Social conceptions versus legal protections of privacy and information security in the context of encryption

Author name and affiliation

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

Postal address:
Te Piringa Faculty of Law
University of Waikato
Private Bag 3105
Hamilton 3240
New Zealand

Email: michael.dizon@waikato.ac.nz
Tel: +64-7-8384466 ext 8590

Abstract

This article examines the disconnect between people's social conceptions of privacy and information security in relation to encryption vis-à-vis the legal protections offered by law. It describes the social conceptions and expectations of participants based in New Zealand and contrasts these with the applicable laws and legal protections concerning privacy, information security and encryption. In light of incongruence between the social and the legal, the article recommends law and policy developments to better align and connect people's social conceptions of privacy and information security with the legal protections provided by law. This includes having greater awareness of the relevance of civil and criminal procedure rights to privacy and information security in the context of encryption and providing stronger legal protections to the right against unreasonable search and seizure and the privilege against self-incrimination.

Keywords

encryption, privacy, information security, data protection, civil rights, criminal procedure

Acknowledgments

This work is based on the ENCRYPT and DECIPHER research project that was supported by the New Zealand Law Foundation under Grant number 2017/ILP/10 and the University of Waikato.

Word count

5,939 without footnotes
6,973 including footnotes

Author bio

Michael Anthony C. Dizon, PhD, is a Senior Lecturer in Law at the University of Waikato, New Zealand. He previously worked as a lawyer and researcher for institutions and organisations in the Netherlands, the United Kingdom and the Philippines. His principal area of research is law and ICT (information and communications technology). He has conducted and published research on law and technology topics such as encryption, hacking, information security, cybercrime, intellectual property, and technology regulation.

Social conceptions versus legal protections of privacy and information security in the context of encryption

Abstract

This article examines the disconnect between people's social conceptions of privacy and information security in relation to encryption vis-à-vis the legal protections offered by law. It describes the social conceptions and expectations of participants based in New Zealand and contrasts these with the applicable laws and legal protections concerning privacy, information security and encryption. In light of incongruence between the social and the legal, the article recommends law and policy developments to better connect people's social conceptions of privacy and information security with the legal protections provided by law. This includes having greater awareness of the relevance of civil and criminal procedure rights to privacy and information security in the context of encryption and providing stronger legal protections to the right against unreasonable search and seizure and the privilege against self-incrimination.

1. Differing conceptions and protections

With the continuing trends of computerisation, digitisation and network connections that characterise life in the network information society, people increasingly recognise the values of privacy and information security. This is especially true in light of the growing data collection and profiling of users by private companies, rising occurrences of large-scale data breaches, and confirmed reports of government mass surveillance programmes. People are rightly concerned about the privacy and security of their data as well as the information and communications technologies they use on a daily basis. Faced with these multiplying cyberthreats and risks, ordinary users and citizens have come to rely on both law and technology for protection, especially encryption as a technical remedy. People believe that their privacy and information security are safeguarded by law and assume that the technologies they regularly use preserve these values. The problem though is that the protection and promotion of privacy and information security whether through law or technology are not straightforward at all as each provides protection in diverse ways. Moreover, there is a seeming disconnect between people's perceptions and expectations of privacy and information security with regard to encryption versus the actual legal protections

offered by law. It appears that people's understanding of how their privacy and information security are protected by law is not sufficiently grounded in legal reality.

The principal aim of this article is to examine the social conceptions of privacy and information security vis-à-vis the legal protections offered by law in relation to the development, access to and use of encryption. Using users, developers and regulators in New Zealand as subjects, this article analyses what their varying conceptions or notions of privacy and information security are in connection with encryption. It then juxtaposes these conceptions with the applicable laws. The article explains why the most significant laws concerning privacy and information security are not the oft-cited data protection laws but those that involve human rights and law enforcement. It is argued that civil and criminal procedure rights involving criminal investigations and proceedings are the most pertinent and germane to the issues of privacy and information security in a digital network environment.

