[376] For example, from requiring the specified person to enter the access information themselves.

This interpretation has a very narrow focus that may not be currently supported when reading subsections (2), (3) and (4) of section 130 of the Search and Surveillance Act together with section 60 of the Evidence Act 2006. Subsections (2) and (4) have the consequence that any claim of privilege against self-incrimination applies must be based on section 60 of the Evidence Act 2006. The Evidence Act 2006 interprets the word self-incrimination broadly because it encapsulates information "that could reasonably lead to, or increase the likelihood of, the prosecution" of a person for a criminal offence.[377] Therefore, if the provision of access information would reveal incriminating documents or images, then the access information would tend to incriminate the person as the

---

[369] Search and Surveillance Act 2012, s 130(3).
[370] See Search and Surveillance Act 2012, s 136(1)(g).
[371] Section 138(2).
[372] Law Commission, *Review of the Search and Surveillance Act 2012*, paras 12.160-12.163.
[373] Law Commission, *Review of the Search and Surveillance Act 2012*, para 12.169.
[374] Law Commission, *Review of the Search and Surveillance Act 2012*, para 12.168.
[375] Law Commission, *Review of the Search and Surveillance Act 2012*, para 12.172.
[376] Law Commission, *Review of the Search and Surveillance Act 2012*, para 12.169.
[377] Evidence Act 2006, s 4 (definition of "self-incrimination").

information revealed would reasonable lead to and increase the likelihood of prosecution. This is evidenced in the claim by regulatory agencies that the use of encryption technologies is prematurely ending investigations.[378]

A restrictive interpretation of the applicability the right against self-incrimination in relation to computer system searches can be problematic. It would be tantamount to granting law enforcement the power to compel the forced disclosure of passwords and other information from anyone (including suspects or the accused) that are or may lead to incriminating or inculpatory evidence about them. This is precisely the kind of unjust situations that the right of self-incrimination is meant to prevent or guard against. It should be recalled that "there is no affirmative common law duty to assist an enforcement officer executing a search power".[379] Moreover, under the general rules on the form and content of search warrants, even if a warrant contains a condition that the occupier "must provide reasonable assistance to a person executing the warrant",[380] this is subject to the qualification that such "person is not required as consequence of a condition" to provide reasonable assistance "to give any information tending to incriminate the person".[381] For example, a person cannot be held liable for failing or refusing to answer the questions "Where did you bury the body?" or "Do you have prohibited goods or illicit materials?" Young, Trendle and Mahoney are of the view that:

> the definition of "self-incrimination" in s 4 of the Evidence Act 2006 refers to information "that could reasonably lead to, or increase the likelihood of,… prosecution". Arguably, *access information* or *information as to the whereabouts* would meet that definition if the fact that the person had that information established the link between him or her and the evidential material. In that event… *the person may not be required to provide the information*".[382]

There is no reason to distinguish between physical and electronic searches of tangible versus intangible evidence, and similar protections (including the right against self-incrimination) should remain.

To conclude, the requirement to assist a law enforcement officer exercising a search power by providing access information is tempered by the express applicability of the right or privilege against self-incrimination. This privilege is the strongest safeguard

---

[378] Law Commission, *Review of the Search and Surveillance Act 2012*, para 12.173.
[379] Warren Young, Neville Trendle and Richard Mahoney, *Search and Surveillance: Act and Analysis* 172.
[380] Search and Surveillance Act 2012, s 103(3)(b).
[381] Search and Surveillance Act 2012, s 103(7).
[382] Warren Young, Neville Trendle and Richard Mahoney, *Search and Surveillance: Act and Analysis* 175 (emphasis added).

available within the context of encryption technologies as it works to prevent the user from being punished for refusing to provide information that could reasonable cause or increase the likelihood of criminal prosecution. On the face of it, the privilege is capable of wide interpretation and application to the various investigatory powers and measures under the law.

3.5.2.3 Impact on sentencing

The use of encryption can also have an effect on the imposition of sentences. For suspects and persons charged, their use of encryption technologies is a consideration that judges may take into account when sentencing. The use of encryption technologies has an impact on the sentencing of a convicted person. For example, in the 2016 case of *R v Darroch*[383], where charges had been brought under the Films, Videos, and Publications Classification Act 1993, the Defendant had gone to great lengths to conceal their offending – in part, through the use of encryption technology – and this was taken into account by the Judge.[384] Similarly, in the 2017 case of *Department of Internal Affairs v Crockett*[385], also featuring charges under the Films, Videos, and Publications Classification Act 1993, the Judge took into account the fact that the Defendant had used encryption (and deletion) software to cover their tracks.[386] Consequently, it appears that a defendant's studious efforts at concealing their offending through the use of encryption technology is an aggravating factor that a court will take into account when determining sentencing.

However, the presence of encrypted files and/or folders on a defendant's computer or other data storage device cannot be inferred as evidence of the committing of a particular offence.[387] At most, what can be inferred is that some offending may be considered to be present in encrypted files and/or folders if there are similarities between non-encrypted file names and encrypted file names and the defendant refuses to provide a password.[388] It is, however, considered inappropriate to base any element of the sentencing of a convicted offender on any speculation regarding the exact nature of what

[383] *R v Darroch* [2016] NZDC 11893.
[384] At [27].
[385] *Department of Internal Affairs v Crockett* [2017] NZDC 7422.
[386] At [16].
[387] See *Cooper v Department of Internal Affairs* HC Wellington CRI 2008-485-86, 18 September 2008 and *R v Darroch*.
[388] *Cooper v Department of Internal Affairs,* at [10].

might or might not be in encrypted files and/or folders.[389] This would violate the right to be presumed innocent and other rights of persons charged and the minimum standards of criminal procedure.[390]

3.5.3 INFORMATION SECURITY AND DATA PROTECTION

Government agencies wish to protect their information from being lost or stolen for much the same reason as businesses and private individuals: prevent fraud, damage to reputation, and a whole myriad of other reasons. The protection of data necessarily relies on encryption to be effective. Consequently, encryption technologies also feature in the legislative framework and jurisprudence of New Zealand regarding information security and data protection.

While there is no general right to privacy in New Zealand, various aspects of privacy and the protection of personal data are safeguarded via several different statutes. For example, the Crimes Act 1961 makes it an offence to use interception devices and to make an intimate visual recording without consent;[391] the Harmful Digital Communications Act 2015 makes it an offence to post a digital communication, which includes any information about the victim or an intimate visual recording of another individual,[392] with the intent that it causes harm and that it does, in fact, cause harm;[393] and there are civil proceedings available for breach of confidence. In New Zealand, information security and data protection are also governed by the Privacy Act 1993.

The Privacy Act is concerned with the promotion and protection of personal information. Personal information is defined broadly to mean information about an identifiable individual.[394] The Privacy Act establishes Information Privacy Principles (IPP) relating to the collection, use and disclosure of personal information held by agencies (i.e., data controllers and data processors), and the access of individuals to ascertain, and correct, the information about them held by an agency.[395] The Privacy Act applies to

[389] *R v Darroch*, at [41].
[390] New Zealand Bill of Rights Act 1990, ss 24-25.
[391] Crimes Act 1961, s 216B and S216H respectively.
[392] Harmful Digital Communication Act 2015, s 4 (definition of "posts a digital communication")>
[393] Section 22(1).
[394] Privacy Act 1993, s 2(1).
[395] Section 6.

agencies, which is defined inclusively – the exceptions are specifically listed.[396] Therefore, the Privacy Act has very wide applicability.

The most pertinent IPP relating to encryption is IPP 5, regarding the storage and security of personal information. Essentially, it requires an agency to ensure that the information they hold is protected and secured by such security safeguards as it is reasonable in the circumstances to take. Assessing what is reasonable in the circumstance depends on the sensitivity/confidentiality of the information involved and what safeguards could have been put in place to protect that information.[397] The Privacy Commissioner also considers the agency's policies and practises, including any staff training, when making the assessment. Additionally, an agency has an ongoing responsibility to develop and maintain appropriate security safeguards for their information.[398] Maintaining a good privacy culture requires system audits, staff training, policies and technology upgrades. This open-textured and flexible application of IPPs – determining reasonableness in the actual circumstances giving rise to a complaint – is considered a strength of the Privacy Act.[399]

Specific guidance regarding minimum standards of reasonableness is not available. The Privacy Commissioner does appear to require that data stored in a cloud must be encrypted to be sent there,[400] and that data physically transmitted between New Zealand government departments must be encrypted when being transferred.[401] However, the Privacy 101 workbooks published by the Commissioner as part of their online learning tools only mentions encryption as something that an agency may consider when transmitting information.[402] The New Zealand Government published guidelines on the IPPs, which suggest that an agency should ask itself if the information is protected by reasonable safeguards.[403] The New Zealand Government also provides advice that an agency should check to see what security requirements apply as some agencies (public

---

396 Privacy Act 1993, s 2(1)
397 See *Case Note 26781* [2003] NZ PrivCmr 21.
398 *Case Note 269784* [2016] NZ PrivCmr 3.
399 See Law Commission, *Review of the Privacy Act 1993. Review of the Law of Privacy Stage 4* (NZLC IP17 2010) at 28.
400 Privacy Commissioner, "What do you have to do to keep information secure?" <privacy.org.nz>
401 Privacy Commissioner, "Privacy Commissioner requires data encryption" (21 February 2008) <privacy.org.nz>.
402 See Privacy Commissioner, "Privacy 101: An Introduction to the Privacy Act. Facilitation Guide" (December 2015) <privacy.org.nz> at 61, and Privacy Commissioner, "Privacy 101: An Introduction to the Privacy act. Participant Guide" (December 2015) <privacy.org.nz> at 48.
403 New Zealand Government, "Information privacy principles. Descriptions and examples of breaches of the IPPs" at 19.

service departments and selected others) fall within the scope of the Protective Security Requirements.[404] The New Zealand Government itself is required to adhere to the New Zealand Information Security Manual,[405] which contains a detailed chapter on cryptography and how it is to be implemented in the New Zealand context.[406] Cryptography is an important consideration for information security and data protection.[407]

An agency's data protection practises only really come under Privacy Commissioner review following a complaint. Complaints to the Privacy Commissioner have usually regarded denied access to an individual's information by an agency or a data breach. Most data breach complaints concern unauthorised disclosure rather than a pure loss of personal information. Indeed, the only time that the lack of encryption appears to have been considered by the Privacy Commissioner is during an investigation which took place in 2013.[408] In this case, a doctor working in a suburban medical practise had his car broken into and a bag stolen, which contained a USB stick holding personal information on a number of patient that was not encrypted. The Privacy Commissioner investigated and held that although the information had been taken offsite without being encrypted first, the response of the medical practise in updating their security policies was adequate to avoid being found liable for breaching a person's privacy. These updates included purchasing encrypted USB sticks and creating an active register of staff who were issued with these encrypted USB sticks. Consequently, the opportunity to discern whether the Privacy Commissioner considers encryption as a minimum standard when it comes to the storage and security of retained personal information is unsettled, as is the opportunity to discern any development over time regarding the appropriateness of encryption since the Privacy Act came into force.

The Privacy Commissioner is authorised by the Privacy Act to issue codes of practise that become part of the law.[409] These codes modify the operation of the Privacy

---

[404] New Zealand Government, "Information privacy principles. Descriptions and examples of breaches of the IPPs" at 20.
[405] "What You Need To Know" <protectivesecurity.govt.nz>.
[406] Government Communication Security Bureau, "17. Cryptography" in *NZISM New Zealand Information Security Manual – Part 2* (Government Communication Security Bureau, online source, December 2017) at 431.
[407] See "Information Security Management Protocol" <https://www.protectivesecurity.govt.nz/home/information-security-management-protocol/information-security-management-protocol/#operational-security-management> at [6.5].
[408] See *Case Note 248601* [2013] NZ PrivCmr 4.
[409] Privacy Commissioner, "Codes of Practise" <https://www.privacy.org.nz/the-privacy-act-and-codes/codes-of-practice/>. See, for guidance, Privacy Commissioner "Guidance Note on Codes of Practice under Part VI of

Act for specific industries and three such codes that cover IPP 5 are: (1) Telecommunications Information Privacy Code; (2) Credit Reporting Privacy Code; and (3) Health Information Privacy Code.[410] These codes do not alter IPP 5 in any significant way. However, the first two concern industries where the use of encryption has long been a default. In 2017, the Ministry of Health published the Health Information Governance Guidelines, which provided information on policies and procedures that must be implemented for a health provider to meet its legal obligation regarding health information.[411] These guidelines require a health provider to comply with the Health Information Security Framework,[412] which contains detailed reference to cryptography.[413] Most significantly, this framework requires that a health provider establish and document a cryptographic policy, adapting then adopting the Protective Security Requirements and the New Zealand Information Security Manual as a security baseline.[414] Furthermore, when building a risk profile, a health provider must consider upgradeable solutions so that encryption protocols and algorithms can be upgradable over the systems lifetime and, when decommissioning, ensuring encryption keys used cannot be compromised.[415]

It is evident from the above discussion that the security and protection of information systems and personal data are important concerns for both the public and private sectors. The use of encryption underpins information security and data protection. Therefore, information security and data protection issues and concerns should be seriously and carefully considered when exercising any investigatory powers and measures. For instance, it may not be reasonable to compel a provider not to use encryption or to weaken the security or privacy protections of its products and services to enable or assist in the conduct of a search, surveillance or other investigatory measure. Ensuring information security and protecting personal data are legitimate reasons for using encryption and these can serve as reasonable excuses for a provider to lawfully

---

the Privacy Act <https://www.privacy.org.nz/news-and-publications/guidance-resources/guidance-note-on-codes-of-practice-under-part-vi-of-the-privacy-act/>.

[410] Out of the three remaining codes, two amend IPP12 (unique identifiers) and the other one concerns authorised disclosure of information during a civil defence national emergency. See Privacy Commissioner "Codes of Practise" <https://www.privacy.org.nz/the-privacy-act-and-codes/codes-of-practice/>.

[411] Ministry of Health, "HISO 10064:2017 Health Information Governance Guidelines" (Ministry of Health, online, August 2017) at [1].

[412] At [5.2.1].

[413] Ministry of Health, "HISO 10029:2015 Health Information Security Framework: (Ministry of Health, online, December 2015), chp15.

[414] At [15.3.3].

[415] At appendix C.

refrain from rendering assistance as part of an investigation. Information security and data protection are critical principles and values that need to be protected for persons living in a networked information society.

3.6 Tacit and implicit rules on encryption

One of the perennial questions discussed in the encryption debate is whether encryption can or should be regulated. This part of the study has shown that this question is more or less moot since encryption is already subject to existing laws and regulations. It is not a question of whether but how encryption is controlled and regulated. Both in New Zealand and internationally, the export of encryption technologies is regulated by export control rules, while the development and implementation of encryption is subject to the restriction on misuse of devices under computer crime laws. Criminal procedures rules, especially those concerning search and surveillance, have the most significant impact on encryption. As discussed above, law enforcement officers in New Zealand and abroad already have significant powers and measures to deal with encrypted data, communications and devices as part of a criminal investigation. Using search and seizure powers, they can conduct searches and gain access to encrypted data and protected computers. Subject to certain human rights and legal protections, law enforcement officers can require reasonable assistance from third parties or force the disclosure of access information such as passwords and encryption keys from persons subject to or involved in a search. Given that encryption keys are the lynchpin of the security and integrity of encryption, such power to demand access information especially from suspects is quite substantial. Under the relevant surveillance rules, law enforcement can also intercept and collect encrypted communications. Under the TICSA, network operators are required to make their networks interception capable and decrypt communications if they have control over the encryption process. On their part, telecommunications service providers have the duty to provide reasonable assistance to law enforcement in carrying out surveillance operations. Both network operators and service providers can also be required to provide content data and traffic data as part of an investigation. In addition to search and surveillance powers, law enforcement can also resort to other investigatory measures such as production orders, examination orders and declaratory orders. In relation to production orders, providers can also be ordered to provide subscriber

information and even access information. But the law enforcement powers and measures that apply to encryption are not absolute and they are checked and counterbalanced by human rights principles and other legal safeguards and protections. The most important of these are the right against unreasonable search and seizure and the right against self-incrimination. A search, surveillance or other investigatory measure must be lawful and reasonable and respect the human rights of persons.

The law enforcement, human rights and other laws discussed in this part represent the tacit and implicit legal framework that controls and regulates access to and use of encryption. It is important to make these rules explicit in order to gain a better understanding of what rules actually apply to encryption and how they operate and interact with each other. It would not be possible to fully comprehend what encryption involves and entails without examining its legal and regulatory context. Laws though are not solely about legal rights and obligations. Legal rules also have a social dimension since they embody and seek to uphold important social goals and values. With regard to encryption, these values mainly relate to the general objectives or aspirations of effective law enforcement and public order as well as human rights and freedoms. The underlying principles and values of encryption are the focus of the next part of this study.

Principles and values of encryption

4.1 Fundamental principles and values

It is apparent from the preceding parts of this report that encryption involves or is concerned with a number of distinct legal, social and technical principles and values. Based on a doctrinal legal research of relevant laws and jurisprudence, secondary research of computer science and social science literature, and observations from and analysis of the collected empirical data, 10 fundamental principles and values involving or associated with encryption are clearly discernible, namely:

- Data protection
- Information security
- Law enforcement and lawful access
- National security and public safety
- Privacy
- Right against self-incrimination (including right to silence and other rights of persons charged)
- Right against unreasonable search and seizure
- Right to property
- Secrecy of correspondence
- Trust

These values are considered fundamental because they are the core concerns relating to the development, access to and use of encryption.

The above list of principles and values is borne out by existing research and literature. For instance, the OECD's Guidelines for Cryptography Policy specifically mention information security, national security, public safety, and law enforcement as

crucial policy objectives of encryption regulation.[1] The Guidelines also enumerate trust, right to property (which is connected to "market driven development" and the right to conduct a business), privacy, data protection, secrecy of correspondence ("confidentiality of data and communications"), and lawful access as among the key principles of any cryptography policy.[2] In his seminal book on cryptography law and policy, Koops similarly refers to national security, public safety, privacy, and information security as "fundamental societal concerns".[3] He also considers the right to privacy, secrecy of correspondence ("confidential communications"), right to a fair trial (including the right against self-incrimination), and law enforcement (as part of "the general rule of law") as the fundamental principles relevant to encryption.[4]

It should be noted that the discussions in the two preceding parts of this report revolve around these very same 10 principles and values. As explained in Part 2 on the technologies of encryption, information security is the primary goal of encryption. Furthermore, this technology helps protect and maintain privacy, data protection, secrecy of correspondence, and trust. With regard to encryption-related laws in Part 3, the values and objectives of law enforcement and lawful access and national security and public safety as embodied in criminal procedure and search and surveillance laws naturally go hand-in-hand with human rights values such as right against unreasonable search and seizure, privacy, secrecy of correspondence, and right against self-incrimination (including right to silence and other rights of persons charged). Information security and data protection are considered additional protections and safeguards provided to users and developers of encryption.

