Principles and values of encryption: Relevance and influence on information technology law and policy (Part 1)

PRINCIPLES AND VALUES IN LAW AND TECHNOLOY

Encryption is a complicated and controversial subject from the viewpoint of information technology law and policy (see Organisation for Economic Co-operation and Development "Recommendation of the Council Concerning Guidelines for Cryptography Policy" (1997)). It can be defined as a technology that transforms information or data into ciphers or codes for purposes of ensuring its confidentiality, integrity and authenticity (Michael Anthony C Dizon and Philip James McHugh "Encryption laws and regulations in one of the Five Eyes: the case of New Zealand" (2022) 31 Information & Communications Technology Law 220 at 222). This technology is used on data, devices, computers, information systems and networks because it helps ensure cybersecurity and data privacy. But it can also help cybercriminals and other malicious actors hide their identities and conceal their crimes. With the growing application of encryption, the legal problems involving this technology have and will continue to be 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 private and public actors regarding lawful access to and use of encryption (Michael Hack "The implications of Apple's battle with the FBI" (2016) 7 Network Security 8). 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 (Electronic Privacy Information Center, "Apple v. FBI: Concerning an order requiring Apple to create custom software to assist the FBI in hacking a seized iPhone" <https://epic.org/amicus/crypto/apple/#background>). 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 (Ellen Nakashima and Reed Albergotti "The FBI wanted to unlock the San Bernardino shooter's iPhone. It turned to a little-known Australian firm" (14 April 2021) The Washington Post

<https://img.washingtonpost.com/technology/2021/04/14/azimuth-san-bernardino-apple-iphone-fbi/>). 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 concerning encryption remain unresolved.

While there have been many studies, reports and publications on the problem of regulating encryption, most of them have focused solely on either the technical aspects or legal arguments. This article is different because it utilizes an interdisciplinary, socio-legal approach. It presents and examines the principles and values of encryption and critically analyzes how they relate to each other. It is argued that regulatory issues concerning encryption cannot be solved through technology alone. While the prospects of using quantum computers to break current 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 encryption and post-quantum cryptography. A purely technical solution is not viable because technological advancements lead to a never-ending arms race. Similarly, an exclusively legal solution to encryption without proper consideration of its technical aspects and social context is also problematic. Technology laws and policies do not exist in a vacuum. They must be grounded on a proper understanding of the subject technology as well as the norms and values of the relevant stakeholders who develop, use and regulate it.

The legal issues surrounding encryption are extremely significant and they are not going away (Bruce Schneier "More crypto wars II" (21 October 2014) <https://www.schneier.com/blog/archives/2014/10/more_crypto_war.html>). State and non-state actors have their views on whether or how to regulate encryption, and it seems inevitable that their conflicting positions will soon come to a head (Dan Milmo "UK ministers seek to allay WhatsApp and Signal concerns in encryption row" (7 September 2023) The Guardian <https://www.theguardian.com/media/2023/sep/06/whatsapp-signal-online-safety-bill-uk-encryption-privacy>; see also US Department of Justice, "International statement: End-to-end encryption and public safety" (11 October 2020) <https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety>). The time is ripe to identify and discern the underlying principles and values of encryption so that the relevant stakeholders can better understand its various meanings and implications, find common ground and reach a workable consensus on how to deal with this critical technology.

The principal aim of this article is to present and analyze the fundamental principles and values of encryption and how they can inform as well as advance information technology law and policy. Focusing on principles and values is crucial because they provide a foundation or basis on which discussions and interactions between the legal and the technical can be had. Both laws and technologies (like encryption) embody and enact principles and values (Michael Anthony C Dizon "Rules of a networked society: Here, there and everywhere" in *Bridging Distances in Technology and Regulation* (R Leenes and E Kosta eds) (Wolf Legal Publishers, Oisterwijk, 2013), at 86-87; see also Helen Nissenbaum "How computer systems embody values" (2001) 34 Computer 120). In many cases, a legal principle is likewise a technical value, or they go by the same name. For instance, cybersecurity laws and information technology protocols uphold the same instrumental and terminal value of information security. While the exact meaning of information security might differ depending on the legal or technical contexts, the use of the same or associated terms (e.g., privacy and data protection) can help establish a connection or a point of intersection for possible dialogue and mutual understanding between the parties involved. This article argues that, while there are significant conflicts between and among the principles and values of encryption, there are also correspondences that can be constructively built on to enable productive deliberation and possible consensus on how to regulate and govern this technology.

This article does not intend nor aspire to resolve the plethora of problems concerning encryption and its regulation. Its chief goals are to provide exploratory and foundational research to discern the fundamental principles and values of encryption as perceived and experienced by three groups of stakeholders, namely: the general public, businesses, and government. It applies a combination of doctrinal legal research and socio-legal research to investigate and interrogate encryption principles and values in relation to technology regulation. With regard to research methods, after obtaining ethics approval, empirical data was collected primarily through focus group interviews conducted in New Zealand in 2018. Informed consent was obtained from all participants and they 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 of encryption. While the research was centered and based in New Zealand, the findings and recommendations can be relevant and useful to other

jurisdictions and contexts given the ubiquity of the same encryption technologies around the world and the similarity of objectives and goals of existing and proposed encryption regulations both nationally and internationally.