This article proceeds in four parts. Part 2 begins with a definition of encryption and explains why it is essential for preserving privacy and information security. It then describes the social conceptions and expectations of privacy and information security in relation to encryption of participants based in New Zealand.[1] Part 3 discusses the laws that provide legal protection to privacy and information security. In Part 4, the article analyses the legal protections and contrasts these with participants' social conceptions. In light of the comparison between the social and the legal, it recommends law and policy developments that can be undertaken to better align and connect people's social conceptions of privacy and information security with the legal protections provided by law. Part 5 concludes with a brief reflection on the findings.

2. Social conceptions

[1] Empirical data was collected through interviews with 10 focus groups composed of members of the general public, businesses, and government in New Zealand in 2018.

2.1 Importance of encryption

Encryption is a *technology that transforms information or data into ciphers or code for purposes of ensuring its confidentiality, integrity and authenticity*. Encryption preserves confidentiality by making sure the information or content is not revealed or disclosed to unauthorised persons.[2] It protects integrity by guaranteeing that the data is complete and unaltered.[3] With regard to authenticity, encryption warrants that the 'entities are who they claim to be, or that information has not been manipulated by unauthorized parties'.[4] Encryption is able to accomplish these purposes by transforming information through the processes of encoding and decoding with the use of cryptographic algorithms and encryption and decryption keys.[5] The security of encryption and encrypted data primarily relies on the secrecy and inviolability of these keys.[6]

Encryption is a crucial technology in the digital age since it is indispensable for safeguarding the privacy and information security of people and their data, computers and systems.[7] Securely and privately creating, storing, transmitting and processing digital information and personal data would be exceedingly difficult, if not close to impossible, without this technology.[8]

2.2 People's conceptions, perceptions and expectations

The research participants who took part in the focus groups interviews are well aware of the importance of encryption in protecting their privacy and information security. Based

---

[2] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* (CRC Press 1996) 4; see also Bert-Jaap Koops, *The Crypto Controversy: A Key Conflict in the Information Society* (Kluwer Law International 1999) 24.
[3] Bert-Jaap Koops, *The Crypto Controversy* 269; see also Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 4.
[4] Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 24.
[5] Jason Andress, *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice* (Syngress Press 2011) 63 and 64.
[6] Auguste Kerckhoffs, 'La cryptographic militaire' (1883) 9 Journal des sciences militaires 5; see also Alfred Menezes, Paul van Oorschot and Scott Vanstone, *Handbook of Applied Cryptography* 3.
[7] Jason Andress, *The Basics of Information Security* 63.
[8] See Jason Andress, *The Basics of Information Security* 79; see also Bert-Jaap Koops, *The Crypto Controversy* 33.

on a list of 10 principles and values related to encryption, participants considered privacy, data protection, and information security as the most important for them.[9] This is expected given that the participants generally understand the role of encryption in preserving the confidentiality, integrity and authenticity of data and communications.

Whether they act as users, providers or regulators of encryption, the participants consider encryption to be essential for living in an increasingly digital and connected world. A participant explains how 'if we want to get involved in a network, distributed computing environment… 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'.[10] Another user recognises that 'encryption is important. This is useful technology. It's useful everywhere'.[11] A regulator agrees, 'We all use encryption these days. You may not even realise it, but you are. You buy something online, you've used it'.[12] A participant sums up the general perception of encryption: 'much of what we do in our everyday life, we rely on encryption – we're all agreed' [13]

Participants explain the significance and connection of encryption to preserving privacy and information security. A regulator states, 'privacy is a top-tier principle of encryption. Otherwise, you won't encrypt. If you don't want privacy, don't encrypt'.[14] A user says, 'encryption is… a way of achieving [privacy]. It relates to keeping everything a bit more private…. encryption should be there'.[15] With regard to information security, a participant explains that encryption provides 'safety.... you feel a bit better about the

[9] The other principles and values concerning encryption are: law enforcement and lawful access; national security and public safety; 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.
[10] Focus group interview with User C.
[11] Focus group interview with User M.
[12] Focus group interview with Regulator P.
[13] Focus group interview with Regulator O.
[14] Focus group interview with Regulator E.
[15] Focus group interview with User I.