4.1.1 MEANINGS

The 10 fundamental principles and values concerning encryption are admittedly theoretically and empirically complex and multifaceted. Each of these terms is subject to much debate and contestation among public and private actors (including policymakers and scholars). The absence of common or universally accepted definitions is not fatal to this or any other research. In fact, most (if not all) research actually stems from and thrives

[1] See OECD, "Cryptography Policy" 8, 9, 11, 13, 16 and 21,
[2] See OECD, "Cryptography Policy" 9, 13, 14, 15, 25, 26, 27 and 28.
[3] Bert-Jaap Koops, *The Crypto Controversy* 117 and 123.
[4] Bert-Jaap Koops, *The Crypto Controversy* 119, 120, 121 and 123.

under this initial theoretical or definitional ambiguity. The key is to be conceptually explicit and clear about what these terms mean within the context of the present research. Thus, in light of the principal aims, scope and subject matter of this study, the principles and values of encryption should be conceived of in the following manner.

Conceptually, *data protection* is primarily concerned with the protection of natural persons with respect to the processing of their personal data.[5] This may involve guarding against "the improper collection, use, security, storage, release or destruction of data about individuals".[6] It also includes safeguarding people from a personal data breach, which is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".[7] Personal data refers to "any information relating to an identified or identifiable natural person"[8] and the processing of personal data covers

> any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.[9]

It is worth pointing out that, despite its name, the Privacy Act 1993 is a data protection legislation and not strictly speaking a privacy law.[10]

On its part, *information security* is about protecting "the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data".[11] This corresponds to the "three basic objectives of information security": confidentiality, integrity and availability (the so-called CIA triad).[12] The meanings of confidentiality and integrity have already been discussed in Part 2. Availability requires that "information and communications systems are [accessible or]

---

[5] See EU General Data Protection Regulation, arts 1(1), 5 and 6; see also Privacy Act 1993, title and s 6.
[6] Stephen Penk, "The Privacy Act 1993" 55; see also Legislation Design Advisory Committee, "Legislation Guidelines" 39.
[7] EU General Data Protection Regulation, art 4(12).
[8] EU General Data Protection Regulation, art 4(1); see also Privacy Act 1993, s 2(1).
[9] EU General Data Protection Regulation, art 4(2); see also Privacy Act 1993, title.
[10] See Stephen Penk, "Thinking About Privacy" 7 and 54 (at most it may called an information privacy law, but it does not establish nor provide for a right to privacy).
[11] Convention on Cybercrime, Preamble.
[12] Bert-Jaap Koops, *The Crypto Controversy* 24 (compare with the objectives of encryption, which are confidentiality, integrity and *authenticity* of information and communications).

available to their users at the right time".[13] Information security has also been described as "protecting information and information systems from unauthorised access, use, disclosure, disruption, modification, or destructions".[14] In relation to information security, encryption is specifically concerned with the confidentiality, integrity and authenticity of data.

While *law enforcement* is often mentioned in laws, policy papers and scholarly works, it has no express definition under the law.[15] In the absence of a specific legal or technical definition, resort to the natural and ordinary meaning of words may be appropriate pursuant to the plain meaning rule of statutory interpretation. A dictionary definition of law enforcement is "the action or activity of compelling observance of or compliance with the law".[16] As a practical matter, it is primarily concerned with the detection, investigation and prosecution of crimes and other offences.[17] According to Koops, law enforcement helps uphold "the right to freedom from crime" which "is part and parcel of the general rule of law".[18] Law enforcement is considered necessary to preserve the rule of law because for the latter to exist the following requisite conditions must be met: "first… a society should try to prevent crimes, and, second… committed crimes should be redressed, usually by prosecuting their perpetrators".[19] *Lawful access* pertains to a particular aspect of law enforcement whereby public telecommunications providers are obligated to ensure that law enforcement agencies have the technical capability to intercept communications and collect data on their services and networks.[20] The Telecommunications (Interception Capability and Security) Act 2013 is an example of lawful access legislation.[21]

National security and public safety is another example of principles and values that are always raised and spoken of but are not explicitly defined in the law. As with other jurisdictions, in New Zealand, the lack of a formal definition of national security is a

[13] Bert-Jaap Koops, *The Crypto Controversy* 24.
[14] Jason Andress, *The Basics of Information Security* 2; see also, Department of the Prime Minister and Cabinet, "New Zealand's Cyber Security Strategy 2015".
[15] See, for example, Policing Act 2008.
[16] Oxford Dictionary of English.
[17] See Convention on Cybercrime, Preamble.
[18] Bert-Jaap Koops, *The Crypto Controversy* 120.
[19] Bert-Jaap Koops, *The Crypto Controversy* 121.
[20] See Canadian Department of Justice, "Summary of Submissions to the Lawful Access Consultation"; see also Telecommunications (Interception Capability and Security) Act 2013, s 9.
[21] See Telecommunications (Interception Capability and Security) Act 2013, ss 5-6.

conscious policy decision.[22] In relation to the Intelligence and Security Act 2017, the Department of the Prime Minister and Cabinet explains that "[b]ecause of the difficulties of defining 'national security', Parliament changed the Bill. The Act now avoids defining the term 'national security' in legislation, and instead lists clearly the types of activities and threats that are covered".[23] This is understandable given that, aside from its theoretical and empirical complexity, national security is a negative value (i.e., absence or freedom from attacks or aggression) whose effectiveness or success is difficult to validate or measure.[24] Absent any express statutory definition, national security can be construed as "the safety of a nation against threats such as terrorism, war, or espionage"[25] and public safety can be understood as simply meaning what it says following the plain meaning rule and the literal approach to statutory interpretation. Resorting to rules of statutory interpretation seems serviceable albeit not satisfying from a conceptual or analytical perspective. While it is true that national security and public safety are inherently broad and ambiguous terms that can mean many things to different people,[26] they are always open to further clarification by providing greater specificity about the means and ends sought – that is, answering the questions: national security and public safety *for whom* and *from what threats*?[27] Examining the purposes and powers granted under the Intelligence and Security Act 2017 and how the Act addresses "matters of national security", it could be reasonably argued that, national security and public safety in the New Zealand context is about protecting the state and the general public from external and internal threats such as terrorism, violent extremism, espionage, sabotage, weapons of mass destruction, and serious transnational crimes, as well as threats that impact government operations and critical information and communications infrastructure, national sovereignty, and international security.[28]

Privacy, like national security, is another complex concept that defies precise or easy definition.[29] While formulating a definitive or a universal definition of privacy seems

[22] See Department of the Prime Minister and Cabinet, "Defining National Security".
[23] Department of the Prime Minister and Cabinet, "Defining National Security".
[24] Arnold Wolfers, "'National Security' as an Ambiguous Symbol" 488 and 496.
[25] Oxford Dictionary of English.
[26] Arnold Wolfers, "'National Security' as an Ambiguous Symbol" 481 and 483.
[27] David Baldwin, "The concept of security" 12, 13 and 15; see also Arnold Wolfers, "'National Security' as an Ambiguous Symbol" 484 and 500.
[28] See Intelligence and Security Act 2017, ss 3 and 59; see Department of the Prime Minister and Cabinet, "Defining National Security"; see also Arnold Wolfers, "'National Security' as an Ambiguous Symbol" 481, 485 and 489.
[29] See Stephen Penk, "Thinking About Privacy" 1.

like an impossible task, describing and defining the extent, elements and characteristics of privacy has proven less problematic. For example, despite there being no explicit right to privacy in New Zealand,[30] there is no question that privacy is a fundamental value.[31] It is also much broader than but includes the value of data protection.[32] Privacy is intimately related to the human rights goals of individual autonomy, dignity and equality.[33] Even though privacy has been described as simply "the right to be let alone",[34] it is not merely a negative freedom since it also involves the positive freedom of "self-development".[35] Privacy has been characterised as being composed of distinct yet interdependent elements such as solitude, intimacy, secrecy (or confidentiality) and anonymity (or inconspicuousness).[36] According to Koops and others, there are possibly nine "ideal types of privacy", namely: bodily privacy, intellectual privacy, spatial privacy, decisional privacy, communicational privacy, associational privacy, proprietary privacy, behavioural privacy, and informational privacy.[37] The existence of many types as well as different possible conceptions of privacy seems to militate against the likelihood of ever formulating a single definition for this value.[38] Regardless of this, privacy is without question a significant principle and value in relation to encryption.[39]

Right against self-incrimination (including right to silence and other rights of persons charged) are important human rights that are also referred to as criminal procedure rights (or rights of the accused).[40] They have legal foundations and bases in statutory law, common law, and international law.[41] The right against self-incrimination involves "[t]he right of a person

---

[30] Stephen Penk, "Thinking About Privacy" 20.
[31] See Stephen Penk, "Thinking About Privacy" 5 and 15.
[32] See Stephen Penk, "Thinking About Privacy" 7 and 54 (even though privacy subsumes data protection, the latter remains a distinct principle and value that deserves to be examined separately).
[33] Stephen Penk, "Thinking About Privacy" 16.
[34] Samuel Warren and Louis Brandeis, "The Right to Privacy" 193 and 205; see also Stephen Penk, "Thinking About Privacy" 3; Bert-Jaap Koops, *The Crypto Controversy* 120.
[35] Bert-Jaap Koops and others, "A Typology of Privacy" 565 and 566.
[36] 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.
[37] Bert-Jaap Koops and others, "A Typology of Privacy" 566.
[38] See Bert-Jaap Koops and others, "A Typology of Privacy" 566; see Daniel Solove, "Conceptualizing Privacy" 1099-1124; see also Stephen Penk, "Thinking About Privacy" 8.
[39] See Stephen Penk, "Thinking About Privacy" 23.
[40] See Legislation Design Advisory Committee, "Legislation Guidelines" 32.
[41] Evidence Act 2006, s 60; New Zealand Bill of Rights Act, ss 23(4), 25(d), 25(a) and 27(1); Search and Surveillance Act 2012, ss 103(7), 130(2), 136(g) and 138; Law Commission, *The Privilege Against Self-Incrimination* 12-14 and 44 (on the common law privilege); International Covenant on Civil and Political Rights, art 14(3)(g); European Convention on Human Rights, art 6; Law Commission, *The Privilege Against Self-Incrimination* 12-14 and 44; see 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; see also Legislation Design Advisory Committee, "Legislation Guidelines" 101.

not to be compelled by the threat of punishment to answer questions which might incriminate himself/herself".[42] As explained by the Law Commission, the rationale for this right is that people "cannot be required by the State to provide information which may expose [them] to criminal liability".[43] 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.[44] According to Butler and Butler, citing the case of *R v Director of Serious Fraud Office, ex parte Smith*, these two rights, together with other human rights, comprise a bundle of "silence immunities":[45]

- *right or privilege against self-incrimination* under common law and s 60 of the Evidence Act 2006;
- *right to silence* under s 23(4) of the New Zealand Bill of Rights Act 1990;
- *right not to be compelled to be a witness or to confess guilt* under s 25(d) of the New Zealand Bill of Rights Act 1990;
- *right to a fair trial* and *right to be presumed innocent until proved guilty according to law* under ss 25(a) and 25(c) of the New Zealand Bill of Rights Act 1990
- *right to justice* under s 27(1) of the New Zealand Bill of Rights Act 1990; and
- *freedom of expression* under s 14 of the New Zealand Bill of Rights Act 1990 (which includes the right not to speak).[46]

In general, the above rights or immunities 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".[47] The Law Commission itself enumerates the reasons why the right against self-incrimination is a necessary part of

[42] Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act* 1430.
[43] Law Commission, *The Privilege Against Self-Incrimination* 1; see also Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act* 1430 and 1431.
[44] 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.
[45] See Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act* 1431; see *R v Director of Serious Fraud Office, ex parte Smith* [1993] AC 1 (HL); see also Paul Rishworth and others, *The New Zealand Bill of Rights* 649.
[46] See Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act* 1431, 1432, 1437, 1438, 1439 and 1454; see *R v Director of Serious Fraud Office, ex parte Smith* [1993] AC 1 (HL); see Law Commission, *The Privilege Against Self-Incrimination* 44; see Paul Rishworth and others, *The New Zealand Bill of Rights* 647-650; see Legislation Design Advisory Committee, "Legislation Guidelines" 24 and 25 (on the constitutional right to procedural fairness and natural justice).
[47] Paul Rishworth and others, *The New Zealand Bill of Rights* 646.

a free and democratic society.[48] For one, it is considered a necessary component of an accusatorial criminal justice system where a person charged is provided with certain protections to defend himself or herself.[49] As a matter of justice and fairness,

> the privilege equalises the parties' respective positions in investigations and proceedings involving the State. This is achieved by requiring the State to obtain its evidence independently of a person's compelled assistance, and by giving the witness some defences against the strength of the State.[50]

In addition, the right can prevent "inhumane treatment and abuses in criminal investigations" as well as "unwarranted intrusions from the State".[51] Further, it provides a safeguard against "unreliable admissions" especially in the context of criminal investigations and prosecutions "where the potential for pressure and suggestibility is greatest".[52] This conforms to the principle that "[n]atural justice operates at its highest level in the case of criminal trials, with strict procedural requirements".[53] Finally, the right against incrimination "protects some innocent defendants from conviction".[54] These policy reasons and justifications underpinning the right against self-incrimination remain robust and relevant especially in the context of rapid technological developments in an increasingly digital and connected world.

The *right against unreasonable search and seizure* is critical for balancing human rights with law enforcement values.[55] It is considered a "'broad and general right' which protects an amalgam of values including property, personal freedom, privacy and dignity".[56] It preserves others values such as "liberty, dignity, bodily integrity, privacy, and the right to peaceful enjoyment by people of their property".[57] The right against unreasonable search and seizure generally protects individual persons from "unwarranted state intrusions…. [or] interferences with [their] person, property, correspondence,

---

[48] Law Commission, *The Privilege Against Self-Incrimination* 20; see also Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act* 1434-1435; see also Paul Rishworth and others, *The New Zealand Bill of Rights* 659.
[49] Law Commission, *The Privilege Against Self-Incrimination* 29.
[50] Law Commission, *The Privilege Against Self-Incrimination* 30; see also Paul Rishworth and others, *The New Zealand Bill of Rights* 646.
[51] Law Commission, *The Privilege Against Self-Incrimination* 30.
[52] Law Commission, *The Privilege Against Self-Incrimination* 30; see also Paul Rishworth and others, *The New Zealand Bill of Rights* 647.
[53] Legislation Design Advisory Committee, "Legislation Guidelines" 25.
[54] Law Commission, *The Privilege Against Self-Incrimination* 30.
[55] New Zealand Bill of Rights Act 1993, s 21.
[56] Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act* 916 and 940 (citing *R v Jeffries*).
[57] Legislation Design Advisory Committee, "Legislation Guidelines" 100.

personal information or electronic communications".[58] The kind of state interference contemplated here normally concerns law enforcement and other activities involving penal liability.[59] It 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".[60] 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".[61] The right "should extend not only to the interception of mail… but also the electronic interception of private conversations, and other forms of surveillance".[62] While the right against unreasonable search and seizure has been traditionally construed as providing protections to property, the modern and current approach in New Zealand and around the world is to construe it as protecting a person's reasonable expectation of privacy.[63] The substantive test for determining whether a person has a reasonable expectation of privacy is: "(a) the person subjectively had an expectation of privacy at the time of the activity; and (b) that expectation was one that society is prepared to recognise as reasonable".[64] It is worth noting that, unlike other jurisdictions, the right against unreasonable search and search does not give rise to a separate or distinct right to privacy in New Zealand.[65]

Although it is not explicitly provided for in the New Zealand Bill of Rights Act 1990, *right to property* is a considered a fundamental principle and value under New Zealand law.[66] The Legislation Design Advisory Committee (LDAC) expressly provides in its Guidelines that "[n]ew legislation should respect property rights".[67] As explained by the LDAC, "[p]eople are entitled to the peaceful enjoyment of their property (which

---

[58] 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.
[59] Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act* 925, 932 and 935; see also Paul Rishworth and others, *The New Zealand Bill of Rights* 418.
[60] Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act* 932 and 935.
[61] Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act* 904 citing White Paper.
[62] Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act* 904 citing White Paper.
[63] 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 Legislation Design Advisory Committee, "Legislation Guidelines" 100.
[64] Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act* 974 and 941; see also Paul Rishworth and others, *The New Zealand Bill of Rights* 420; see also Stephen Penk, "Thinking About Privacy" 20.
[65] Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act* 904, 919 and 920 (privacy is a value not a right).
[66] Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act* 61 (property rights traditionally protected under common law); See Legislation Design Advisory Committee, "Legislation Guidelines" 21 and 24.
[67] See Legislation Design Advisory Committee, "Legislation Guidelines" 24.

includes *intellectual property* and *other intangible property*)".[68] Part of the right to property is the ability to develop and use one's property without interference, including the right to innovate, produce, use and distribute technologies such as encryption. It could be argued that property or ownership rights are implicitly protected by the right to justice, which requires compliance with principles of natural justice (i.e., substantive and procedural due process) when "any tribunal or other public authority" makes "a determination in respect of that person's rights, obligations, or interests protected or recognised by law".[69] Of course, like other rights, property rights are never absolute and are subject to reasonable control as provided for by law.[70]

With regard to *secrecy of correspondence* or communications, while it is covered under the right against unreasonable search and seizure, it remains a distinct value that is expressly mentioned in the law and is worth analysing separately because of the unique elements and issues it raises especially in the context of digital communications and electronic surveillance.[71] It is integral for preserving privacy, confidentiality, anonymity, aspects of freedom of association, anonymous speech, and freedom of expression.[72]

It is worth noting though that freedom of expression is not included among the fundamental principles and values of encryption in this study. Freedom of expression is undoubtedly important in a networked society and encryption can enable the exercise of this right.[73] In the United States, encryption and freedom of speech is considered an important issue.[74] However, in the New Zealand context, it is not yet a major area of concern. Freedom of expression was not specifically raised or alluded to in the focus group interviews and it was not flagged as a critical matter in the analysis of the legal and technical dimensions of encryption. In any event, with regard to the freedom not to speak, this is already covered by the right against self-incrimination and right to silence.