information being protected'.[16] A user agrees about the significance of encryption to information security: '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'.[17] Another user says, '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]'.[18]

According to the participants, encryption also protects the confidentiality and integrity of their digital information and online data. For example, it was not a big problem when someone's laptop was lost since the hard drive was encrypted and the data could not be accessed by unauthorised parties.[19] Encryption provides a sense of security or reassurance. A participant explains, '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.… at least… it's encrypted'.[20] The person continues, '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'.[21] Participants view encryption as indispensable for secure and private communications. A provider states that, '[i]f there's anything transmitted over a wire that someone can access, you need it'.[22] Encryption is also seen as crucial for authenticity (i.e., authentication and identification). A regulator explains how people in the private and public sectors have come to depend on encryption: 'people… interact with government services…. using digital identifiers.… they have to trust that system'.[23]

[16] Focus group interview with Regulator G.
[17] Focus group interview with User G.
[18] Focus group interview with User H.
[19] Focus group interview with a user.
[20] Focus group interview with Regulator B.
[21] Focus group interview with Regulator B.
[22] Focus group interview with Provider D.
[23] Focus group interview with Regulator L.

Participants consider the use of encryption valuable not just for individuals but also for private and public entities such as businesses and government agencies. They note how the use encryption is standard protocol or practice for an increasing number of companies, organisations and government departments. According to them, companies, especially those involved in information security or deal with customer data, have encryption turned on by default. A provider explains how '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'.[24] Another provider concurs that use of encryption is a matter of policy, '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'.[25]

It appears that businesses recognise the importance of encryption for information security and many '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'.[26] Encryption is becoming more integral in how businesses operate and are embedded in their products and services. A provider explains how, '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'.[27] Another provider relates how when a 'product…carries customers' data and stores it…. we ought to take security very seriously, and so encryption is a big part of that'.[28]

[24] Focus group interview with Provider Q.
[25] Focus group interview with Provider A.
[26] Focus group interview with Provider H.
[27] Focus group interview with Provider D.
[28] Focus group interview with Provider L.

The use of encryption to ensure privacy and information security has also been embraced by government. A participant explains how in government,

> 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.[29]

Encryption is considered critical to the day-to-day operations of government. A regulator relays 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.[30]

Another regulator recounts how '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'.[31] Reliance on encryption is especially crucial when dealing with highly sensitive information like patient data. A participant narrates 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.[32]

Securing sensitive patient data would be near impossible to do without encryption.

> 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.[33]

[29] Focus group interview with Regulator B.
[30] Focus group interview with Regulator G.
[31] Focus group interview with Regulator L.
[32] Focus group interview with a regulator.
[33] Focus group interview with a provider.

A participant shares how encryption is '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'.[34]

3. Legal protections

It is evident that the participants use and rely on encryption to preserve privacy and information security. They assume that these values are protected by law, particularly data protection laws such as the Privacy Act 2020. The problem though is that people's conceptions and expectations about privacy and information security in the context of encryption do not correspond with and are not supported by the actual legal protections provided by law.

3.1 Data protection

There are different types of laws that are relevant to encryption: export control, substantive cybercrime, criminal procedure, human rights, information security, and data protection laws. Of these laws, the participants generally consider data protection laws, particularly the Privacy Act, as providing the strongest recognition and protection of their privacy and information security. This seems logical given that privacy is in the very name of the Act. However, from a legal perspective, the Privacy Act 2020 is more precisely categorised as a data protection law and not a privacy law in its truest sense. The primary purpose of the Privacy Act 2020 is to protect people's 'right to privacy of personal information'.[35] Personal information is defined in the Act as 'information about an identifiable individual',[36] which is equivalent to the concept of 'personal data' under the EU General Data Protection Regulation.[37] Thus, as a data protection law, the Privacy Act 2020 is principally concerned with the protection of natural persons against the unlawful processing

[34] Focus group interview with a provider.
[35] Privacy Act 2020, s 3(a).
[36] Privacy Act 2020, s 7(1).
[37] EU General Data Protection Regulation, art 4(1).

of their personal information. This means that while the Act safeguards data protection (i.e., informational privacy), the protection of many other types of privacy such as bodily, intellectual, spatial, decisional, communicational, associational, proprietary, and behavioural privacy[38] are outside its scope. The Privacy Act would be better called the Data Privacy Act or the Data Protection Act to more accurately describe its specific purpose and narrower remit in relation to privacy.

The Privacy Act 2020 does contain important information privacy principles (IPPs) that ensure the lawful processing of personal information.[39] For instance, IPP 5 requires the protection of the storage and security of personal information.[40] Pursuant to this principle, persons and agencies should ensure that the personal information they possess and process are safeguarded against loss and unauthorised access, use or disclosure.[41] While not mandatory, the use of encryption is generally necessary for the secure and private storage of data.

While the IPPs seek to protect personal information, they are subject to a host of express legal exceptions and qualifications, including a general exemption for law enforcement to gain access to and use personal information. For example, even though IPP 2 requires that 'the information must be collected from the individual concerned',[42] non-compliance with this principle is permitted when necessary:

> (i) to *avoid prejudice to the maintenance of the law by any public sector agency*, including *prejudice to the prevention, detection, investigation, prosecution, and punishment of offences*; or
> (ii) for the *enforcement of a law that imposes a pecuniary penalty*; or
> (iii) for the protection of public revenue; or
> (iv) for the *conduct of proceedings before any court or tribunal* (being proceedings that have been commenced or are reasonably in contemplation);[43]

[38] See Bert-Jaap Koops and others, 'A Typology of Privacy' (2017) 38 University of Pennsylvania Journal of International Law 483, 566.
[39] Privacy Act 2020, part 3.
[40] Privacy Act 2020, art 22 (IPP 5 (a)).
[41] Privacy Act 2020, art 22 (IPP 5 (a) and (b)).
[42] Privacy Act 2020, art 22 (IPP 2 (1)).
[43] Privacy Act 2020, art 22 (IPP 2 (2)(e)) (emphasis added).

The same broad exception for law enforcement is allowed in other IPPs that are crucial to preserving privacy and information security when processing personal information such as IPP 3 (collection of information from subject), IPP 10 (limits on use of personal information), and IPP 11 (limits on disclosure of personal information).[44] It is important to note that save for a limited exception concerning subject access requests,[45] IPPs are not 'enforceable in a court of law'.[46] In case of infringements and complaints, the remedy is to pursue administrative proceedings (including settlement) before the Privacy Commissioner and the Human Rights Review Tribunal.[47] Compared to the EU General Data Protection Regulation, there is limited legal recourse under the Privacy Act 2020.

Despite the Privacy Act 2020 being limited to protecting personal information, many participants wholeheartedly believe that their privacy is sufficiently protected by this law. Many of the participants do not have a legal background and simply assume that a right to privacy exists and it is legally protected. But this belief is not borne out in reality. From a legal standpoint, aside from data protection offered by the Privacy Act 2020 and the recognition of specific privacy-related torts in case law,[48] there is no general right to privacy in New Zealand.[49] This is in spite of the fact that the country has ratified the International Covenant on Civil and Political Rights, which includes an express right to privacy.[50] Under current New Zealand laws and policies, privacy is considered at most an important value or

[44] Privacy Act 2020, art 22 (IPP 3 (4)(b), IPP 10 (1)(e) and IPP 11 (1)(e)).
[45] Privacy Act 2020, art 31(2) (IPP 6 (1) on access to personal information).
[46] Privacy Act 2020, art 31(1) (the main remedies are administrative proceedings before the Privacy Commissioner and the Human Rights Review Tribunal).
[47] Privacy Act 2020, part 5.
[48] *Hosking v Runting* [2005] 1 NZLR 1 (CA) (tort of improper disclosure of private material); *C v Holland* [2012] NZHC 2155 (HC) (tort of intrusion into seclusion).
[49] See *R v Jefferies* [1994] 1 NZLR 290; see also Stephen Penk, 'Thinking About Privacy' in S Penk and R Tobin (eds) *Privacy Law in New Zealand* (Thomson Reuters 2016) 20 and 23; see also Petra Butler, 'The Case for a Right to Privacy in the New Zealand Bill of Rights Act' (2013) 11 NZJPIL 213.
[50] International Covenant on Civil and Political Rights, art 17 (while New Zealand is a signatory, it has not incorporated a general right to privacy into its national law).