Trust is not commonly mentioned in most non-technical literature on encryption. But, as explained in greater detail below, trust plays an important moderating and

---

[68] See Legislation Design Advisory Committee, "Legislation Guidelines" 24 (emphasis added).
[69] New Zealand Bill of Rights Act 1993, s 27(1); see US Constitution, Fourteenth Amendment.
[70] New Zealand Bill of Rights Act 1993, s 5; Legislation Design Advisory Committee, "Legislation Guidelines" 24.
[71] See Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act* 944 and 949.
[72] See Human Rights Council, "Report of the Special Rapporteur on the promotion and protection of the right of freedom of opinion and expression".
[73] Human Rights Council, "Report of the Special Rapporteur on the promotion and protection of the right of freedom of opinion and expression" 1.
[74] See Robert Post, "Encryption Source Code and the First Amendment"; see Lee Tien, "Publishing Software as a Speech Act".

balancing role for the other principles and values cited above. The ordinary meaning of trust is a "firm belief in the reliability, truth, or ability of someone or something".[75] From a sociological perspective, it has "distinct cognitive, emotional, and behavioral dimensions".[76] Cognitively speaking, "trust is based on a cognitive process which discriminates among persons and institutions that are trustworthy, distrusted, and unknown".[77] In terms of its emotional base, "trust consists in an emotional bond among all those who participate in the relationship".[78] With regard to behaviour, "to trust is to act as if the uncertain future actions of others were indeed certain in circumstances wherein the violation of these expectations results in negative consequences for those involved".[79] There are many types of trust but the ones most relevant to encryption are personal or interpersonal trust and institutional trust (i.e., trust in the technology itself, trust in the developers and providers of encryption technologies, and trust in government).[80] The opposite of trust – distrust – also plays a crucial role. Like trust, distrust equally "reduces complexity by dictating a course of action based on suspicion, monitoring, and activation of institutional safeguards".[81] For example, with respect to trust in government, a healthy distrust "in any set of political incumbents is functional for the continuance of democratic institutions".[82] Trust is distinct from but also involves critical elements or notions such as reliability, credibility, sincerity, competence and confidence.[83] There are different levels of trust varying from weak to strong and even neutral.[84]

4.1.2 CATEGORIES

Quite interestingly, the 10 fundamental principles and values of encryption have already been categorised in the New Zealand context. In relation to search and surveillance powers, which are extremely pertinent to encryption as shown in Part 3, the Law Commission groups the principal values connected with these powers into two

[75] Oxford Dictionary of English, "Trust".
[76] J. David Lewis and Andrew Weigert, "Trust as a Social Reality" 969.
[77] J. David Lewis and Andrew Weigert, "Trust as a Social Reality" 970.
[78] J. David Lewis and Andrew Weigert, "Trust as a Social Reality" 971.
[79] J. David Lewis and Andrew Weigert, "Trust as a Social Reality" 971.
[80] See J. David Lewis and Andrew Weigert, "Trust as a Social Reality" 973-974; see also Kirsimarja Blomqvist, "The Many Faces of Trust" 281.
[81] J. David Lewis and Andrew Weigert, "Trust as a Social Reality" 969.
[82] J. David Lewis and Andrew Weigert, "Trust as a Social Reality" 969.
[83] Kirsimarja Blomqvist, "The Many Faces of Trust" 277-279 and 282.
[84] Kirsimarja Blomqvist, "The Many Faces of Trust" 282.

general categories: "human rights values" and "law enforcement values".[85] Human rights values include privacy, secrecy of correspondence, right against self-incrimination (in relation to "personal integrity"), right to property ("protection of property rights"), and "[maintenance of the] rule of law" (particularly in relation to the right against unreasonable search and seizure).[86] On the other hand, law enforcement values are meant to uphold the policy goals and objectives of "national security, public safety or the economic well-being of the country, [and] the prevention of disorder or crime".[87] Based on the explanation of the Law Commission, the overriding value of "appropriate and effective law enforcement" is further composed of various elements such as effectiveness, simplicity, certainty, responsiveness, and consistency with human rights (especially relating to the reasonable expectation of privacy).[88]

This categorisation of principles and values into human rights values vis-à-vis law enforcement values is reasonable and analytically useful. For the purposes of this research though, it would be helpful to rename the categories to "human rights and freedoms" and "law enforcement and public order" since these labels are more precise and apt for examining the subject of encryption. In this way, the category of human rights and freedoms covers the principles and values of: data protection; privacy; right against self-incrimination (including right to silence and other rights of persons charged); right against unreasonable search and seizure; right to property; and secrecy of correspondence. Whereas, law enforcement and lawful access and national security and public safety fall within the category of law enforcement and public order. On its part, information security is an overarching concern of encryption. Whether as a goal or as a means, it is pertinent to both human rights and freedoms and law enforcement and public order. With regard to trust, it is notable that it underpins, connects and mediates the other principle and values. Therefore, like information security, it sits across both categories.

The table below illustrates the basic categorisation of the principles and values of encryption. It is important to note though that, empirically speaking, the principles and values of encryption are much more complex and messy than this table represents. Nevertheless, this table is useful as an analytical tool to normatively and logically

---

[85] Law Commission, *Search and Surveillance Powers* 37.
[86] Law Commission, *Search and Surveillance Powers* 38, 39, 40, 41.
[87] Law Commission, *Search and Surveillance Powers* 42.
[88] Law Commission, *Search and Surveillance Powers* 42-43; see also Law Commission, *Review of Search Surveillance Act 2012* 49; see also Bert-Jaap Koops, *The Crypto Controversy* 121.

categorise such discrete concepts. The intricate relations and interconnections between and among the principles and values are further elaborated in Section 4.3.

Categories of encryption principles and values

Human rights and freedoms	Law enforcement and public order
Data protection	Law enforcement and lawful access
Privacy	National security and public safety
Right against self-incrimination	
Right against unreasonable search and seizure	
Right to property	
Secrecy of correspondence	
Information security	
Trust	

4.2 Hierarchy of principles and values

4.2.1 RANKING ACROSS AND AMONG STAKEHOLDERS

Aside from the above categorisation, the principles and values related to encryption conform to a certain hierarchy. Based on the coding and qualitative data analysis of the focus group interviews, particularly the group ranking exercise that participants undertook, there is a discernible hierarchy or prioritisation of principles and values for the three groups of stakeholders (i.e., general public, business and government). The principles and values are ranked according to what the focus group participants consider to be the most important and the least significant to encryption (see table below). The classification of principles and values into top tier and second tier is based on the qualitative data analysis of the focus group interviews. Specifically, it is founded on how the focus group participants ranked the principles and values as well as the prominence or importance they placed on each principle and value in the overall discussions during the focus group interviews.

For all categories of stakeholders, privacy is deemed the topmost principle and value concerning encryption. Together with privacy, data protection, information

security, trust, national security and public safety, and right to property make up the top tier. The second tier is comprised of secrecy of correspondence, law enforcement and lawful access, right against unreasonable search and seizure, and right against self-incrimination (including right to silence and other rights of persons charged).

Ranking of encryption principles and values across stakeholders combined

The grouping of the principles and values into top and second tiers generally holds true across the three groups of stakeholders albeit with some variations (see table below). For instance, members of the general public consider secrecy of correspondence a top-tier value and national security and public safely a second-tier one. For businesses, information security is accorded the highest value while secrecy of correspondence is similarly placed in the top tier. Representatives from businesses also place greater importance on national security and public safety and right to property compared to the overall ranking. With regard to government, national security and public safety is second only to privacy as the topmost value. In contrast to the other stakeholders, focus group

participants from government assign right against unreasonable search and seizure to the top tier, but relegate information security to the second tier. Curiously, government participants (as with other stakeholders) view law enforcement and lawful access as only a second-tier value.

Ranking of encryption principles and values among stakeholders compared

Ranking compared

	Overall	General public	Business	Government
Top tier				
1	Privacy	Privacy	Information security ⇈	Privacy
2	Data protection	Data protection	Data protection	National security & public safety ⇈
3	Information security	Information security	National security & public safety ⇈	Trust ⇈
4	Trust	Trust	Privacy	Data protection ⇊
5	National security & public safety	Right to property ⇈	Right to property ⇈	Right to property ⇈
6	Right to property	Secrecy of correspondence ⇈	Trust + Secrecy of correspondence ⇊ ⇈	Right vs. unreasonable search & seizure ⇈
Second tier				
7	Secrecy of correspondence	National security & public safety ⇊		Law enforcement & lawful access ⇈
8	Law enforcement & lawful access	Law enforcement & lawful access	Law enforcement & lawful access	Information security ⇊
9	Right vs. unreasonable search & seizure	Right vs. unreasonable search & seizure	Right vs. self-incrimination ⇈	Secrecy of correspondence ⇊
10	Right vs. self-incrimination	Right vs. self-incrimination	Right vs. unreasonable search & seizure ⇊	Right vs. self-incrimination

Note: Higher (⇈) or lower (⇊) compared to overall ranking

4.2.2 MOST IMPORTANT – THOSE CONCERNING PRIVACY AND INFORMATION SECURITY

The focus group participants as a whole are concerned most about the principles and values of *privacy*, *data protection* and *information security*. This comes as no surprise given that, as explained in Part 2, the principal objective of encryption is to provide information security, that is, to ensure the confidentiality, integrity and authenticity of data and communications.

Virtually all of the focus groups participants believe encryption is necessary to protect the privacy and security of their information and communications. Regulator E explains, "privacy is a top-tier principle of encryption. Otherwise, you won't encrypt. If you don't want privacy, don't encrypt.[89] For User I, "encryption is… a way of achieving [privacy]. It relates to keeping everything a bit more private…. encryption should be there".[90] As a matter of individual privacy and security, "encryption is fantastic on a personal level," claims Regulator E.[91] User G is similarly emphatic about the importance of encryption: "I personally wouldn't subscribe to an app that doesn't enable encryption. But if WhatsApp chooses to not encrypt, then I'll use something that does".[92] User H concurs, "I want a… way to chat with someone and I do not want that information to be leaked or to be taken otherwise in a different context, I'll probably use some messaging service that is encrypted rather than using SMS or something [insecure]".[93]

For focus group participants, using encryption helps protect the confidentiality and integrity of their digital and online data. When a user's computer was stolen, it was reassuring that the hard drive was encrypted because the data remained inaccessible from unauthorised use.[94] With regard to online activities, Regulator G explains that encryption provides "safety.... when you buy things [on the internet]… you feel a bit better about the information being protected".[95] For Regulator B,

> on a personal level, that sort of encryption – you look for a little lock on the webpage. It's the only level of comfort you as a consumer can get from transacting with somebody. That's at least a known state… at least if it's encrypted, I know it's a 2-way transaction and it's not going to fall apart.[96]

Regulator B continues,

> you're looking for that, because [they're] your things. Before, we went and we locked your things in a safe. Now, your mortgage documents are just going into your Dropbox, so you do want that level of comfort and security. The only real digital insurance you can take out is encryption. It's the only thing you can rely on.[97]

---

[89] Focus group interview with Regulator E.
[90] Focus group interview with User I.
[91] Focus group interview with Regulator E.
[92] Focus group interview with User G.
[93] Focus group interview with User H.
[94] Focus group interview with a user.
[95] Focus group interview with Regulator G.
[96] Focus group interview with Regulator B.
[97] Focus group interview with Regulator B.

Encryption is likewise seen as indispensable for secure communications. "If there's anything transmitted over a wire that someone can access, you need it," explains Provider D.[98] With regard to authenticity and identification, Regulator L explains how government services rely on encryption:

> people… interact with government services… by using digital identifiers. So, looking at… RealMe, they have to trust that system to say that when I go to interact with, say, IRD, Internal Affairs is just passing out my details so that I can interact with government agencies a lot quicker.[99]

But encryption is not limited to personal use. A growing number of companies, organisations and government departments use encryption as standard protocol or practice. Businesses in particular, especially those involved in information security or deal with customer data, turn on encryption by default. Provider Q explains that "it's essential in the business I work for that our communications with customers have to be protected at all times, even if it's considered 'unclassified'. The customers expect to be protected at all times".[100] "So, it really is a policy thing," states Provider A, "We have to have that. Nobody's going to use our product if they think people can possibly intercept that or if it's not safe on the trip between the client and the server, so yeah, it's really important for us…. it just simply has to be secure".[101] Businesses like Provider H's that recognise the importance of information security "have standards that talk about encryption protocols you can use, encryption ciphers… key lengths… things like that… and what data should be encrypted and what types of communication must occur over an encrypted channel. So, we're quite precise".[102] Encryption is clearly an integral part of their businesses, products and services. According to Provider D, "for us, we go to great lengths to encrypt things both because we're driven by the customer to do so and because we design encryption into our products".[103] For Provider L, since our "product that carries customers' data and stores it. So, we ought to take security very seriously, and so encryption is a big part of that".[104]

[98] Focus group interview with Provider D.
[99] Focus group interview with Regulator L.
[100] Focus group interview with Provider Q.
[101] Focus group interview with Provider A.
[102] Focus group interview with Provider H.
[103] Focus group interview with Provider D.
[104] Focus group interview with Provider L.

Government departments and agencies likewise implement encryption on their information and communications systems as a matter of security and privacy. Regular B explains,

> we've got a principle that you are encrypted and secure by default. We're always thinking, "How do we make it more secure? How do we find the ways?" It's part of, if you select systems or solutions that you want to embed into your organisation. It starts with secure by default. If it's not secure, it's not even on my list. It's just an automatic out.[105]

Regulator G recounts how "we have processes set up the same way other government departments have to ensure that what goes around from place to place is confidential because we've got [sensitive] details, [confidential] strategies and all that sort of stuff, which need to be protected as much as they need to be".[106] Regulator L notes how "for us, we use encryption every single day. And that's [for data] going overseas, but even within our own room – everything gets encrypted even when we're sending stuff to each other".[107] The importance of encryption is especially pronounced when dealing with highly sensitive information like patient data. A regulator relates how

> we've got to encrypt patient data. We are required to do so by the health standards the government has put in place. And they set some pretty explicit encryption requirements for how patient data is stored, how it's transmitted. And we've set up a network between health providers that's encrypted. It's only available to health providers.[108]

A provider believes that encryption is vital to protecting health data:

> for us, encrypting data… the copy of the data that we hold about the patient on our servers and also the transmission and also all the configuration files that we have on the practices' computers, all of that needs to be encrypted so that no one is able to tamper with that or people who should not have access to read it are not able to do it. So, yeah, encryption for us is very important for those purposes.[109]

Another provider exclaims that, "it's pretty important, especially when you consider the adversarial aspect of working with a lot of government clients, we also take on a lot of the responsibility of protecting their data as well. So, [it's] very important for us".[110]

---

[105] Focus group interview with Regulator B.
[106] Focus group interview with Regulator G.
[107] Focus group interview with Regulator L.
[108] Focus group interview with a regulator.
[109] Focus group interview with a provider.
[110] Focus group interview with a provider.

It is evident that all three categories of stakeholders view encryption as necessary for living in an increasingly digital and connected world. User C notes that "if we want to get involved in a network, distributed computing environment, which is what we now have – and increasingly so – then we need these protections in place, as much to protect us from ourselves as to protect us from those people who want to do us harm".[111] User M acknowledges that "encryption is important. This is useful technology. It's useful everywhere".[112] Regular P agrees, "We all use encryption these days. You may not even realise it, but you are. You buy something online, you've used it".[113] Regulator I sums up the stakeholders' general perception of encryption: "much of what we do in our everyday life, we rely on encryption – we're all agreed" [114]

4.2.3 LEAST SIGNIFICANT – THOSE RELATING TO CRIME AND CRIMINAL INVESTIGATIONS

At the other end of the spectrum, the focus group participants on the whole regard crime and law enforcement related principles and values such as *law enforcement and lawful access*, *right against unreasonable search and seizure*, *secrecy of correspondence*, and *right against self-incrimination (including right to silence and other rights of persons charged)* as having the lowest priority. As Provider H explains, "People think about encryption, about secrecy, about [data] protection. I don't think people think about law enforcement and rights of [persons charged]".[115] One possible explanation that has been advanced to account for this intriguing finding is that focus group participants may have a preference for individual rights (e.g., privacy and right to property) over public interest values (such as law enforcement and lawful access). However, based on observations of the data, the focus group participants cannot be said to be individualistic. In fact, all categories of stakeholders exhibit a strong sense of community and social awareness. Furthermore, national security and public safety, which is a law enforcement and public order value, is ranked in the top tier.

[111] Focus group interview with User C.
[112] Focus group interview with User M.
[113] Focus group interview with Regulator P.
[114] Focus group interview with Regulator O.
[115] Focus group interview with Provider H.

The most plausible reason, based on the analysis of the empirical data, is that focus group participants do not consider these crime-related principles and values pertinent or applicable to them on a personal level because they esteem themselves to be law-abiding people. Since they are not criminals and are not involved in criminal activities, such criminal procedure rights and the goal of effective law enforcement are not particularly relevant to them. This reasoning is akin to the "nothing to hide" argument that "permeates the popular discourse about privacy and security issues" especially government surveillance.[116] The logic goes, upstanding people should not remonstrate against the scrutiny or intrusion of government because, if they have not committed anything unlawful, they have nothing to fear or hide.[117] This sentiment is espoused by some focus group participants. Regulator Q expresses the familiar refrain that "if I haven't got anything to hide, then I don't really care if somebody looks at it because I'm not intentionally engaging in something that" is illegal.[118] Regulator R even opines that "I mean, just by saying you've got nothing to hide, you've clearly got something to hide".[119] Regulator L claims that "we don't want to actually breach the privacy of individuals who are civic-minded, but we're not going to actually overlook criminal behaviour".[120]

The converse of the "nothing to hide" argument is that mainly criminals would need to use encryption. Regular R notes, "you've got the question of how… 'bad actors' are using it as well".[121] As Regulator H says, "we can't just let basically the criminals and everyone who wants to hide from what they should be doing, just say, 'Let's let them do it'".[122] "I don't think there's any problem with that if someone's broken the law", Provider O argues, "that comes down to my morals. My morals say that if someone has committed a crime, I want them to be held accountable for it. And I have kids, and I don't want that murderer to be on the street or that rapist to be on the street, and potentially hurt them".[123]

While the focus group participants understand that encryption is an example of dual-use technology (i.e., it is designed and used for both legitimate and illegal purposes),

[116] See Daniel Solve, "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy" 748.
[117] See Daniel Solve, "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy" 748.
[118] Focus group interview with Regulator Q.
[119] Focus group interview with Regulator R.
[120] Focus group interview with Regulator L.
[121] Focus group interview with Regulator R.
[122] Focus group interview with Regulator H.
[123] Focus group interview with Provider O.

they are worried about its criminal use and the negative impact on effective law enforcement. Regulator F states, "I think the problem is that we want it for good purposes, but how do we protect it from being used for bad? And I think that once you get it out there, anyone can use it".[124] Regulator H explains,

> from a law enforcement and security side, if everything is encrypted, then the bad guys are using it as well too. And it'd basically be like opening up the borders and being like, "Let's let everybody bring whatever they like on aircrafts and ships and things like that and the government shouldn't see it."[125]

Provider H also feels

> sometimes [the use of encryption is] a bad thing. If I want to investigate you being up to no good or I'm working for someone who wants to investigate you, encryption makes my life harder. So, it's not always a good thing. So, for… law enforcement, I'd rather not have encryption sometimes.[126]

Use of encryption by "bad actors [is] going to make it more challenging," explains Provider O, "so if it's smashed up everywhere else, I think they'll change the law to make sure the provider can give that to law enforcement".[127] User K points out, "the fact that, through the widespread use of crypto, you can no longer target those smaller [criminal] groups. So, everyone's use of crypto does affect" policing and law enforcement.[128]

Some focus group participants though question the association of encryption with criminality. As User J exclaims, "But why is this different from other things? We don't say people can kill people with cars when terrorists commit acts with cars that we should ban cars or make all vehicles remotely operated. Why is encryption singled out?"[129] User J continues, "you can get the same argument with cash. If everyone used cash, it would become really hard to trace, so no one should use cash".[130] User M agrees,

> that's the thing that kind of grinds my gears with all the public debate and advocacy from law enforcement about encryption being a problem. The London cases, the terrorist who, "Ahh! WhatsApp is the problem!" Dude used a car and a $5 knife after being radicalised, right? You're not talking to Hyundai or the makers of knives. So, I get that it's the new technology, it's

[124] Focus group interview with Regulator F.
[125] Focus group interview with Regulator H.
[126] Focus group interview with Provider H.
[127] Focus group interview with Provider O.
[128] Focus group interview with User K.
[129] Focus group interview with User J.
[130] Focus group interview with User J.

> the thing that's helping the network affect him, and the bit that you're shut out of as a law enforcement surveillance agency[131]

User O is even more incredulous:

> the constant statement by the state actors is that encryption enables bad people. It almost feels like misinformation, potentially a distraction. You can't tell me they stopped… [finding a] leak. They've adapted, absolutely adapted. So, do we really believe the state actors have gotten themselves this stuck on encryption in the last five years? I don't know, maybe the politicians are that stupid. So, it's an interesting debate. I like the hammer analogy. It's just a common tool.[132]

User P exclaims, "There we go! What should hammers look like? Should they be big? Should they be small? Hammers can also be used in aggravated robberies. Hammers can also be used in a lot, so encryption should be" as well.[133]

A number of focus group participants believe that associating encryption with criminality has a detrimental effect on users, but has no significant impact on actual criminals. Provider O argues, "I think one of the interesting things with that is… it actually makes life more difficult for people who are not going to break the rules. And the people who are going to break the rules, they know how to get past them anyway".[134] User L explains, "the counter argument is always, well, we can't catch the bad guys then. Which I think is false".[135] User J interjects, "you weren't catching them to begin with".[136] User L elaborates further, "the thing is that if you're a bad guy, you're going to use encryption. It's science. You can't take it away. You can stop normal people from using it, but then what do you gain? Nothing. You can't spy on the bad guys".[137] User M concurs, "if you're a serious criminal, you're going to know what technology is available. Serious, organised criminals have always used technology, they're at the forefront of tech use. They just always have, that's what they do. Encryption is no different".[138] User L contends, "I'm sorry, I still don't quite understand how you regulate and what the benefits of regulating encryption would be, because, if you're a criminal, you're a criminal. You

[131] Focus group interview with User M.
[132] Focus group interview with User O.
[133] Focus group interview with User P.
[134] Focus group interview with Provider O.
[135] Focus group interview with User L.
[136] Focus group interview with User J.
[137] Focus group interview with User L.
[138] Focus group interview with User M.

don't care about regulation or laws. So, it doesn't gain you anything".[139] Some participants are of the opinion that, "the benefits to encryption outweigh any detraction that you might have from some criminal misuse of it".[140]

Despite the heated and strongly-worded arguments about the legitimate and illegal uses of encryption among different stakeholders, it is noticeable that the discourse mainly works on theoretical level and is more or less a general plea to logic and rationality. For people taking part in the encryption debate, there does not seem to be any personal stake involved. And why should there be, when most of the focus group participants have not and will likely never find themselves in situations where they will need to claim the right to self-incrimination and other rights of persons charged.[141]

Conspicuously, this is in stark contrast to the great concern that all categories of stakeholders have for privacy. Privacy is top of mind for most focus group participants and was one of the perennial topics raised and discussed in all focus groups. In a host of focus groups, the issue of privacy (e.g., the Facebook and Cambridge Analytica scandal) was the subject of much enthusiastic debate even though the use of encryption cannot directly address or solve privacy concerns on social networking sites since most of the information shared and stored on these platforms are meant to be openly shared with others. Unlike privacy though, the right against unreasonable search and seizure and other crime-related principles and values do not hit close to home for many focus group participants. As a personal or practical matter, such principles and values do not even show up in their consciousness. This could be explained by the fact that the focus group participants do not see the right against unreasonable search and seizure as a foundation of privacy. It is also possible that the participants do not see how the right against unreasonable search and seizure also protects against excessive or intrusive government surveillance.

What is ironic though about this finding is that, as explicated in Part 3 on the laws of encryption, the legal rights, principles and values that protect privacy and personal integrity the most are the very same ones considered least significant by the focus group participants, namely: the right against unreasonable search and seizure (including secrecy of correspondence) and right against self-incrimination (including right to silence and

[139] Focus group interview with User L.
[140] Focus group interview with Provider G.
[141] It should be noted though none of the focus group participants were recruited because they are convicted criminals or persons previously charged with an offence.

other rights of persons charged). People as a whole fail to see the criticalness of the right against unreasonable search and seizure in protecting their reasonable expectation of privacy. This is especially noteworthy give that, in New Zealand as well as in other jurisdictions, the protection of privacy is principally founded on or springs from the right against unreasonable search and seizure.

Going back to the concept of nothing to hide, people often forget that human rights (whether related to crime or not) apply to and protect all persons and not just suspected criminals. It bears remembering that "New Zealand does not have one Bill of Rights for law-abiding persons and another for those suspected of significant crimes".[142] Asserting one's human rights and freedoms is an essential part of living in a free and democratic society and doing so does not and should not imply that you are criminal.

4.3 Relationships between principles and values

4.3.1 ACCORDING TO DIFFERENT STAKEHOLDERS

Although the hierarchy or ranking in the previous section provides a basic overview of the relative importance placed on the different principles and values of encryption, it does not capture the dynamic relations and interactions between and among them. There is so much more to the principles and values of encryption than where they rank in order of importance. In truth, it is the interactions and interconnections between the principles and values that are most revealing.

While the bracketing of principles and values into top and second tiers is consistent among the three groups of stakeholders, their understanding, conceptualisation and visualisation of the relations among the principles and values are unique. Asked to rank and order the 10 principles and values as part of a focus group exercise, the three categories stakeholders followed their own logic or reasoning for organising and visualising the principles and values.

4.3.1.1 For businesses

A focus group of business people arranged the principles and values in fairly straightforward manner (see figure below). They were sorted into two columns: one for

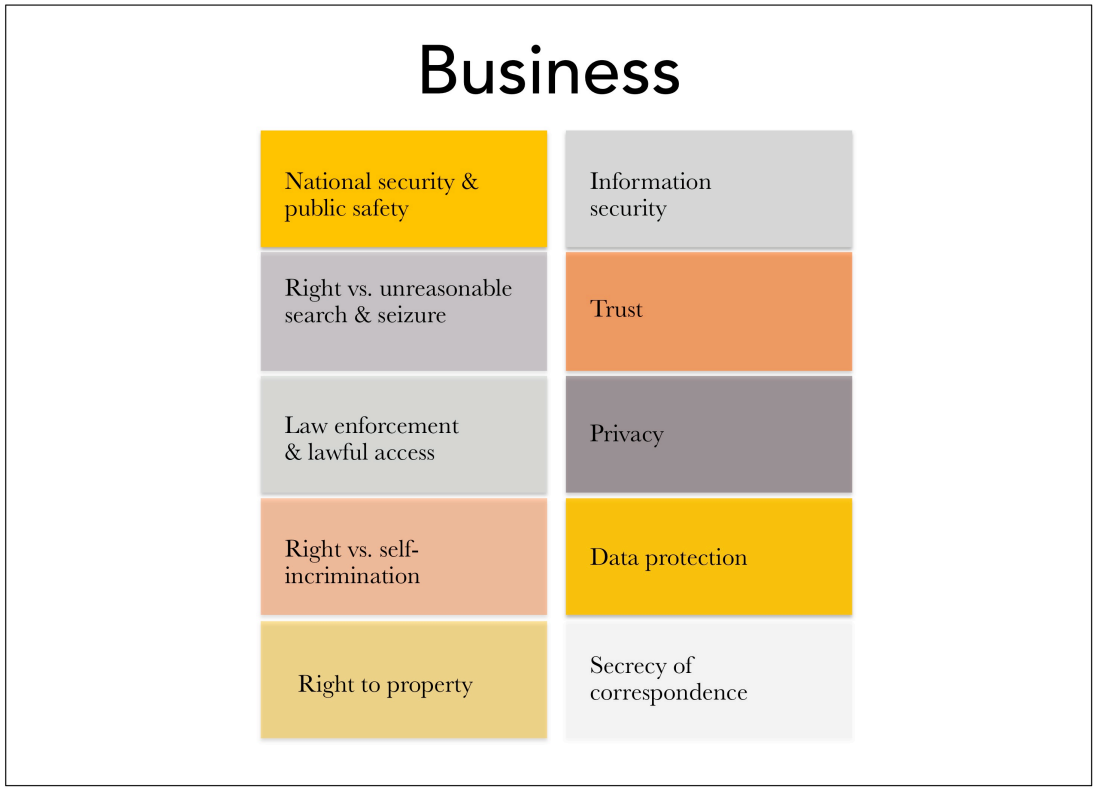
[142] Paul Rishworth and others, *The New Zealand Bill of Rights* 470.

those connected with national security and law enforcement and another for information security. "They're two strands, aren't they?" notes Provider Q, one is about "government and nation" and the other pertains to the "commercial" or "private sector".[143] Provider N agrees, "Yeah, it's kind of a big bracket thing".[144] Provider P elucidates further:

> You can kind of classify these into two areas… these [on the left column] are kind of your moral reasons as to why you would have encryption. And then over here [on the right]… [are] what we're actually trying to do with encryption.[145]

On the left column, the focus group participants placed national security at the top and below it was right against unreasonable search and seizure, law enforcement and lawful access, and right against self-incrimination (including right to silence and other rights of persons charged). On the right column, the participants put information security at the highest level followed by trust, privacy, data protection and secrecy of correspondence.

Organisation of principles and values by business



[143] Focus group interview with Provider Q and Provider O.
[144] Focus group interview with Provider N.
[145] Focus group interview with Provider P.

According to Provider N, "For me, information security is probably going to be pretty high up there. I think that's one of the primary purposes of encryption".[146] Provider O agrees, "This is up there".[147] Explicating the relationships between the principles and values in the right column on information security, Provider N says, "the trust aspect… might give you an indirect sense of trust, but not directly. There's privacy [which can preserve trust], because privacy encompasses more than just encryption. Whereas… secrecy of correspondence and data protection are what encryption [provide] as a technical definition".[148] Provider O expounds on the importance of trust for information security, "As a customer, you trust your provider to keep your data private…so effectively what we're looking to do as the person who sells or the person I'm buying stuff from [is that] I can trust them while my privacy is protected. The information security is just how they're doing it".[149]

With respect to national security concerns in the left column, Provider O believes that

> the security of our nation is critical and that security is based on keeping us safe. While we'd all like to think that people are doing the right thing and being nice, there are many organisations and many country state actors that are not. And that impacts our economy as well.[150]

Provider O says, "national security and public safety is the same as law enforcement [and covers] right against unreasonable searches".[151] But with respect to right against unreasonable search and seizure, "I would probably put that one near the bottom," comments Provider N.[152] Provider O concurs, together with "rights of persons charged".[153] Nevertheless, these are still important because "if I'm charged with something, then I'm innocent until proven guilty. The law enforcement agencies need to be able to get the data to charge me with fact, and my own lawyers need to be able to protect me".[154]

Notably, the focus group participants from business set apart right to property from the others. For them, it does not seem to fit within the two columns of national

[146] Focus group interview with Provider N.
[147] Focus group interview with Provider O.
[148] Focus group interview with Provider N.
[149] Focus group interview with Provider O.
[150] Focus group interview with Provider O.
[151] Focus group interview with Provider O.
[152] Focus group interview with Provider N.
[153] Focus group interview with Provider O.
[154] Focus group interview with Provider O.

security and information security. Provider Q sees right to property "in terms of intellectual property".[155] Provider O agrees, "It's a very intellectual [right or] power".[156]

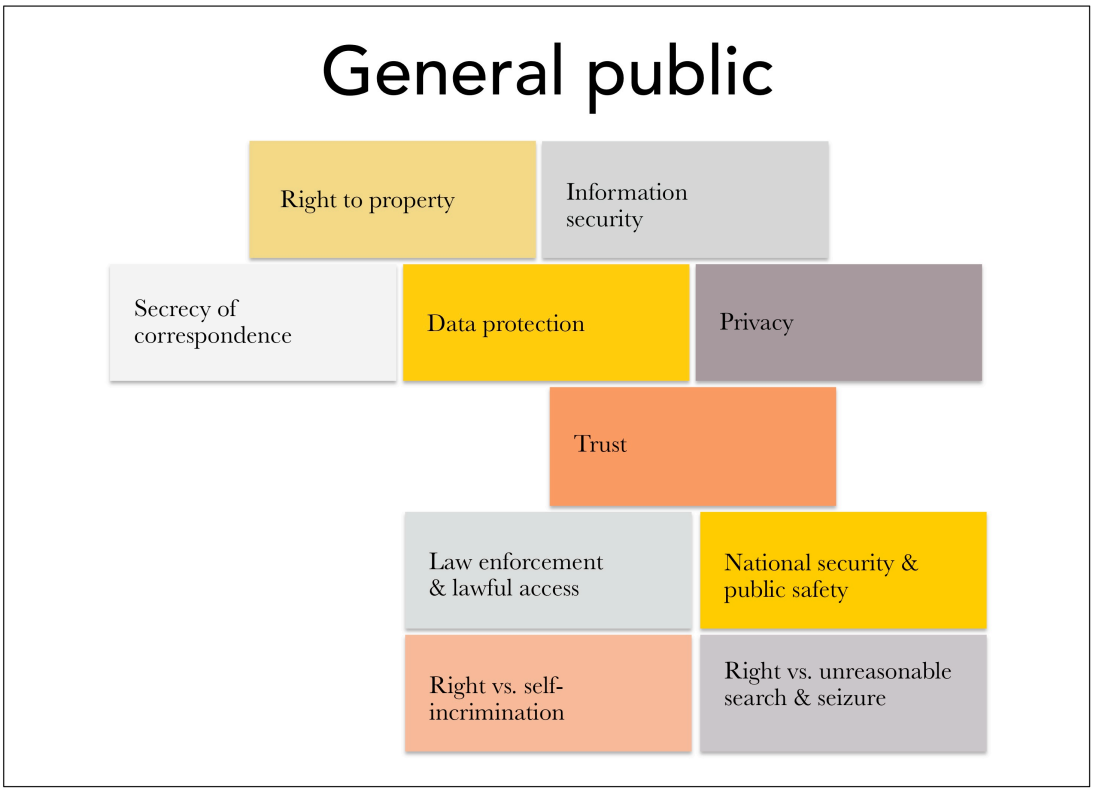
4.3.1.2 For the general public

A focus group of members of the general public also organised the principles and values of encryption into two main groups: privacy and national security (see figure below). The first category covers information security, data protection, privacy, secrecy of correspondence, and right to property. The second category contains law enforcement and lawful access, national security and public safety, right against self-incrimination (including right to silence and other rights of persons charged), and right against unreasonable search and seizure. However, unlike how business stakeholders arranged the principle and values above, representatives of the general public placed trust in between the two groups. User G explains that these are "the rights of the individual versus the rights of the greater good…. At the centre of it… there's trust".[157] User D elucidates further,

> they all kind of relate to the same thing. Because as you're trying to balance those [two sets of principles and values]… there's something about the trust between them. How decisions about that [national security] start to affect this [privacy], or things trying to maintain this [privacy] sort of affect that [national security].[158]

[155] Focus group interview with Provider Q.
[156] Focus group interview with Provider O.
[157] Focus group interview with User G.
[158] Focus group interview with User D.

Organisation of principles and values by the general public



For stakeholders from the general public, the issue of backdoors to encryption illustrates the tension between individual rights and public order concerns and the moderating role of trust. User H posits,

> If I have a device and the government wants to install a backdoor on it and says, "You don't have to worry about anything. Even though we have the backdoor, the data is not going to be seen by anybody. It's only going to be used in certain special circumstances." So, for the public good, do you trust the government to give them the right on your property?"[159]

User I notes,

> I think I'd like to trust the government to look after my national security and public safety if there's something. I really would like them to know that there's a bomb that's going to be going off or that sort of level. But for personal data, well, no. That's I suppose [the] challenge of individual versus [public interests].[160]

[159] Focus group interview with User H.
[160] Focus group interview with User I.