interest, but does not yet amount to a general right.[51] A true general right to privacy should be expressed or provided for in the New Zealand Bill of Rights Act 1990, which has been proposed and considered but never adopted.[52]

3.2 Civil and criminal procedure rights

In contrast, the normally neglected civil and criminal procedure rights are the ones that actually provide extensive and robust legal protection to privacy and information security particularly in relation to encryption. The right against unreasonable search and seizure offers crucial protection. Pursuant to this right, 'Everyone has the right to be secure against unreasonable search or seizure, whether of the person, property, or correspondence or otherwise'.[53] This right provides stronger privacy protection than the Privacy Act 2020 since the former has a wider scope and is not narrowly focused on data protection matters. Not limited to merely ensuring the lawful processing of personal information, the right against unreasonable search and seizure is concerned with preserving a person's reasonable expectation of privacy in its fullest sense.[54] The law will protect a person's reasonable expectation of privacy when (1) the person has a subjective expectation of privacy in the place or thing being searched and (2) that expectation is one that society is prepared to recognise as reasonable.[55] With such expansive coverage, this right protects not just information privacy but all types of privacy including bodily ('person'), intellectual, spatial ('property'), decisional, communicational ('correspondence'), associational, proprietary ('property'), and behavioural ('or otherwise'). The use of the term 'correspondence' means

[51] See Law Commission, *Privacy Concepts and Issues* (NZSP 19, 2008); but see Thilini Karunaratne *The Reasonable Expectation of Privacy in New Zealand Law* (LLM thesis, University of Waikato 2020).
[52] See Petra Butler, 'The Case for a Right to Privacy in the New Zealand Bill of Rights Act'.
[53] New Zealand Bill of Rights Act 1990, s 21.
[54] See *R v Alsford* [2017] NZSC 42 [63].
[55] See Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act: A Commentary* (LexisNexis NZ Limited 2015) 936.

this right also upholds the associated right to secrecy of communications whether it involves sealed letters or encrypted messages.

The right against unreasonable search and seizure together with encryption are a potent combination for preserving privacy and information security in a digital age because they offer dual legal and technical protections. Under the law, the right against unreasonable search and seizure requires certain legal conditions must be proven or met in order to conduct a lawful search, seizure and surveillance.[56] The absence or impairment of any of these conditions would allow a person whose encrypted data or communications are subject to a search or surveillance to question the reasonableness and lawfulness of such government actions. Further, in case of an unlawful search or surveillance, encryption provides an extra layer of protection because unauthorised persons (including law enforcement officers) cannot access or use the encrypted data without the encryption and decryption keys. With encryption, the confidentiality, integrity and authenticity of data is doubly secure.

In addition to the right against unreasonable search and seizure, the privilege against self-incrimination is another right that provides crucial protection to privacy and information security that is similarly underappreciated. This right is expressly stated in section 60 of the Evidence Act 2006:

> (a) a person [cannot be] required to provide specific information –
> (i) in the course of a proceeding; or
> (ii) by a person exercising a statutory power or duty; or
> (iii) by a Police officer or other person holding a public office in the course of an investigation into a criminal offence or possible criminal offence; and
>
> (b) the information would, if so provided, be likely to incriminate the person under New Zealand law for an offence punishable by a fine or imprisonment.[57]

The law guards against self-incrimination, which is 'the provision of information that could reasonably lead to, or increase the likelihood of, the prosecution of that person for a criminal

[56] See Search and Surveillance Act 2021, part 4.
[57] Evidence Act 2006, s 60(1)(a-b).

offence'.[58] As stated in the Evidence Act 2006, a 'person… cannot be prosecuted or penalised for refusing or failing to provide the information, whether or not the person claimed the privilege when the person refused or failed to provide the information'.[59]