With regard to the use of backdoors for law enforcement purposes, User G says,

> Yeah, it's different… [with] physical property… we say it's just a search warrant. Generally, there's an awareness, you know. They [the police] come, they knock on the door, people come, they've been through your stuff. Unless they're really covert, I guess, and do it in the middle of the night or when you're not there.[161]

But with computer data and information networks,

> You don't know what or when. They [the police] could completely do it without any of your knowledge that they've used that backdoor. There is no means by which, no one [knows]… what they [are] doing. That probably [is] the bigger issue than even what they [are] actually using the data for. It [is] the covert nature of it. And, I think, because it [is] in a virtual world, you just don't know.[162]

User D further reflects how

> there's a lot of talk about trust and systems and social license around the use of data. So, the degree to which other people are able to access data without your expressed permission and consent… is sort of floating around. So, it's kind of like – what's legitimate… use of information? And that kind of gets to that reasonable/unreasonable boundary and who's making that decision and those sorts of things. So, there's all this work going on in that space to try to work out where that line is sitting. What can we get away with? And what can't we? What do we have to have conversations around before people feel comfortable about it? And so, there's a lot of conversation about the relationship that sits between the people here and what they expect if this was kind of more individual stuff and the public uses, whether it's national security or other things.[163]

User F believes trust is important, but, at the moment, "there is no trust between these two [groups of principles and values] actually".[164] User I states, "I think if there was a protocol so that you knew when things are happening, then potentially, but I'd be very wary to say yes".[165] A number of the focus group participants from the general public agree that one could potentially build trust by adopting technical or industry standards that provide transparency and offer "mechanisms which allow end-users to control their data somehow".[166]

---

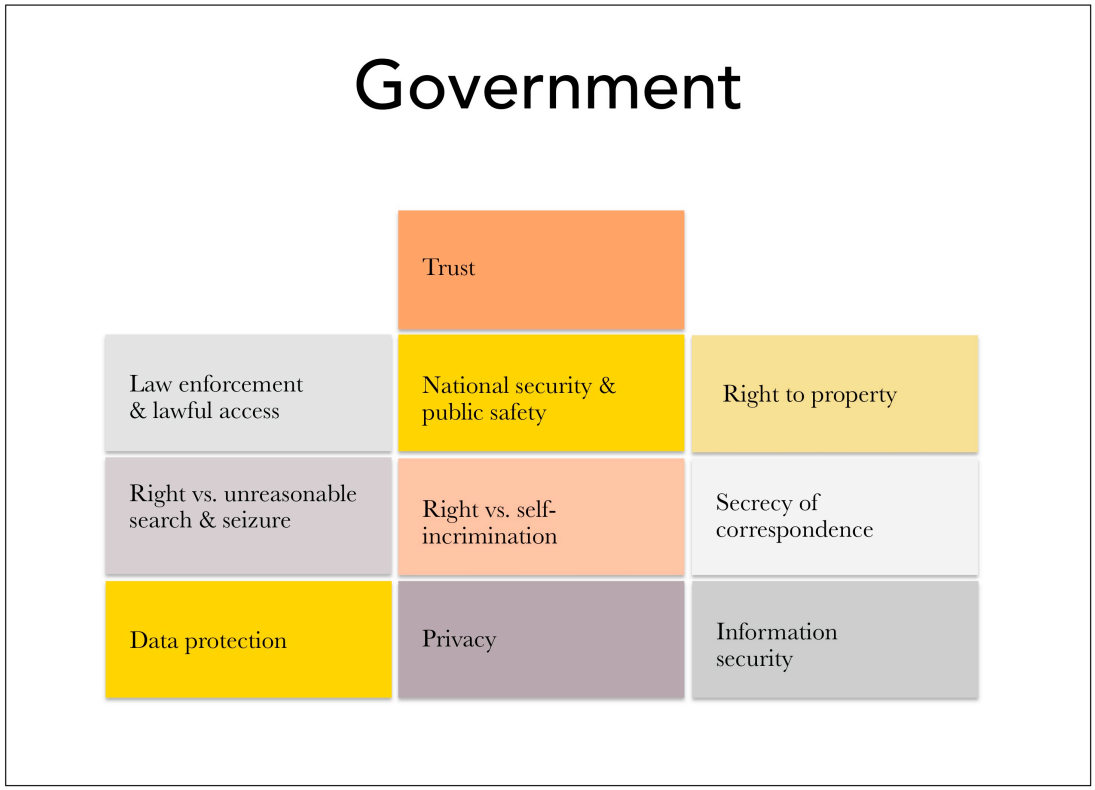
[161] Focus group interview with User G.
[162] Focus group interview with User G.
[163] Focus group interview with User D.
[164] Focus group interview with User F.
[165] Focus group interview with User I.
[166] Focus group interview with Users G, E and F.

4.3.1.3 For government

A focus group of representatives from government had a more formal and structured approach to organising the encryption principles and values. As seen in the figure below, data protection, privacy, and information security make up the base of the structure. On the second level are right against unreasonable search and seizure, right against self-incrimination (including right to silence and other rights of persons charged), and secrecy of correspondence. The next level up is comprised of law enforcement and lawful access, national security and public safety, and right to property. Trust sits at the very top. Regulator B describes how they are

> almost trying to build this tower of encryption principles. Because if this is our foundation of why we encrypt (data protection, privacy, information security), you've got these things [in the middle], and then you sort of have these ones [on a higher level] that sort of go like this, and you've got a tower up. And that is our pyramid of encryption.[167]

Organisation of principles and values by government



[167] Focus group interview with Regulator B.

The focus group participants from government have a generally purposive or functional notion of the principles and values of encryption. The principles and values for them are about "why do [we] encrypt?" and "what's the higher-level purpose of why we encrypt?".[168] According to Regulator E, privacy is a fundamental principle of encryption because if "you don't want privacy, don't encrypt. That's sort of where we've come from. You don't lock it away in the safe, you just put it up on the front counter so [anyone] can read it".[169] Regulator E continues, "data protection… is about… integrity, ensuring the information that is stored and retrieved is the same information".[170] With regard to national security and public safety, Regulator B states that they are

> paramount because I'd like to see you protected and I'd like to see myself protected. And if it is the government that is given the power, we've surrendered our power, a monopoly on personal values to this government to secure us, I'm happy with it if I participate in the selection and the checking of that government.[171]

Regulator F agrees, "I think that's important…. I'm thinking of what we want to be protected against in society – against kidnappings, against terrorists and [other] things".[172] With regard to trust, Regulator B says that "when you encrypt, you must trust. Because if you can't trust the encryption… then it's sort of null and void".[173]

Drawing a connection between the privacy-related principles and values at the base and those involving national security and public safety at the higher levels, Regulator E remarks, privacy "is a thing we *do*, this is a thing we do, but national security and public safety is *what* we ensure [or] maintain".[174] Regulator B elaborates further,

> Because if it's about the principles of encryption, I think you've got to sort of – are we asking if we're encrypting to support national security for public safety or are we saying we want to ensure that when we do encryption that we are able to do that. Because if you look at data protection and privacy, the principle of encryption [is] we do encryption to ensure privacy. Through encryption we drive the principle of data protection, so they sort of become the *whys* – and that's the principle of why you do it. And when you look at this, you've got to sort of have a word here around the *what* about national security and public safety – the protection or ensuring that by itself that this

[168] Focus group interview with Regulators E and B.
[169] Focus group interview with Regulator E.
[170] Focus group interview with Regulator E.
[171] Focus group interview with Regulator B.
[172] Focus group interview with Regulator F.
[173] Focus group interview with Regulator B.
[174] Focus group interview with Regulator E (emphasis added)

> one is almost the verb. We encrypt to make private, [we] encrypt to protect the data.[175]

Regulator B explains that privacy and data protection

> feed up into the national security and public safety, because one of the things you would secure as far as data is concerned is victim's data, for example. You've got someone being released from prison, they're coming out. They've brutalised somebody and they went to prison for it, but they're coming out and they want to find out where this person stays so they can go and do the same thing that they did to them again. Data protection is very important there. Privacy is very important there. If you live in a society where you trust the government to some level, then this becomes implicit.[176]

For the focus group participants, the structure is further divided into "two very distinct" halves: one for national security and the other concerning individual rights.[177] Regulator B explains how the principles and values relate to and interact with each other:

> national security is one where [the left side] ties in very strongly, but [individual rights] is the one where I see that the right to property, secrecy of correspondence and those things sort of sit there [on the right]. They're sort of on the [individual rights] side, and this one [law enforcement and lawful access] sits on the national security side. And, yes, this one [right against unreasonable search and seizure] does feed into [individual rights]. You don't want to have unlawful access of things, but I've got my right to property, so I want to encrypt my property. I've got a right to correspond in a secret way, but with [individual rights] it's my right to communicate and not put myself at risk. But if I put others at risk, then it goes to the national security side, and this [law enforcement and lawful access] sort of ties into it. I think that one [right against self-incrimination (including right to silence and other rights of persons charged] sort of sits in that space. They sort of sit together, because you don't want to have unlawful access. You want to make sure that the [individual rights] side of my things versus the greater good of the community is balanced. And then, right of persons charged… sits sort of in the middle between the two [halves].[178]

Regular F muses, "so, that's almost like a balancing principle. So, we want [national security and public] safety, but at the same time, we don't want the state to be able to do anything it thinks is in the interest of [public] safety. We want some sort of qualifier…. it has to be qualified".[179] Regulator E reiterates the significance of the privacy-related principles and values at the foundation of the structure:

---

[175] Focus group interview with Regulator B (emphasis added).
[176] Focus group interview with Regulator B.
[177] Focus group interview with Regulator B.
[178] Focus group interview with Regulator B.
[179] Focus group interview with Regulator F.

> if we've got privacy principles for encryption then law enforcement and lawful access is, again, subservient to privacy. It's subservient to data protection because the lawful access must ensure that the data protection and integrity is not influenced while they access it. Because that's the whole thing, otherwise if you get lawful access to it and you can manipulate the data, then data protection goes out the window and then your case is sort of weakened.[180]

4.3.2 CONFLICTS AND CONNECTIONS BETWEEN PRIVACY AND NATIONAL SECURITY

The conflict between privacy and national security is a familiar refrain in the encryption debate. It is a truism that privacy and national security seem antithetical to each other. They are viewed by many to be inherently incompatible and eternally at odds with one another. The schism between these two is clearly discernible in the consistently binary categorisation, ranking and organisation of encryption principles and values in the previous sections.

The focus group participants on the whole recognise the clash between privacy and national security. Provider B states, "To me, it's all about privacy. But I don't know how… by keeping the individual private does that decrease [national security and] public safety?"[181] Highlighting the tension between the two principles and values, Provider B emphasises, "That's the governments job [national security], the individual's job [privacy]".[182] According to Regulator H, the incongruence comes from the fact that privacy is about the "good of the individual" while national security and public safety are for "the good of the country".[183] Regulator G contemplates that:

> privacy and national security and public safety, that's the counter balance. That's the push and pull. You've got your one and you're giving up the other side of it. For national security and public safety, it's also crucially important, because, I mean, the police are the only agency that can do any arrests for methamphetamine problems that we've got. And society could just fall apart if they're not able to tap into the need to crack where the next shipment's coming with Customs and the other agencies, and that's just absolutely crucial for that to happen.[184]

[180] Focus group interview with Regulator E.
[181] Focus group interview with Provider B.
[182] Focus group interview with Provider B.
[183] Focus group interview with Regulator H.
[184] Focus group interview with Regulator G.

But despite the ostensible conflict between privacy and national security, paradoxically, some focus group participants perceive a strong and intimate connection between them. Provider A is convinced that they are "two sides of the same coin".[185] Provider D believes that "they're complementary. From the start, I think they're complementary. You can't really get one without the other".[186] Provider D continues, "and there [are] reasons for that, because if you achieve this [national security], then you'll achieve that [privacy]. Look, because [the former] is critical to [the latter]".[187] User Q argues, "I see people talk about privacy as a right and all these other things. Then we end up in all these false dichotomies of do you prioritise [national security and] public safety over privacy? I mean, it's not one [thing over]… the other".[188]

Ultimately, the focus group participants believe that striking a balance between these two competing principles and values is possible or at least conceivable. But achieving a balance is fraught with conceptual and practical difficulties because of the paradoxical nature of the problem. As Regulator E notes, "It's a bit of a conundrum…. there's a balance to be found and there's a sweet spot somewhere, and I don't know where".[189] User E agrees, "So, it's very nuanced and it's context dependent, right? It's complicated…. you want [privacy] protection, but, at the same time, you can appreciate how if there is a genuine national security threat, you want [government to have access]".[190] Provider G recounts,

> when there is a terrorist attack like the Manchester bombings, there's all these cries like, "Well why didn't the government know about this? Why aren't you protecting us? Why aren't you saving us? You're supposed to be watching these terrorists?" And it comes out later that they probably were. They say, "Oh, the government should have access to it!" Then there's some privacy person [who] will say, "There's limits to the power of the government to exercise certain types of investigation" and stuff. So, there's a balance to be struck between privacy of the individual and the power of the government to govern.[191]

Regulator B similarly relates how

[185] Focus group interview with Provider A.
[186] Focus group interview with Provider D.
[187] Focus group interview with Provider D.
[188] Focus group interview with User Q.
[189] Focus group interview with Regulator E.
[190] Focus group interview with User E.
[191] Focus group interview with Provider G.

> the initial conversation that we hear a lot about it is, "No, no, no" [to government access to encryption]. But now we're seeing as the community gets informed and educated around what these things do and what it can be used for, it becomes a "Yes, but"…. We have to find that balance…. I think it becomes a very, very fine balance [192]

As discussed in Part 3, search and surveillance laws and criminal procedure rules appear to be the foremost law and policy area where such a balance can be struck.

4.3.3 SIGNIFICANCE OF TRUST

Proposals to find a balance between privacy, national security and the other principles and values of encryption make sense. But aside from general motherhood statements about the need to strike such a balance, no concrete, workable or feasible law and policy approach, strategy or framework has yet to be put forward. However, pursuant to the principles- and values-based approach of this research and grounded on the analysis of the legal, social and empirical data, it is evident that *trust plays a pivotal and decisive role in negotiating, balancing and reconciling the conflicts and correspondences between and among the various principles and values of encryption*. It underpins and connects them all. Furthermore, it has a hand in moderating the legal, social and technical aspects and effects of encryption.

4.3.3.1 Mediating role

"Trust is a really important principle", states Regulator J and User Q, and they "would put trust at the top" among the principles and values of encryption.[193] Many of the focus group participants consider it an underlying foundation of encryption. "Trust is the number one thing for encryption", says Provider B. This is so because "when you encrypt, you must trust".[194] Regular J elaborates,

> if you look at encryption as the value proposition behind everything you do, what's fundamental to that? That whole establishing and maintaining the trust in your organisation, in the way you manage your data…. trust in how they manage their keys or how they implement their systems and technologies and things like that.[195]

[192] Focus group interview with Regulator B.
[193] Focus group interview with Regulator J and User Q.
[194] Focus group interview with Regulator B.
[195] Focus group interview with Regulator J.

Technically speaking, the networked information society could not function adequately without trust in encryption. As Regulator B explains, "now we're in a society where we have to communicate. Our world is not five city blocks like the old days. Now it is global. We communicate with people across the world. So, you want to have an open conversation with them, and you want to trust" the technologies and systems you are using.[196] User G points out that, "if you're being really nerdy, you might even say trust is just another word for encryption".[197]

Focus group participants give paramount importance to trust because, according to Regulator P, "it kind of underlies all of" the other principles and values.[198] For example, "if you're looking at trust, you're looking at national security…. [and] public safety aspects".[199] With respect to the right against unreasonable search and seizure, Regulator H notes, "we could argue about what is 'unreasonable'. I think it can't be a free-for-all. That comes back to the trust issue".[200] Regulator L explains how

> it's a chain reaction…. If you have the top four – privacy, data protection, trust and… right to property – the knock-on effect is that in turn, the rights of the persons charged will actually be built up because you can trust the system. And the system also says that we have the trust of the citizens.[201]

Some focus group participants also see trust as naturally "clustered together" with "privacy and data protection".[202]

In relation to the multifarious issues and discussions about encryption, trust is a central although often implicit concern. Regulator E points out, "That's a big question about trust. If we look at all these conversations, everything boils down to trust".[203] Regulator E states, "the question is of trust. I look at the technology today, we are looking at the exact same problems. We talk about key escrow, we talk about trusting certain governments and jurisdictions. It's all about trust".[204] "I agree with you that there is that assumed trust", says Regulator B, "and I think that's where if you talk about

[196] Focus group interview with Regulator B.
[197] Focus group interview with User G.
[198] Focus group interview with Regulator P.
[199] Focus group interview with Regulator L.
[200] Focus group interview with Regulator H.
[201] Focus group interview with Regulator L.
[202] Focus group interview with Regulator M.
[203] Focus group interview with Regulator E.
[204] Focus group interview with Regulator E.

information… protection of your data, your private information, security, integrity, confidentiality, I think it… [goes] down to this layer" of trust.[205]

4.3.3.2 Trusting by nature

Focus group participants believe that there is a very trusting culture in New Zealand. "We're very trusting," states User G.[206] "Yeah," Provider A says, "there is a lot of trust".[207] Regulator B explains how "there's a lot of trust here. There's a lot of faith, trust. When you meet somebody, 'My name is so and so. This is what I do.' You trust them, just like that…. So, trust is massive and all those other things feed into it".[208] Regulator O cites a recent national survey, "What is it about Kiwi society that helps it function well? One of them is that basic trust that our fundamentals actually [are fine]".[209] Regulator R says:

> Yeah, I trust my government. I trust my law enforcement by and large. I trust private providers to keep this safe. I trust my doctor with my data and so on. So, I trust they won't stick something on the internet if I ask them not to. So, some of it is *trust about the technology and some of it is trust about institutions and individuals*.[210]

Among focus group participants, trust in government is relatively high. Regulator G says, "the general trust with… government agencies is good and I really value that".[211] Regulator E provides one possible reason for the high trust in government: "you don't have 3-4 layers of government. People tend to trust the government more because they are closer to it. They can walk into their MP's office and have a chat".[212] In addition, Regulator F opines how,

> there's much more uniformity in New Zealand, where maybe there's much more diversity just in terms of police, let's say, for trust in government or the fact that we believe the government will do the right thing, and they're like us. Whereas in the [United] States, there's a lot more differences along those lines of thinking.[213]

---

[205] Focus group interview with Regulator B.
[206] Focus group interview with User G.
[207] Focus group interview with Provider A.
[208] Focus group interview with Regulator B.
[209] Focus group interview with Regulator O.
[210] Focus group interview with Regulator R (emphasis added).
[211] Focus group interview with Regulator G.
[212] Focus group interview with Regulator E.
[213] Focus group interview with Regulator F.

Regulator A states, "how trusting of our government we are…. We're a lot more trusting than America where there's all kinds of conspiracy theories going around. Whereas here, if you hear one, it's very rare".[214] Regulator R adds, "You don't fear your door being kicked down in the middle of the night by people".[215]

Despite their trusting nature, people are not naïve. Provider C notes the growing awareness among people that there is "a lot of over-trust as well" in technologies and other people.[216] Regulator B acknowledges that, while "we have a more trusting relationship [compared to other countries], I think that makes us more vulnerable if we sort of trust by nature".[217] Regulator B continues, "what I call the 'ignorant state' is sort of being slowly broken down, and people are saying, 'Oh, yeah, yeah. I trust you, but…' You know, I think that sort of is going to change for us".[218] User G adds, "We are highly, highly trusting in particularly with big brands. And, oh, the government will look out for me. They won't do anything bad anyway because if they could they would have been stopped by now. And therefore, I'll sign up. We're a very trusting society".[219]

4.3.3.3 Levels of trust

The focus group participants have different levels of trust for various persons, things and institutions. According to Regulator B, there are "multiple tiers or layers of trust levels that you need to assess continuously and to try to work out".[220] In relation to encryption, the "degree of trust" varies depending on the technology or actor being relied on. [221] For instance, trust is important on a personal level. Provider G explains,

> it's one that people can, you know, Joe Six-Pack on the street can visualise. They can put their hands on trust. They know what it means. They might not be able to articulate it, but it's a feeling they get. And, they might not be security specialists… but it's something that's important to people, and encryption is an enabling component of that.[222]

[214] Focus group interview with Regulator A.
[215] Focus group interview with Regulator R.
[216] Focus group interview with Provider C.
[217] Focus group interview with Regulator B.
[218] Focus group interview with Regulator B.
[219] Focus group interview with User G.
[220] Focus group interview with Regulator B.
[221] Focus group interview with Provider B.
[222] Focus group interview with Provider G.

As individuals, people often believe and say to themselves that "I trust myself… I've got my own password…. I trust that my data is private".[223] It should be noted though that there is a common sentiment among focus group participants that there is a general lack of awareness and basic knowledge and skills about encryption among the general populace as well as some businesses and government actors.

Then, there is the interpersonal or social dimension where people need to interact with and trust others. For User P, it is about "being able to have trust in how I interact online, being able to have trust in who I'm talking to…. It's different than having an amount of privacy in what I do. It's about… trust [that] the person I'm talking to is the person I believe it is".[224] Provider G adds, it's about "trusting that I'm speaking to the person I think I'm speaking to. Or that the message… or some other characteristic of the data… hasn't been tampered with whilst it's in transit".[225] Regulator B says that trust is "quite important… [in] an open, digitally enabled world" since you are "trusting [another] person with your information".[226] In a connected and technologically-mediated world, it is unavoidable for people to put their "trust in somebody else".[227] User C explains how, "[we] rely on our Dropboxes, on our Amazons, on our Googles and Facebooks and everything else that uses those cloud services. These people rely on these people that are looking after that thing…. Cause these people trust those people who trust those people".[228] Aside from the technology, people need to be able to trust other persons and institutions including businesses (that develop and provide encrypted products and services) and government actors (who regulate how encryption is used and accessed).

Trust is very important for private and public entities that provide services to or directly deal with the public. For commercial companies, "it comes down to trust. Business is about trust".[229] Provider K states, "I don't think that any individual would trust any of the data that we provide if they knew that anyone would fake [the] results or something like that. That encryption piece is part of the user's trust in the service that we provide".[230] Trust is closely related to information security. As Provider G explains,

---

[223] Focus group interview with Provider B.
[224] Focus group interview with User P.
[225] Focus group interview with Provider G.
[226] Focus group interview with Regulator B.
[227] Focus group interview with Provider A.
[228] Focus group interview with User C.
[229] Focus group interview with Provider L.
[230] Focus group interview with Provider K.

"Essentially… security is a means to an end. This is not a thing you should do just for the heck of it, because there's usually a business requirement to do so. And the business requirement is usually trust".[231] Provider H says,

> if this is about trust – why do I do business with Bank A or Bank B? I trust them. Why do I do business with you? I trust you. That trust is built upon, I know you. I can shake your hand. It's based upon [the fact that] I know the integrity of the information you sent me, it's a whole range of things, but it is trust.[232]

Provider G adds, "yeah, it's a business outcome. Or it could be a personal outcome if you're talking about personal banking. It's the outcome you're interested in".[233] User D notes, "encryption becomes more about… how the commercial end or who is running it maintains the confidence of its users".[234]

Likewise, government actors see the importance of maintaining the trust and confidence of the general public. Regulator J explains,

> government is trying to modernise rapidly, and we have some strong drivers to bring more of our services online. For people to engage with government, they have to have really strong trust with them. I'm willing to engage over this dirty battlefield called the internet, and I'm willing to send my information to you and trust you to manage that properly. So again, trust is part of the value proposition of any organisation that is providing digital services.[235]

Regulator L notes that "it's building that trust to allow people to actually interact with national services, and being able to actually maintain their privacy, but also still be able to keep it nice and contained".[236] Regulator B adds, "for us, in our customer services, we just go secure by default and that's how our customers expect it to be. And that's a good thing, because that's a trust relationship".[237] Regulator A agrees, "confidentiality for our clients, obviously, is paramount. But often, again it goes back to trust".[238]

---

[231] Focus group interview with Provider G.
[232] Focus group interview with Provider H.
[233] Focus group interview with Provider G.
[234] Focus group interview with User D.
[235] Focus group interview with Regulator J.
[236] Focus group interview with Regulator L.
[237] Focus group interview with Regulator B.
[238] Focus group interview with Regulator A.

4.3.3.4 (Dis)trust of businesses and government

Focus group participants though have a healthy distrust of businesses and government alike. Regulator B notes people's reservations about companies especially in relation information privacy and data breaches:

> You're not trusting them with that information if they've got 50 backdoors and will just leak it out. And, I think when this whole Facebook/Cambridge Analytica thing came about.... Because, everybody trusted Facebook, because you're trusting and it's your little community of friends and information you share. But they've actually broken that trust".[239]

User G states, "If Google came to me and said [its service is encrypted], I'm not convinced I'd be as sure. And if it was a WhatsApp or Snapchat or as you get more into that informal space, I don't think my level of trust would be anywhere near as high".[240] Regulator P also points out how "there's also the tendency to like smaller businesses rather than large. Big – bad, small – good. So, the fact that the big can be professional and small can [have] small resources and potentially more dodgy… that doesn't really enter" people's consciousness.[241]

Focus group participants though remain critical and wary of government. According to User D, "there might be a generally trusting culture but… lots of people that have to engage with the government regularly don't trust the government". .[242] There are "pockets of people who don't trust the government" including from the Maori community.[243] Regulator N explains that trust in government "depends on the agency. In government, I think, and that's what the surveys will represent, there's some that are really highly trusted and others that really aren't".[244] Regulator Q interposes that one's level of trust "depends on who you are as well".[245] Regulator R concurs,

> You ask me about trust in government or trust in businesses, I'd say, "Yeah, I trust it." But that probably speaks more about me and my place currently in society rather than whether or not that's a reasonable rational level of trust that I've got. It's more that my government doesn't impinge on me in a way that makes me fear it. Maybe if I'm having to go into WINZ [Work and Income New Zealand], I'm more concerned or if I have an active, ongoing

[239] Focus group interview with Regulator B.
[240] Focus group interview with User G.
[241] Focus group interview with Regulator P.
[242] Focus group interview with User D.
[243] Focus group interview.
[244] Focus group interview with Regulator N.
[245] Focus group interview with Regulator Q.

> ACC [Accident Compensation Corporation] claim, which isn't going my way, I might answer the questions differently.[246]

Regulator O points out that this may be due to the distinction between "perceived trust versus experienced trust in terms of government services".[247]

Aside from people's different experiences with government, there are other reasons for focus group participants' distrust of government. For one, there is the government's perceived lack of knowledge and expertise in encryption and information security. User G argues, "I'm not sure I don't trust the government… [because] they intend to do the wrong thing. I just don't trust the government to be smart enough to do it well".[248] Provider C echoes this concern,

> It's not that I don't trust them in that regard. It's that I don't trust them to keep that information to themselves. And even if you do trust that party that has access to your information, they make mistakes. And it happens all the time, and people that you don't want to have access to that information end up getting it. And so, it's a weakness that ends up getting exploited in a lot of cases too. So, because of that, you pull back.[249]

Regulator E raises a similar problem:

> you will trust some governments, and you won't trust others on the basis of their platforms, of their policies and so on and so forth, and on the basis of whether they keep their promises or not. You look at them, and you say, "Come on, guys, if you say you are going to do this and you can't even do this, how can I trust you when you say you are going to keep our data safe without accessing it, when you obviously couldn't keep this promise?[250]

Second, there is concern over government surveillance. User D says, "If you use [public] services, any kind of services, you already feel like they've got you under surveillance".[251] Regulator R also points out,

> you've got to have confidence – not only in the people that are using it, but confidence in the government. Because the government is actually surveilling people that are using that type of system, and they're kind of going, "What happens if the actual key gets into the wrong hands?"[252]

[246] Focus group interview with Regulator R.
[247] Focus group interview with Regulator O.
[248] Focus group interview with User G.
[249] Focus group interview with Provider C.
[250] Focus group interview with Regulator E.
[251] Focus group interview with User D.
[252] Focus group interview with Regulator L.

User D notes how governments are collecting vast amounts of data: "You see more and more of that now. And they're putting it together and more available. So they're becoming… Google-like".[253] Lack of transparency and government secrecy is another issue. Regulator M argues,

> people do care more when government do it. I think because there's a whole secret agency, we don't know what they're doing. They have all these powers. There's that aspect of government that naturally makes people more worried regardless of what they're actually doing.[254]

Finally, there is also the apprehension of the possibility of a change in government or fundamental switch in government policy. Regulator F notes how trust "can change with the change of government".[255] Regulator F continues, "what if… like what we've got here… the [current] government… is okay, but then, something happens, and you get a less favourable government?"[256] Regulator H summaries the focus group participants' trust and distrust of government: "we can't just say, 'Well, good old government, we can trust governments, so let's give government the full control of everything' either. I think that tension and that constant movement between the two is really important".[257]

It is noteworthy that focus group participants seem to trust businesses a bit more than government. This is the same as with countries like the United States but different in Europe where people tend to trust the state more than private companies. User E conveys a general sentiment:

> I think the scepticism and mistrust of government is interesting, especially when you think about it as it relates to people's opinions of governance. And then thinking about it as it relates to companies like Google. I think there's much more trust in companies at the moment than there is in government. And I think that in and of itself is troubling. These are really kind of complex [issues]."[258]

In relation to encryption key management, Provider H explains how "key escrow agents tend to be private sector…. A large bit of it is because they'd [businesses] rather trust a private organisation and don't trust a government-run organisation".[259] For members of the general public, User O explains,

---

[253] Focus group interview with User D.
[254] Focus group interview with Regulator M.
[255] Focus group interview with Regulator F.
[256] Focus group interview with Regulator F.
[257] Focus group interview with Regulator H.
[258] Focus group interview with User E.
[259] Focus group interview with Provider H.

> People probably don't care that much about encryption in public. They care about individual entities. They trust Facebook. They trust their bank. They don't trust the government. So, when the government makes this security stuff up, even when it's tiny, Boom! Absolutely massive outrage over the thing. But if a bank does it, it's like, well, I'm probably going to get the money back anyway, because banks generally cover that.[260]

Regulator I notes, "Yeah, so… citizens don't mind if corporates breach their information, their privacy, but if the government does it, whoa!"[261]

Regulator P reflects, "There's a distinction between the government and the companies that you're consciously around, that are consciously important to your life".[262] Regulator O argues though, "Is there? At least for the time being I vote for government, I don't have a lot of voting power as far as Mr. Facebook is concerned".[263] "But you don't have to use Facebook," Regulator P counters, "You don't have to buy a Samsung smart fridge in ten years' time".[264] Regulator M muses, "I just don't know [if] it's okay to say that everyone's fine with it when corporates do it. I think it's more that everyone has so much of their lives on Facebook, it would take something more".[265] Regulator L raises other relevant points,

> I think realistically what you have to look at is when you look at people, citizens are financially invested in government. They don't pay to get access to Facebook. They don't care about corporations or if they're making a profit. But when they look at government, they pay their taxes, the first question they ask is, "What's my taxpayer's median?" So, they're financially invested there. They're kind of going, "Oh God, how can government do this to us? They're supposed to be there looking after us. We pay them to look after us![266]

Regulator H also notes that "you're compelled as well to give your data to IRD or whatever, where you've got the choice with Facebook. So even though you're not going to delete your Facebook, you could".[267] Regulator M highlights another important difference between businesses and governments:

> the government has the ability to prosecute you. The government has all this power. Corporates only want to sell you more stuff. The fact that they do it in

[260] Focus group interview with User O.
[261] Focus group interview with Regulator I.
[262] Focus group interview with Regulator P.
[263] Focus group interview with Regulator O.
[264] Focus group interview with Regulator P.
[265] Focus group interview with Regulator M.
[266] Focus group interview with Regulator L.
[267] Focus group interview with Regulator H.

> increasingly creepy ways, like, oh well, they only want to sell me more stuff. Whereas, what will government do? They'll find out that I was jaywalking last Wednesday and they'll arrest me.[268]

4.4 Complex relations and possible connections

In summary, encryption involves 10 fundamental principles and values. These principles and values can be further categorised into (a) human rights and freedoms or (b) law enforcement and public order. They also have varying degrees of significance to different groups of stakeholders (the general public, businesses and government). Across all stakeholders, the highest importance is placed on privacy, data protection and information security. At the other end, the least priority is given to crime and law enforcement-related principles and values such as secrecy of correspondence, law enforcement and lawful access, right against unreasonable search and seizure, and right against self-incrimination (including right to silence and other rights of persons charged). In addition to their relative rankings, the relationships between and among the principles and values are complex and conflicting especially between those belonging to the two main categories (i.e., human rights and public order). This is particularly evident in the long-running debate over privacy versus national security. Despite their perennial clashes, there are noteworthy connections and correspondences between and among the principles and values of encryption. The most significant of these involves trust, which is itself a paramount principle and value. As discussed above, trust can act as an intermediary that intercedes between, balances and reconciles the other principles and values with each other. This and other notable insights, conclusions and recommendations are presented in greater detail in the next and final part of this report.

[268] Focus group interview with Regulator M.

Conclusions and general policy directions

Based on the examination of the technical, legal and social dimensions of encryption in the previous parts of this report, it is clear that encryption is a complex and multifaceted technology. Despite this complexity, this study has shown that focusing on the principles and values of encryption provides a clear, grounded and useful framework for observing and analysing the competing interests and concerns of different stakeholders. Gaining a better understanding of what these principles and values are and how they relate or interact with each other creates possibilities for developing new approaches and finding other ways to address the multifarious problems and issues raised by this technology. While it is beyond the scope of this research to put forward specific or detailed legislative proposals on how to regulate encryption, the research findings and analysis, particularly those involving principles and values, can be productively used to inform and guide the development and improvement of laws and policies that affect encryption in New Zealand and possibly other jurisdictions as well. These normative insights and general policy recommendations are set out below.

5.1 Encryption is integral to information security

Any existing or proposed law or policy that impacts encryption should recognise that information security is the central focus of encryption. Information security is the primary goal of encryption because, from its very definition, encryption aims to protect the confidentiality, integrity and authenticity of data. Furthermore, encryption is essential for cybersecurity. The security of data, computers and information systems would be difficult to guarantee without encryption.

In light of the importance of encryption to information security, the development and use of encryption should be encouraged. This is so because safeguarding information

security is an important responsibility of both public and private actors. For example, it is the legal duty of many businesses and providers to protect the privacy and data of their customers and users under data protection or other relevant laws. The widespread use, implementation and development of encryption, including the use of encryption by default, should be actively promoted since these are necessary for protecting computers and data from misuse or improper disclosure. Information security underpins the protection of a whole host of property, privacy and other rights of individuals and entities.

Corollary to this, laws and policies on encryption that undermine or weaken information security (whether intentionally or as an unintended effect) should be avoided. As a matter of policy, businesses and providers should be able to spend their time and resources improving the security of their products and services rather than weaken them. This recommendation is borne out by the very nature of encryption. As discussed in Part 2, from a technical standpoint, encryption is geared towards the protection and preservation of information security. As a theoretical and practical matter, encryption should provide the appropriate level of security and be resistant to attacks. Since information security is considered an ongoing and evolving process, the continued development and improvement of encryption and other aspects of information security should be supported. The need for constant security improvement is all part of the adversarial nature of encryption. Since new ways are always being found or developed to break encryption or to breach cybersecurity, it is imperative to continually strengthen and improve security of computers and data. Because of the inherent difficulties of keeping data and information system secure, laws and policies should not inhibit or dissuade developers and providers from enhancing the security of their products and service especially if they are subject to a legal duty to protect the privacy and security of their users.

This recommendation is supported by the *Apple v FBI* case. It should be recalled that the FBI was able to access the shooter's iPhone with the help of a third-party vendor. Further, after an internal investigation, the US Department of Justice came to the conclusion that the FBI should have first tried to find and exhaust all technical means available to them before seeking to legally compel a company like Apple to render

technical assistance.[1] It is also notable that a company has been selling a device called GrayKey to law enforcement that allows the latter to access any locked iPhone.[2] These technical developments show that encryption and information security systems are not foolproof and technical workarounds are possible and are always being developed. The continuous improvement and testing of the security of information systems and devices is a necessary part of information security.

Business stakeholders should also be able to raise or claim information security as a reasonable excuse or defence in relation to the exercise of the law enforcement powers and measures discussed in Part 3. As a general rule, any request or order to providers for assistance as part of a criminal investigation that negatively impacts the information security of their products and services may be deemed unreasonable and unnecessary under the circumstances. For instance, it would not be reasonable to require providers to modify their products and services if this would result in compromising the latter's information security. Further, any requests for assistance must be within the existing technical capabilities of the provider. Using encryption to protect information security is a legitimate and common use of this technology and should not be restricted, impaired or interfered with in any significant or substantial way.

It would similarly be deemed unreasonable to require businesses and providers to provide their encryption keys as part of a criminal investigation. As mentioned in Part 2 on the primacy of encryption keys, the security of encryption fundamentally depends on who controls or has access to the keys. The secrecy and inviolability of encryption keys is a crucial part of the integrity of encryption and the data and information systems that it protects. Therefore, the use of the power to compel disclosure of access information like encryption keys from providers should be used sparingly and judiciously. The production or disclosure of encryption keys should not be required if it undermines the integrity of a product or service or substantively affects and places at risk the security and privacy of other users or members of the general public who are not the subject of the investigation.

It is worth pointing out that the protection of other principles and values of encryption depend on information security. Privacy and data protection cannot be

[1] See US Department of Justice, Office of the Inspector General, "A Special Inquiry Regarding the Accuracy of FBI Statements Concerning its Capabilities to Exploit an iPhone Seized During the San Bernardino Terror Attack Investigation".
[2] Matt Burgess, "UK police are buying top secret hacking tech to break into iPhones" Wired <https://www.wired.co.uk/article/police-iphone-hacking-grayshift-graykey-uk> accessed 2 July 2019.

ensured effectively in an online or digital environment without encryption. Secrecy of correspondence of electronic communications relies on encryption. In certain respects, protecting national security and public safety is reliant on the security of critical information infrastructures and government-held data from external threats. Information security is indeed a central principle and value that should be considered in any law and policy discussion about encryption.

5.2 Encryption is necessary to protect privacy and data protection

Privacy and data protection are important principles and values for people living in a networked information society. Since many aspects of people's lives involve or are carried out through online or digital means, vast amounts of data are produced, stored, collected and processed about them. It is no wonder then that the focus group participants from all three groups of stakeholders (the general public, businesses and government) are very concerned about issues surrounding privacy and data protection and consider them of utmost importance. As mentioned in Part 4, many of the discussions in the focus group interviews gravitated toward and revolved around people's privacy concerns and how encryption can be used to address them.

For many stakeholders, encryption naturally involves privacy and data protection because, practically speaking, encryption offers the most reasonable and effective means for people to control or preserve their information privacy. Encryption helps ensure the confidentiality and integrity of information and the secrecy of communications. In today's connected world, it would be very difficult to protect privacy and data protection without encryption. This is so because encryption ultimately protects data whether it be at rest (stored data), in motion (communications) or in use (processed data). There is no other technology that is as intrinsically linked to preserving privacy and data protection as encryption.