The privilege against self-incrimination plus encryption are able to safeguard privacy and information security because they mutually reinforce each other. As explained earlier, encryption helps protect the confidentiality, integrity and authenticity of data by transforming information into ciphers and code that are inaccessible, unintelligible or unusable to unauthorised parties (including law enforcement officers) who do not have access to the encryption and decryption keys. The privilege against self-incrimination fortifies the technical safeguards offered by encryption by providing added legal protection that prevents a person from being compelled against their will to provide information (including encryption passwords and other access information) that would expose them to criminal liability.[60] Since the robustness of encryption depends of the secrecy and security of passwords and encryption keys, the right against self-incrimination provides vital legal protection to encryption as well as people's privacy and information security.

4. Social vis-à-vis legal

4.1 Incongruence

There is an evident variance between the participants' social conceptions of privacy and information security in relation to encryption and the legal protections found in the law. It is ironic that people claim to prize the values of privacy, data protection and information security the most, but give the least importance to the legal rights that actually uphold and protect these values – civil and criminal procedure rights. This is apparent in a participant's

[58] Evidence Act 2006, s 4.
[59] Evidence Act 2006, s 60(2)(b).
[60] See Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act* 1437.

statement, 'People think about encryption, about secrecy, about [data] protection. I don't think people think about law enforcement and rights of [persons charged]'.[61]

How does one reconcile the disparity between the social and the legal? Based on the analysis of the empirical data, the most plausible reason is that the participants do not consider these crime-related rights relevant to them on a personal level because they see themselves as law-abiding people. They seem to believe that since they are not criminals and are not involved in criminal activities these civil and criminal procedure rights are not applicable to them. This reasoning is akin to the 'nothing to hide' argument that 'permeates the popular discourse about privacy and security issues' especially concerning government surveillance.[62] 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.[63] This sentiment is espoused by some participants. A participant 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]'.[64] Another person even opines that 'I mean, just by saying you've got nothing to hide, you've clearly got something to hide'.[65] A regulator also 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'.[66]

The converse of the 'nothing to hide' argument is that criminals are mainly the ones who need to use encryption. A participant notes, 'you've got the question of how… "bad actors" are using it as well'.[67] Another regulator says, 'we can't just let basically the

[61] Focus group interview with Provider H.
[62] See Daniel Solve, '"I've Got Nothing to Hide" and Other Misunderstandings of Privacy' (2007) 44 San Diego Law Review 745, 748.
[63] See Daniel Solve, '"I've Got Nothing to Hide" and Other Misunderstandings of Privacy' 748.
[64] Focus group interview with Regulator Q.
[65] Focus group interview with Regulator R.
[66] Focus group interview with Regulator L.
[67] Focus group interview with Regulator R.

criminals and everyone who wants to hide from what they should be doing, just say, "Let's let them do it"'.[68] 'I don't think there's any problem with that if someone's broken the law', a participant 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'.[69]

The participants understand that encryption is dual-use technology (i.e., it can be designed and used for both legitimate and illegal purposes). However, they are worried about its criminal use and the negative impact on law enforcement and policing. A regulator states, 'I think the problem is that we want [encryption] 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'.[70] Another regulator 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.'[71]

A participant similarly 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.[72]

The use of encryption by 'bad actors [is] going to make it more challenging,' explains a provider.[73] A user points out, 'the fact that, through the widespread use of crypto, you can no

[68] Focus group interview with Regulator H.
[69] Focus group interview with Provider O.
[70] Focus group interview with Regulator F.
[71] Focus group interview with Regulator H.
[72] Focus group interview with Provider H.
[73] Focus group interview with Provider O.

longer target those smaller [criminal] groups. So, everyone's use of crypto does affect' policing and law enforcement.[74]

It is noticeable that the discourse about the use of encryption in relation criminality mainly works on abstract or theoretical level. For the participants, there does not seem to be any personal stake involved. This is understandable since most of the 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.[75]

This is in stark contrast with the participants' great concern for privacy. Privacy is top of mind for most 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 (particularly the Facebook and Cambridge Analytica scandal) was the subject of much intense discussion even though the use of encryption cannot directly address or solve privacy concerns on social networking sites since the information shared and stored on these platforms are meant to be accessible and openly shared with others.