Given the indispensability of encryption to privacy and data protection, individuals and entities should have the freedom to develop and use encryption. Moreover, encryption technologies should be widely available and used by default. Encryption is an essential element of privacy by design. Any laws and policies that seek to curb the development and use of encryption or limit the choice or availability of encryption technologies should not be pursued. For instance, a ban on the use of

encryption by the general public will not only be infeasible but it would effectively deny them of their right to protect their privacy and personal data. As mentioned in Part 3, the use of encryption inescapably involves a person's reasonable expectation of privacy. As such, any direct or indirect interference with the principles and values of privacy and data protection must be based on lawful grounds and must comply with the general standard of reasonableness.

5.3 Encryption involves law enforcement and public order values and concerns

Despite the seemingly strong emphasis on protecting individual rights and interests such as information security, privacy and data protection, essential public interest and public order concerns must also be taken into account in relation to encryption. As stated in Part 4, human rights and freedoms must be balanced and reconciled with public order values such as national security and public safety and law enforcement and lawful access. The right or ability to develop, access and use encryption is not absolute and is subject to reasonable control under the law.

What is notable though is that, based on the examination of the laws of encryption in Part 3, there are existing laws and rules in place in New Zealand that embody and effectuate these public interest concerns in relation to encryption. The country has export control and cybercrime laws that regulate the export and development of encryption technologies. More importantly, with regard to law enforcement and public order values, public actors have specific powers and measures that they can use to deal with the technical and practical challenges raised by encryption. In relation to potential difficulties with regard to the search, seizure and surveillance of encrypted data and devices, law enforcement officers have powers and authorities under the Search and Surveillance Act to, among others: gain access to protected computers and encrypted data through technical means; require reasonable assistance from persons to gain access to the subject data or computer; compel reasonable assistance from providers to intercept encrypted communications and provide traffic data; and demand the disclosure of access information to encrypted systems and data including passwords and encryption keys. These powers and measures can be effectively utilised to gain access to encrypted data, communications and systems as part of a criminal investigation or law enforcement

action. There is also room for these investigatory powers to be updated and expanded by authorising a data surveillance power and law enforcement hacking subject to specific requirements and conditions.

While the adequacy or reasonableness of these existing investigatory powers and measures remain open to debate (see the discussion in the immediately succeeding section), the existence and availability of such powers demonstrate that encryption is already subject to legal control and regulation. Moreover, considerations of law enforcement and public order values are sufficiently ingrained in the law. For example, the grant of power to law enforcement officers under the Search and Surveillance Act to require the disclosure of access information is a clear attempt by the state to uphold the principle and value of law enforcement and lawful access in light of technological developments including the greater use of encryption. As the law currently stands, it endeavours to strike a balance between the competing concerns of human rights and freedoms versus law enforcement and public order values.[3] Even though the balance between these conflicting private and public interests can still be adjusted and improved, it is noteworthy that the laws that apply to encryption recognise the importance of these public order concerns.

Since encryption is subject to these existing laws and powers, the question then is less about whether encryption can be regulated (because it already is), but how can these powers and measures that apply to encryption be improved to better balance human rights and freedoms vis-à-vis law enforcement and public order values. A critical but often neglected area is the essential role that the right against unreasonable search and seizure and the right against self-incrimination play in maintaining this balance.

5.4 The right against unreasonable search and seizure and the right against self-incrimination are critical to encryption

Based on the analysis in Part 3, it is evident that the right against unreasonable search and seizure and the right against self-incrimination represent the crux of the protection of human rights and freedoms with regard to access to and use of encryption. Given the many investigatory powers and measures available to law enforcement officers,

[3] See New Zealand's Cyber Security Strategy 2019 15.

these two rights represent the final or ultimate line of protection or defence against potential abuse or unreasonable outcomes. The right against unreasonable search and seizure is particularly relevant to the issue of reasonable assistance, while the right against self-incrimination is impacted by the forced disclosure of access information.

From both a social and a legal perspective, these two principles and values need to be recognised and emphasised more and should be top of mind for all stakeholders. As mentioned in Part 4, quite surprisingly, the focus group participants on the whole gave a low priority to the principles and values involving crime and criminal investigations. However, these lowly ranked rights such as the right against unreasonable search and seizure and right against self-incrimination provide some of the strongest legal sources and bases for the protection of their human rights and freedoms. There should be greater awareness then of the criticality of these rights to the issues surrounding encryption. People need to realise that the laws that regulate and impact encryption the most are those that concern criminal investigations and law enforcement. The Search and Surveillance Act may not be explicitly called an encryption law but it is the law that has the most impact on how encryption is developed and used. It should be remembered that law enforcement powers and rules do not apply to criminals alone but to everyone. This means that everyone should be concerned about how their rights are protected and balanced under these laws and rules.

With regard to the right against unreasonable search and seizure, the law seems to have struck a reasonable balance. While there is still room for improvement, on a fundamental level, the general rules on searches, seizures and surveillance under the Search and Surveillance Act in relation to the NZBORA are adequate, fair and just. For instance, the general warrant requirement to conduct a search or surveillance recognises and properly balances personal freedoms and public interest concerns. However, the requirement of reasonable assistance on the part of suspects and third parties demands further attention and consideration. As explained in Part 3, the meaning and extent of reasonable assistance need to be further clarified and specifically delineated in statute, regulatory policy or case law. The ambiguity or lack of clarity of what reasonable assistance entails tends to cause much confusion and can lead to unfair or unjust results whether for private or public actors. If the duty of reasonable assistance is demanded without sufficient restraint or controls, businesses may end up undermining the

information security of their products and services or could go out of business as seen in the case of the encrypted email service Lavabit.[4] On the other hand, if law enforcement officers use the power to compel reasonable assistance too broadly or aggressively, any evidence that was collected might be deemed inadmissible if a court subsequently rules that such assistance that was required of a third party or suspect was not reasonable, proper or appropriate under the circumstances. Greater clarity of what reasonable assistance means can benefit all stakeholders whether they are users, developers or regulators of encryption.

The right against self-incrimination is also crucial to encryption. Since encryption relies on the secrecy and inviolability of encryption keys and passwords, a fairer balance needs to be struck between the right or privilege against self-incrimination and the power of law enforcement officers to compel the disclosure of access information. As the law currently stands, the protection of the right against self-incrimination is not as strong as it could or should be. While the Search and Surveillance Act states that the privilege against self-incrimination is available in computer system searches, vague and abstruse wording of the law has rendered the protection and exercise of such right weak or ineffective.[5] Furthermore, as discussed in Part 3, limiting the right against self-incrimination to the compelled disclosure of passwords that are in themselves incriminating (e.g., the password must be "I shot the sheriff" to be inculpatory) is severely restrictive and would render the right nugatory. Given their testimonial quality and the essentiality of passwords and keys to the confidentiality and integrity of encryption, the protection of the right against self-incrimination should be made more robust. As a general rule, persons who are suspected and charged with a crime should be able to claim the right against self-incrimination and they should not be penalised for exercising their right. This is in accord with the basic principles of justice and fairness.[6]

The right against self-incrimination and the forced disclosure of passwords is admittedly a complex topic that demands further research and study. Other jurisdictions

[4] 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.
[5] See Search and Surveillance Act 2012, s 130.
[6] See New Zealand Bill of Rights Act 1990, ss 25 and 27.

are also trying to clarify and make sense of this issue.[7] As a matter of law and policy, this is an area that demands more consideration and analysis. It is outside the scope of this study to make specific recommendations on this subject. Nevertheless, a recognition of the primacy of these rights in relation to encryption is an essential starting point to any debate or discussion.

5.5 Encryption requires balancing and reconciling competing principles, values and interests

Encryption is a complex technology that embodies conflicting principles, values and interests. There are always at least two opposing sides to any issue or matter raised by encryption. This dialectic quality of encryption is evident in the various aspects of encryption discussed in the previous parts of this report. Encryption involves both cryptography and cryptanalysis, that is, the creation as well as breaking of cryptographic schemes. From a technical standpoint, encryption has been rightfully characterised as being adversarial in nature and involves a race between those who want to make it more secure and those who intend to break and circumvent it. Further, it is considered a dual-use good that can be utilised for both military and non-military purposes. As explained in Part 4, even the principles and values of encryption can be organised into the two seemingly opposing categories: human rights and freedoms versus law enforcement and public order values. With regard to encryption, there is a perennial conflict between private rights and public interests. Also, as a practical matter, encryption can be equally used for legitimate and illicit purposes (e.g., as a crucial means to protect privacy or to problematically conceal the commission or evidence of a crime). It is this dual character of encryption that makes this technology and the problems that it raises harder to address from the perspective of law and policy.

Despite the naturally contradictory nature of encryption and the difficulties that it engenders, balancing and reconciling these conflicts is conceptually possible. As this study has shown, a principles- and values-based approach is a useful starting point for finding solutions to address the encryption dilemma because it makes clear what these principles

[7] See Bert-Jaap Koops, "Commanding decryption and the privilege against self-incrimination" in CM Breur and others (eds) *New trends in criminal investigation and evidence Volume II* (Intersentia 2001); see Orin Kerr, "Compelled Decryption and the Privilege Against Self-incrimination".

and values are and how they relate to each other. One cannot reasonably balance these competing principles and values if one does not fully understand them first. Examining the different principles and values of encryption and their interactions can therefore reveal *both conflicts as well as correspondences* between them. It is worth noting that such areas of conflict can also become points of connection. It is these correspondences that can be potentially developed or pursued in order to find the right balance between such apparently opposing principles, values and interests. For instance, the principle and value of information security is often set against national security and public safety. But information security can protect national security and public safety when it comes to protecting the integrity of public or government information systems. Finding these correspondences is only possible when one has an adequate conceptual understanding and empirical grounding of these principles and values and what they actually mean and entail for the relevant stakeholders. As seen in Part 4, various stakeholders have differing notions and reactions to these principles and values and such differences need to be taken into consideration when seeking to find that optimal balance. Having conceptual clarity and a strong empirical foundation about the principles and values of encryption are necessary in order to properly reconcile the attendant competing interests and concerns. And this greater conceptual and empirical understanding is only possible when one more fully and intently examines the technical, legal, social and other dimensions of encryption.

5.6 Encryption fundamentally relies on trust

As explained in Part 4, trust is a paramount principle and value of encryption. It cuts across and belongs to both categories of encryption principles and values (i.e., human rights and freedoms and law enforcement and public order concerns). Further, it plays an indispensable role in interceding between the other principles and values. Trust's mediating function is highly relevant to the matter of balancing and reconciling the competing interests and concerns surrounding encryption. It may be said that the act of balancing and reconciling these encryption principles and values is primarily about maintaining or building trust either in the technology of encryption itself or between and among the relevant stakeholders involved. In this way, trust also serves as an essential standard or criterion for evaluating whether a balance can be or has been struck among the competing private and public issues and concerns. For example, if the principle and

value of information security is diminished or sacrificed in the name of national security and public safety (e.g., requirement of mandatory backdoors in encryption), then such a regulatory approach may be objected to on the ground that people would neither trust nor consequently use encryption that did not provide an adequate level of information security because it had a built-in weakness. If the right against self-incrimination is deprecated in order to grant greater powers for law enforcement and lawful access (e.g., forced disclosure of passwords from suspects or persons charged in all possible contexts and situations), this may result in less trust or greater distrust of government. In these two examples, the existence or level of trust acts a test or guide for determining whether an appropriate balance can or has been attained. Simply put, if trust is negatively affected or substantially impaired, then the proposed regulatory action or approach to encryption should be reconsidered, improved or set aside.

Because of its fundamental importance to encryption, the maintenance and building of trust should be a principal focus when developing or proposing laws and policies on encryption.[8] As Regulator B says, "It is a balance of trust".[9] Regulator B continues, "So, I think it is important, how do we continue to grow a trust model that the community and society can buy into".[10] So there must first be trust in the technology of encryption. Encryption will not be trusted if it is considered unsafe or insecure. This is the main reason why mandatory backdoors in encryption have been vehemently opposed by users and providers alike because they do not engender trust in the technology, the government, or whoever has potential access to it. User H states, "Do you trust the government with the backdoor? Do you also trust them that if there is a backdoor to keep it secret? To keep it safe? What if that backdoor then goes into somebody else's hands?".[11] Provider G further argues that the presence of backdoors

> just undermined the trust argument…. If you say that somebody – oh, it might be a government person – might have a backdoor to the key, then people won't trust it. And, governments, intelligence agencies included, have shown how irresponsible they've been with some pretty sensitive data. So, if they can't protect their own data, why should we trust them with ours?[12]

Regulator B likewise contends that, with backdoors, it's

[8] See New Zealand's Cyber Security Strategy 2019 8 (trust is one of the guiding principles).
[9] Focus group interview with Regulator B.
[10] Focus group interview with Regulator B.
[11] Focus group interview with User H.
[12] Focus group interview with Provider G.

> when you start losing control, because then, how many backdoors have you built? Who has access to the backdoors? Well, when I sold this company and the property, now the government takes over, have I divulged all the backdoors? Or what happened to those staff members that built the backdoors?[13]

Aside from trusting the technology itself, there must also be trust in the providers of the encrypted products and services and government actors that seek to regulate or control such encryption technologies. Regulator E notes that while it is one thing to "say I trust… this technology. The broader stroke being I trust society and institutions".[14] The problem with trust and the development of law and policy is that one cannot directly legislate trust. Trust can be the outcome or end result of what are considered legitimate laws and policies but trust cannot be produced by law per se. Regulator B remarks, "So, I think that from a technology side that we have got a significant challenge, but there's a society decision that they've got to take at some point as 'What is good enough? What is enough trust?' versus 'What is legislated trust?' Because, can you legislate trust?"[15] Regular E concurs, "You cannot legislate trust. And that is a very fundamental concept in encryption and in information systems security".[16]

Businesses and government actors must therefore earn or maintain that trust. This trust is constructed and perpetuated through the continuous interactions and relationships among the stakeholders concerned: users, providers and regulators. Trust can be earned and lost or it can be strengthened or diminished depending on the actions, perceptions and relations of the persons involved. For instance, integrity is an important issue when it comes to trust. Provider L explains, "Well, it comes down to the integrity…. That's a word I like, because it's the integrity of the government not to abuse and the wider national security and public safety. If they go about their business or they access data, they [have to] do it with integrity".[17] There is also the matter of accountability. User J explains how accountability can improve trust in government:

> political accountability, that's another way – any abusiveness, not just political accountability, but due process. So, you want to know that not only if they do an unreasonable search and seizure, that they'll say, 'Oh, you shouldn't do that again'. You want to know that someone's going down for

[13] Focus group interview with Regulator B.
[14] Focus group interview with Regulator R.
[15] Focus group interview with Regulator B.
[16] Focus group interview with Regulator E.
[17] Focus group interview with Provider L.

> that at whatever level of the power hierarchy. And if you don't have that accountability, all you have [are] promises. Broken promises. And you're [not] going to trust in your encryption, have no trust in the state, and it's all useless.[18]

If there are transparent, just and equitable systems or processes in place that ensure integrity and accountability, these can help boost trust.

Trust is inherently connected to the matter of balancing of interests. User Q opines, "I think we're better framed to look at it from… [the perspective of] power balance".[19] Regulator H similarly believes, "I think we need to keep managing that balance".[20] Finding that balance can be hard as Regulator E notes, "So, there's that balance that has to be found, and I don't know the way it is, but it's a horrendously difficult issue. I guess there's checks and balances".[21] User P gives an example, "it should be a balance… the power [of the government] should be balanced. So, the state might have a right to request. You've got a right to due process to deny that request".[22]

Encryption is undeniably founded and built on trust. It is imperative then that any existing or proposed laws and policies on encryption should be assessed through the lens of trust. Does the power or measure strengthen, maintain or weaken trust in encryption and between the relevant parties? Mechanisms, procedures and approaches that help maintain or build trust in encryption should be explored, examined or adopted. Trust is a core consideration that must be taken into account when developing or implementing encryption laws and regulations.

5.7 A principles- and values-based framework for encryption

The principles- and values-based approach developed and used in this study can help provide guidance and direction to the development of encryption laws and policies in New Zealand and also other jurisdictions. It can serve as an overarching framework for assessing the validity, legitimacy or utility of existing or proposed laws, powers and measures concerning encryption. For instance, faced with the problems posed by encryption to national security and law enforcement (e.g., a suspect has an encrypted

[18] Focus group interview with User J.
[19] Focus group interview with User Q.
[20] Focus group interview with Regulator H.
[21] Focus group interview with Regulator E.
[22] Focus group interview with User P.

device), the knee-jerk reaction of some government actors is to consider banning or prohibiting the use of encryption altogether. Using the principles- and values-based framework, it is evident that such an action or proposition would be untenable. For one, a prohibition on either the development or use of encryption would go against the principal role of encryption, which is to provide information security. Bans on encryption would also have negative effects on the principles and values of privacy, data protection, secrecy of correspondence, and trust. As mentioned many times in this report, the security and safety of computers, data and information systems rely on encryption. Encryption is essential for the efficient and effective workings of an information-driven and technologically-mediated world. The information society and the digital economy cannot function properly without encryption.

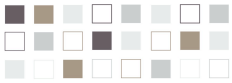
Mandatory backdoors are another common legislative proposal to encryption. Viewed from the perspective of principles and values, while the requirement of mandatory backdoors in encryption could make the protection of national security and public safety and law enforcement and lawful access easier for government actors, it would clash with the principles and values of information security and trust. Backdoors would make encryption inherently insecure. Furthermore, encryption with a backdoor would be untrustworthy and most persons would not use it. Forced backdoors in encryption would also impact the privacy and data protection of users and infringe on the freedom of businesses and developers to innovate and improve their products and services. Mandatory backdoors and other legislative attempts to weaken encryption are clearly problematic.

There is also the proposed system of mandatory key escrow where the encryption keys of all persons are kept by a designated private or public entity and are only disclosed to law enforcement when required (e.g., pursuant to a warrant). The main problem with key escrow is trust. It would be very hard to find a person, entity or institution that all stakeholders trust with their encryption keys. There are also some stakeholders who believe the best and most secure approach to encryption and key management is to "trust no one" with one's keys or that providers should have zero-knowledge of users' keys. Further, having a central entity that holds everyone's encryption keys creates risks that could have a significant and wide-ranging impact on the information security, privacy,

and data protection of users and businesses in case that central entity is subject to a cyberattack or a security breach.