Unlike privacy though, the right against unreasonable search and seizure and other civil and criminal procedure rights do not hit close to home for many participants whether they are users, providers or regulators of encryption. As a personal or practical matter, these rights do not even show up in their consciousness. This can be explained by the fact that the participants are not aware of the crucial role that the right against unreasonable search and seizure plays in protecting privacy in its broadest sense and not just data protection. It is also possible that the participants do not understand the importance of this right in guarding against excessive or intrusive government surveillance.

[74] Focus group interview with User K.
[75] It should be noted that none of the focus group participants were recruited because they are convicted criminals or had been previously charged with an offence.

What is ironic about these findings is that, the legal rights that protect privacy the most are the very ones considered least significant by the participants: the right against unreasonable search and seizure and privilege against self-incrimination. People as a whole fail to realise the criticalness of the right against unreasonable search and seizure in protecting their reasonable expectation of privacy. This is especially noteworthy give that the protection of privacy is principally founded on or springs from the right against unreasonable search and seizure.

Revisiting the nothing to hide argument, people often forget that human rights (whether they relate to crimes 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'.[76] Valuing and asserting one's civil rights and freedoms is an essential part of living in a free and democratic society. People have the right to access, use and develop encryption to preserve privacy and information security, and doing so is not per se a crime and should not imply that they are criminals.

4.2 Better correspondence

In light of the incongruity between people's social conceptions and the legal protections of privacy and information security in relation to encryption, there are law and policy developments that can be undertaken to achieve better conformity between the social and the legal.

For one, there should be greater awareness of the relevance of civil and criminal procedure rights. The right against unreasonable search and seizure and privilege against self-incrimination represent the crux of the protection of human rights and freedoms with regard to access to and use of encryption. The right against unreasonable search and seizure is

[76] Paul Rishworth and others, *The New Zealand Bill of Rights* (Oxford University Press 2003) 470.

particularly relevant when it comes to the search and surveillance of encrypted devices and data, while the privilege against self-incrimination is pertinent in cases of disclosure of encryption keys, passwords and other access information.

From both social and legal perspectives, these rights need to be emphasised more and should be top of mind. This is in contrast to the low priority given to these rights by the participants. As explained earlier, these overlooked civil and criminal procedure rights provide some of the strongest legal grounds to protect human rights and freedoms. There should be greater recognition then of the criticality of these legal rights to the protection of privacy and information security. People need to realise that the laws that impact encryption the most and provide considerable legal protection are those that concern criminal investigations and law enforcement. In response to the nothing to hide argument, it should be remembered that the rights of persons suspected or charged with a crime do not apply to criminals alone but to everyone. This means that everyone should be concerned about these rights that protect them against unreasonable interference or infringement.

In addition to the wider social recognition of the importance of the privilege against self-incrimination and the right against unreasonable search and seizure to preserving privacy and information security in a digital age, there should also be stronger legal protection of these rights. The privilege against self-incrimination is crucial to encryption and how this technology protects privacy and information security. Since encryption fundamentally relies on the secrecy and inviolability of encryption keys and passwords, a fairer balance needs to be struck between the privilege against self-incrimination and the power of law enforcement officers to compel the disclosure of access information. As the law currently stands, a broad range persons (potentially even suspects or persons charged with a crime) can be required to provide assistance as part of a search, including the reasonable provision of necessary

information such as passwords and access information.[77] The protection of the privilege against self-incrimination in digital and computer searches is not as strong as it could or should be. While the Search and Surveillance Act 2012 states that the privilege against self-incrimination is available in computer system searches, vague and abstruse wording of the statute has rendered the protection and exercise of such right weak or ineffective.[78] Furthermore, interpretations limiting the applicability of the privilege against self-incrimination to cases where the passwords that are forcibly disclosed are *in themselves* incriminating (e.g., the password must be 'I shot the sheriff' to be inculpatory)[79] is severely restrictive and would render nugatory this important right. Given the testimonial quality of passwords[80] and the essentiality of encryption keys to the confidentiality and integrity of encryption, the protection of the privilege 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 privilege against self-incrimination and they should not be penalised for exercising their right.[81] This is in accord with the basic human rights principles of justice and fairness.[82]

When used together with encryption, the right against unreasonable search and seizure is critical to protecting privacy and information security. On the whole, the rules on searches, seizures and surveillance under the Search and Surveillance Act 2012 in relation to the New Zealand Bill of Rights Act 1990 are fair and just. For example, the general warrant requirement to conduct a search or surveillance recognises and balances human rights and

[77] See Search and Surveillance Act 2012, s 130.
[78] See Search and Surveillance Act 2012, s 130; see also Law Commission, *Review of the Search and Surveillance Act 2012* (NZLC R141, 2017), paras 12.160-12.162.
[79] See Law Commission, *Review of the Search and Surveillance Act 2012*, paras 12.168-12.169; see also Warren Young, Neville Trendle and Richard Mahoney, *Search and Surveillance: Act and Analysis* (Thomson Reuters 2012) 211.
[80] Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act* 1442.
[81] Law Commission, *The Privilege against Self-Incrimination* (NZLC PP25, 1996), para 1.
[82] See New Zealand Bill of Rights Act 1990, ss 25 and 27.

law enforcement interests. However, the law in this area can still be improved to better uphold privacy and information security. Specifically, the power to demand assistance as part of search and surveillance operations demands further clarification and delimitation. Law enforcement officers are granted the authority to request assistance from persons during a search or surveillance of encrypted devices, data or communications.[83] There is lack of clarity though as to the meaning and extent of this duty of assistance especially with regard to third party providers. Providers may end up undermining the privacy and information security of their products and services to comply with this duty. As seen in the case of the encrypted email service Lavabit, providers may even be forced to go out of business.[84] Lavabit was compelled through a court order to provide its decryption keys to US law enforcement authorities. After providing the keys, the operator of Lavabit shut down the service in order to prevent the privacy and information security of all its users from being further put at risk or compromised.[85] Greater clarity and legal safeguards really need to be put in place on the duty of assistance to avoid such potentially unreasonable or unjust results from occurring.

5. Concurrence between social and legal

Privacy and information security are significant values for people living in a digital and connected world. With vast amounts of data being produced, stored, collected and processed about them, it is no wonder that people are very concerned about issues surrounding privacy and information security and consider them of utmost importance. They expect and have come to rely on both technology and law to protect these cherished values. But, people's conceptions and expectations about how their privacy and information security are protected need to be grounded in both the technical and legal realities. From a technical

[83] Search and Surveillance Act 2012, ss 130(1) and s 55(3); Telecommunications (Interception Capability and Security) Act 2013, s 24.
[84] 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.
[85] See Ladar Levinson, 'Secrets, lies and Snowden's email: why I was forced to shut down Lavabit'.

standpoint, encryption offers the most direct and effective means for people to control or preserve their privacy and information security. This technology can help ensure the confidentiality and integrity of information and the secrecy of communications.

However, the protection of privacy and information security through technical means can only go so far. It also needs to be supported and bolstered by legal protections. Without appropriate or additional legal safeguards, even the technical protections offered by encryption can be undermined or nullified by existing legal powers and procedures (e.g., the authority to the compel persons to disclose passwords to encrypted data and devices during a search). It is not enough to depend on technology alone. People need to recognise the significance and seek recourse under those laws that preserve and advance their privacy and information security the most. Going beyond data protection laws, laws concerning civil and criminal procedure rights are the ones that provide some of the strongest and broadest protection, specifically the right against unreasonable search and seizure and the privilege against self-incrimination. To ensure that privacy and information security vis-à-vis encryption are sufficiently protected, it is paramount for people's social conceptions to be better aligned and coincide with the legal protections provided by law, and vice versa.