As discussed in Part 3, the power to demand decryption already exists in New Zealand. Under the Search and Surveillance Act, specific persons may be required to disclose access information such as passwords and encryption keys and provide reasonable assistance to law enforcement as part of an investigation. While such powers are useful to uphold law enforcement and lawful access and national security and public safety, it comes into conflict with the right against unreasonable search and seizure and the right against self-incrimination. This is a complex matter and more work has to be done to find the right balance in the law as it is currently written between these two opposing sides. One proposal that has not been widely discussed or considered in New Zealand is the grant of expanded investigatory powers to law enforcement including the ability to break or circumvent encryption through technical means. Such a power seems to be implicitly included in the powers of law enforcement in conducting a search and seizure. Granting or confirming the availability of such an investigatory power to law enforcement would avoid the human rights concerns surrounding the forced disclosure of passwords from suspects since law enforcement officers could break the encrypted data or device on their own. Of course, this would be subject to the continued protection of substantive rights and adherence to procedural rules as provided in the law. This so-called power of "law enforcement hacking" is also in line with adversarial nature of encryption whereby those who seek to gain access to encrypted data (e.g., law enforcement officers) should take it upon themselves to continuously improve their ability and expand the available tools that enable them to gain access to encrypted data and communications. As explained in Part 2, most encryption is not unbreakable and technical solutions are available or can be developed to circumvent encryption itself or exploit the security vulnerabilities of the computers and devices on which such encryption is used. It is true that this approach may require more time and effort for government actors, but in an increasingly digital and connected world, these forms of technical techniques and measures are an inherent part of law enforcement and criminal investigations. Law enforcement officers need to keep up-to-date and stay ahead of the technical advances needed to effectively investigate and prosecute crimes in the digital age.

The above conclusions and recommendations of this study are meant to inform or guide the development and direction of encryption laws and policies in New Zealand. The resolution of the encryption dilemma and its consequent problems will require much more research, analysis, public deliberation, democratic debate, consensus building, and ultimately difficult law and policy decisions on the part of all stakeholders concerned. Whatever laws, regulations and rules on encryption that the country finally decides to enact, the key is to recognise and understand the fundamental principles and values of encryption that are at play and strive to resolve or reconcile these conflicts by finding connections or correspondences between them, especially with regard to maintaining or building trust. It is only then that a workable balance between the competing principles, values and interests concerning encryption can eventually be achieved.



Bibliography

Adams on Criminal Law (Thomson Reuters 2019)

Amies R and Woollaston G, *Electronic Business and Technology Law (NZ)* (LexisNexis NZ Limited 2019)

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

Associated Press, "Australia plans law to force tech giants to decrypt messages" <https://apnews.com/621e0913072a4cb5a1a7f7338721b059/Australia-plans-law-to-force-tech-giants-to-decrypt-messages> accessed 15 July 2017

Baldwin DA, "The concept of security" (1997) 23 Review of International Studies 5

Barrett B, "The Apple-FBI Battle is Over, But the New Crypto Wars Has Just Begun" Wired <https://www.wired.com/2016/03/apple-fbi-battle-crypto-wars-just-begun/> accessed 13 July 2017

Blomqvist K, "The Many Faces of Trust" (1997) 13 Scandinavian Journal of Management 271

Brown J, "NotPetya's impact on NZ firms" <http://www.newshub.co.nz/home/new-zealand/2017/06/notpetya-s-impact-on-nz-firms.html> accessed 13 July 2017

Bryman A, *Social Research Methods* (Oxford University Press 2012)

Burgess M, "UK police are buying top secret hacking tech to break into iPhones" Wired <https://www.wired.co.uk/article/police-iphone-hacking-grayshift-graykey-uk> accessed 2 July 2019

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

Canadian Department of Justice, "Summary of Submissions to the Lawful Access Consultation" <https://www.justice.gc.ca/eng/cons/la-al/sum-res/faq.html> accessed 23 August 2019

Canetti R and others, "Deniable encryption" in *Annual International Cryptology Conference* (Springer 1997)

Charmaz K, *Constructing Grounded Theory: A Practical Guide Through Qualitative Analysis* (SAGE Publications 2006)

Cherdantseva Y and Hilton J, "A reference model of information assurance & security" in *Availability, Reliability and Security (ARES) Conference* (IEEE 2013)

CNBC, "End-to-end encryption on messaging services is unacceptable: UK minister" <http://www.cnbc.com/2017/03/26/london-attack-whatsapp-encrypted-messaging-apps-khalid-masood.html> accessed 13 July 2017

Council of Europe, Explanatory Report to the Convention on Cybercrime

Cullen M and Reddy P, "Intelligence and Security in a Free Society: Report of the first Independent Review of Intelligence and Security in New Zealand" (Independent Review of Intelligence and Security, 29 February 2016).

Delfs H and Knebl H, *Introduction to Cryptography: Principles and Applications* (Springer 2015)

Department of the Prime Minister and Cabinet, "Defining National Security" <https://dpmc.govt.nz/our-programmes/national-security-and-intelligence/intelligence-and-security-act-2017/defining-national-security> accessed 6 November 2018

Dizon MAC, *A Socio-Legal Study of Hacking: Breaking and Remaking Law and Technology* (Routledge 2018)

Dutch Cabinet Position on Encryption <https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2016Z00009&did=2016D00015> accessed 13 July 2017

Dwork C and Naor M, "Pricing via processing or combatting junk mail" in *Annual International Cryptology Conference* (Springer 1992)

Free Software Foundation, "What is free software?" <https://www.gnu.org/philosophy/free-sw.en.html> accessed 9 August 2018

Friese S, *Qualitative Data Analysis with ATLAS.ti* (SAGE Publications 2014)

Funnell J, "E-Devices: Supplementary Briefing for Foreign Affairs, Defence and Trade Committee" (New Zealand Customs Service, 21 February 2017)

Funnell J, "Response to Select Committee Questions raised on 13 March 2017" (New Zealand Customs Service, 15 March 2017)

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

Gentry C, "A fully homomorphic encryption scheme" (PhD thesis, Stanford University 2009)

Gibbons LJ, "No Regulation, Government Regulation, or Self-regulation: Social Enforcement or Social Contracting for Governance in Cyberspace" (1997) 6 Cornell Journal of Law and Public Policy 475

Goldreich O, *Foundations of Cryptography: Volume 2 Basic Applications* (Cambridge University Press 2009)

Goldsmith J, "Regulation of the Internet: Three Persistent Fallacies" (1998) 73 Chicago-Kent Law Review 1119

Goldsmith J and Wu T, *Who Controls the Internet?: Illusions of a Borderless World* (Oxford University Press 2006)

Government Communication Security Bureau, "17. Cryptography" in *NZISM New Zealand Information Security Manual – Part 2* (Government Communication Security Bureau 2017)

Greenberg A, "Whatsapp just switched on end-to-end encryption for hundreds of millions of users" Wired <https://www.wired.com/2014/11/ whatsapp-encrypted-messaging/> accessed 26 July 2018

Hack M, "The implications of Apple's battle with the FBI" (2016) Network Security 8

Hitlin S and Piliavin J, "Values: Reviving a Dormant Concept" (2004) 30 Annual Review of Sociology 359

Hoepman JH and Jacobs B, "Increased security through open source" <https://arxiv.org/abs/0801.3924> accessed 23 August 2019

IICS WG, "Interagency report on status of international cybersecurity standardization for the internet of things (IoT)" in *NIST Interagency Report 2018*.

InternetNZ, "Encryption: ways forward that protect the Internet's potential"

InternetNZ, "83 organisations send strong message to Five Eyes" <https://internetnz.nz/news/83-organisations-send-strong-message-five-eyes> accessed 13 July 2017

Johnson D and Post D, "Law and Borders: The Rise of the Law in Cyberspace" (1996) 48 Stanford Law Review 1367

Kamp PH and others, "Linkedin password leak: Salt their hide" (2012) 10 ACM Queue 20

Kerckhoffs A, "La cryptographic militaire" (1883) 9 Journal des sciences militaires 5

Kerr OS, "Compelled Decryption and the Privilege Against Self-incrimination" (2018-2019) 97 Texas Law Review 767

Kimball D, "The Wassenaar Arrangement at a Glance" <https://www.armscontrol.org/factsheets/wassenaar > accessed 22 August 2019

Khare R and Rifkin A, "Weaving a web of trust" (1997) 2 World Wide Web Journal 77

Kluckholm C and others, "Values and Value-Orientations in the Theory of Action" in T Parsons and EA Shils (eds), *Toward a General Theory of Action* (Harper Torchbooks 1951)

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

Koops BJ, "Commanding decryption and the privilege against self-incrimination" in CM Breur and others (eds) *New trends in criminal investigation and evidence Volume II* (Intersentia 2001)

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

Krueger RA and Casey MA, *Focus Groups: A Practical Guide for Applied Research* (SAGE Publications 2009)

Law Commission, *The Privilege Against Self-Incrimination* (NZLC PP25, 1996)

Law Commission, *Review of the Privacy Act 1993. Review of the Law of Privacy Stage 4* (NZLC IP17, 2010)

Law Commission, *Review of the Search and Surveillance Act 2012* (NZLC IP40, 2016)

Law Commission, *Review of the Search and Surveillance Act 2012* (NZLC R141, 2017)

Law Commission, *Search and Surveillance Powers* (NZLC R97, 2007)

Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books 1999)

Lawrence Lessig, *Code: version 2.0* (Basic Books 2006)

Legislation Design Advisory Committee, "Legislation Guidelines" (2018 Edition)

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

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

Lewis JD and Weigert A, "Trust as a Social Reality" (1985) 63 Social Forces 967

Lysyanskaya A, "Signature schemes and applications to cryptographic protocol design" (PhD thesis, Massachusetts Institute of Technology 2002)

McCullagh A and Caelli W, "Non-repudiation in the digital environment" (2000) 5 First Monday

Menezes AJ, van Oorschot PC and Vanstone SA, *Handbook of Applied Cryptography* (CRC Press 1996)

Ministry of Foreign Affairs and Trade, "New Zealand Strategic Goods List" (October 2017)

Ministry of Foreign Affairs and Trade, "Trading weapons and controlled chemicals: Which goods are controlled?" <mfat.govt.nz>

Ministry of Health, "HISO 10064:2017 Health Information Governance Guidelines" (August 2017)

Nakamoto S, "Bitcoin: A peer-to-peer electronic cash system" (2008)

New Zealand Customs Service, "Customs and Excise Act 1996 Review: Discussion Paper 2015" (March 2015)

New Zealand Customs Service, "Customs and Excise Act 1996. Summary of Submissions" (March 2016)

New Zealand Parliament, "Customs and Excise Bill – First Reading" (6 December 2016) 7719 NZPD 15546

New Zealand Police Annual Reports 2011/2012 to 2016/2017

New Zealand Government, "Information privacy principles. Descriptions and examples of breaches of the IPPs"

New Zealand's Cyber Security Strategy 2015

New Zealand's Cyber Security Strategy 2015 Action Plan

New Zealand's Cyber Security Strategy 2019

Oechslin P, "Making a faster cryptanalytic time-memory trade-off" in *Annual International Cryptology Conference* (Springer 2003)

Office of the Privacy Commissioner, "Privacy law reform resources" <https://www.privacy.org.nz/the-privacy-act-and-codes/privacy-law-reform-resources/> accessed 13 July 2017

Organisation for Economic Co-operation and Development, "Cryptography Policy: The Guidelines and the Issues" (1998)

Organisation for Economic Co-operation and Development, "Recommendation of the Council Concerning Guidelines for Cryptography Policy" (1997)

Organisation for Economic Co-operation and Development, "Report on Background and Issues of Cryptography Policy".

Oxford Dictionary, "Encryption" <https://en.oxforddictionaries.com/definition/encryption> accessed 25 July 2018

Oxford Dictionary, "Private" <https://en.oxforddictionaries.com/definition/private> accessed 7 August 2018

Oxford Dictionary, "Secret" <https://en.oxforddictionaries.com/definition/secret> accessed 7 August 2018

Oxford Dictionary of English, "Trust"

Penk S, "The Privacy Act 1993" in S Penk and R Tobin (eds), *Privacy Law in New Zealand* (Thomson Reuters 2016)

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

Perlroth N, Larson J and Shane S, "NSA able to foil basic safeguards of privacy on web" New York Times <https://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html> accessed 23 August 2019

Post R, "Encryption Source Code and the First Amendment" (2000) 15 Berkeley Technology Law Journal 713

Privacy Commissioner, "Codes of Practise" <https://www.privacy.org.nz/the-privacy-act-and-codes/codes-of-practice/> accessed 23 August 2019

Privacy Commissioner "Guidance Note on Codes of Practice under Part VI of the Privacy Act <https://www.privacy.org.nz/news-and-publications/guidance-resources/guidance-note-on-codes-of-practice-under-part-vi-of-the-privacy-act/> accessed 23 August 2019

Privacy Commissioner, "Privacy 101: An Introduction to the Privacy Act. Facilitation Guide" (December 2015) <privacy.org.nz>

Privacy Commissioner, "Privacy 101: An Introduction to the Privacy act. Participant Guide" (December 2015) <privacy.org.nz>

Privacy Commissioner, "Privacy Commissioner requires data encryption" (21 February 2008) <privacy.org.nz>

Privacy Commissioner, "Privacy on the line: A resource document in relation to Privacy in Telecommunications" (June 2010) <www.privacy.org.nz>

Privacy Commissioner, "What do you have to do to keep information secure?" <privacy.org.nz>

Protective Security Requirements, "Information Security Management Protocol" <https://www.protectivesecurity.govt.nz/home/information-security-management-protocol/information-security-management-protocol/#operational-security-management>

Protective Security Requirements, "What You Need To Know" <protectivesecurity.govt.nz>

Radio New Zealand, "NZ computers caught up in global cyberattack" <http://www.radionz.co.nz/news/world/330677/nz-computers-caught-up-in-global-cyberattack> accessed 13 July 2017

Radio New Zealand, "Calls for strong encryption in 'Five Eyes' countries" <http://www.radionz.co.nz/news/national/334256/calls-for-strong-encryption-in-five-eyes-countries> accessed 13 July 2017

Raymond E, *The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary* (O'Reilly Media 2001)

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

Rivest RL, "Foreword" in AJ Menezes, PC van Oorschot and SA Vanstone, *Handbook of Applied Cryptography* (CRC Press 1996)

Rivest R, "The case against regulating encryption technology" Scientific American (October 1998)

Robshaw MJB, "Stream ciphers" in *RSA Laboratories Technical Report* (1995).

Sanguinetti B and others, "Quantum random number generation on a mobile phone" (2014) 4 Physical Review X

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

Schiller J and Crocker S, "Randomness requirements for security" <http://www.hjp.at/(st_a)/doc/rfc/rfc4086.html> accessed 23 August 2019

Schneier B, "More Crypto Wars II" <https://www.schneier.com/blog/archives/2014/10/more_crypto_war.html> accessed 13 July 2017

Security For All, <https://www.securetheinternet.org/> accessed 13 July 2017

Severson D, "The Encryption Debate in Europe" Hoover Institution Aegis Paper Series No. 1702 (2017)

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

Stilgherrian, "Encrypting data at rest is vital, but it's just not happening" <https://www.zdnet.com/article/encrypting-data-at-rest-is-vital-but-its-just-not-happening/> accessed 17 August 2018

Solove DJ, "Conceptualizing Privacy" (2002) 90 California Law Review 1087

Daniel Solve, "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy" (2007) 44 San Diego Law Review 745

Tien L, "Publishing Software as a Speech Act" (2000) 15 Berkeley Technology Law Journal 629

The Guardian, "New law would force Facebook and Google to give police access to encrypted messages" <https://www.theguardian.com/technology/2017/jul/14/new-law-would-force-facebook-and-google-to-give-police-access-to-encrypted-messages> accessed 15 July 2017

Toor A, "France and Germany want Europe to crack down on encryption" The Verge <https://www.theverge.com/2016/8/24/12621834/france-germany-encryption-terorrism-eu-telegram> accessed 13 July 2017

United Nations Human Rights Council, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression"

US Department of Justice, Office of the Inspector General, "A Special Inquiry Regarding the Accuracy of FBI Statements Concerning its Capabilities to Exploit an iPhone Seized During the San Bernardino Terror Attack Investigation"

Walter M, *Social Research Methods* (Oxford University Press 2013)

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

Wassenaar Arrangement, "Origins" <wassenaar.org>

Wassenaar Arrangement Secretariat "Public Documents, Vol. 1 – Founding Documents" (WA-DOC (17) PUB 001, February 2017)

Weitzner D and others, "Information accountability" (2008) 51 Communications of the ACM 82

Weis S, "Protecting data in-use from firmware and physical attacks" Black Hat 2014

Wolfers A, "'National Security' as an Ambiguous Symbol" (1952) 67 Political Science Quarterly 481

Young W, Trendle N and Mahoney R, *Search and Surveillance: Act and Analysis* (Thomson Reuters 2012)

Treaties, statutes and regulations

Animal Products Act 1999

Animal Welfare Act 1999

Arms Act 1983

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

Convention on Cybercrime

Copyright Act 1994

Corporations (Investigation and Management) Act 1989

Courts Security Act 1999

Crimes Act 1961

Customs and Excise Act 1996

Customs and Excise Act 2018

Customs Export Prohibition Order 2017

EU General Data Protection Regulation

European Convention on Human Rights

Evidence Act 2006

Films, Videos, and Publications Classification Act 1993

Fisheries Act 1996

Government Communications Security Bureau Act 2003

Harmful Digital Communications Act 2015

Immigration Act 2009

Inspector-General of Intelligence and Security Act 1996

Intelligence and Security Act 2017

Intelligence and Security Committee Act 1996

International Covenant on Civil and Political Rights

Misuse of Drugs Act 1975

National Animal Identification and Tracing Act 2012

New Zealand Bill of Rights Act 1990

New Zealand Security Intelligence Act 1969

Policing Act 2008

Privacy Act 1993

Reserve Bank of New Zealand Act 1989

Search and Surveillance Act 2012

Tax Administration Act 1994

Telecommunications Act 2001

Telecommunications (Interception Capability and Security) Act 2013

Terrorism Suppression Act 2002

Trade Marks Act 2002

Wine Act 2003

Cases

Carpenter v United States of America 585 US (2018)

Cooper v Department of Internal Affairs HC Wellington CRI 2008-485-86, 18 September 2008

Department of Internal Affairs v Crockett [2017] NZDC 7422

Dotcom v AG [2014] NZSC 199

Hamed v R [2011] NZSC 101

Henderson v AG [2017] NZHC 606

Houghton v Saunders [2014] NZHC 2229

Privacy Commissioner Case Note 248601 [2013] NZ PrivCmr 4.

Privacy Commissioner Case Note 26781 [2003] NZ PrivCmr 21

Privacy Commissioner Case Note 269784 [2016] NZ PrivCmr 3

R v Alsford [2017] NZSC 42

R v Spark [2008] NZCA 561

R v Darroch [2016] NZDC 11893

R v Director of Serious Fraud Office, ex parte Smith [1993] AC 1 (HL)

S v R [2016] NZCA 448

S v R [2016] NZSC 172

Trans Rail Ltd v Wellington District Court [2002] 3 NZLR 780

W v R [2017] NZCA 522

Wikitera v Ministry for Primary Industries [2018] NZCA 195