After this introduction, the article is organized in the following manner. The next section elaborates on the 10 fundamental principles and values of encryption and their meanings and categorization. In Part 2 of this article, the first section explains how members of the general public, businesses and government in New Zealand perceive and understand these principles and values. It further delves into how the three groups of stakeholders prioritize and organize the principles and values in relation to each other. Observing both conflicts and correspondences between and among the principles and values, the second section examines how they can be balanced and reconciled in and through technology regulation. Part 2 ends with a summary and reflection on the relevance of principles and values to information technology law and policy.

FUNDAMENTAL PRINCIPLES AND VALUES

Encryption involves or is concerned with a number of distinct legal, technical and social principles and values. Based on 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, there are 10 fundamental principles and values involving or associated with encryption, namely: (1) data protection; (2) information security; (3) law enforcement and lawful access; (4) national security and public safety; (5) privacy; (6) right against self-incrimination and criminal procedure rights; (7) right against unreasonable search and seizure; (8) right to property; (9) secrecy of correspondence; and (10) 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 Organisation for Economic Co-operation and Development's Guidelines for Cryptography Policy specifically mention information security, national security, public safety, and law enforcement as crucial policy objectives of encryption regulation (Organisation for Economic Co-operation and Development (OECD) "Report on background and issues of cryptography policy" (1998) at 8-9, 11, 13, 16 and 21). 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 (OECD at 9, 13, 14, 15, 25, 26, 27 and 28). In his book

on cryptography law and policy, Koops similarly refers to national security, public safety, privacy, and information security as "fundamental societal concerns" (Bert-Jaap Koops *The Crypto Controversy* (Kluwer Law International, The Hague, 1999) at 117 and 123). 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 (Koops at 119, 120, 121 and 123).

An examination of the technical and legal dimensions of encryption also reveals these very same principles and values. From a technical standpoint, information security is the primary goal of encryption. Furthermore, this technology helps protect and maintain privacy, data protection, secrecy of correspondence, and trust. In relation to law, one has the conflicting objectives of law enforcement and lawful access and national security and public safety vis-à-vis human rights values such as right against unreasonable search and seizure, privacy, secrecy of correspondence, and right against self-incrimination and criminal procedure rights.

Definitions

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 academics and policymakers). 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 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 research. Thus, in light of the principal aims of this article, the principles and values of encryption can be conceived of in the following manner.

The principle and value of *data protection* is primarily concerned with the protection of natural persons with respect to the processing of their personal data (EU General Data Protection Regulation, arts 1(1), 5 and 6; see also Privacy Act 2020). This may involve guarding against "the improper collection, use, security, storage, release or destruction of data about individuals" (Stephen Penk "The Privacy Act 1993" in S Penk and R Tobin (Des) *Privacy Law in New Zealand* (Thomson Reuters, Wellington, 2016) at 55; see also Legislation Design Advisory Committee "Legislation guidelines" at 39). 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" (EU General Data Protection Regulation, art 4(12)). Personal data refers to "any information relating to an identified or identifiable natural person" (EU General Data Protection Regulation, art 4(1)) 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 (EU General Data Protection Regulation, art 4(2)).

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" (Budapest Convention on Cybercrime, preamble). This corresponds to the "three basic objectives of information security": confidentiality, integrity and availability (the so-called CIA triad) (Koops at 24). Confidentiality is described as "the property that data are kept secret from people who are not authorized to access them" (Koops at 269 and 24), while integrity is "the property that data are unaltered and complete" (Koops at 269 and 24). Availability requires that "information and communications systems are [accessible or] available to their users at the right time" (Koops at 24). Information security has also been described as "protecting information and information systems from unauthorised access, use, disclosure, disruption, modification, or destructions" (Jason Andress *The Basics of Information Security* (Syngress Press, Boston, 2011) at 2; Department of the Prime Minister and Cabinet (DPMC) "New Zealand's cyber security strategy" (2015)). In relation to information security, encryption is specifically concerned with the confidentiality, integrity and authenticity of data.

While the principle and value of *law enforcement* is often mentioned in laws, policy papers and scholarly works, it has no express definition under New Zealand law (Policing Act 2008). 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" (*Oxford Dictionary of English* 2016). As a practical matter, it is primarily concerned with the detection, investigation and prosecution of crimes and other offences (Budapest Convention on Cybercrime, preamble). According to Koops, law enforcement helps uphold "the right to freedom from crime" which "is part and parcel of the general rule of law" (at 120). 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" (Koops at 121). *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 ability to intercept communications and collect data on their services and networks (Canadian Department of Justice "Summary of submissions to the lawful access consultation" (2003); see also Telecommunications (Interception Capability and Security) Act 2013, s 9).

National security and public safety is another example of a principle and value that is always raised and spoken about but is not explicitly defined in the law. In New Zealand, the lack of a formal definition of national security is a conscious policy decision (DPMC "Defining national security" (2017)). In relation to the Intelligence and Security Act 2017, the DPMC 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" (DPMC 2017). 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 (Arnold Wolfers "'National security' as an ambiguous symbol" (1952) 67 Political Science Quarterly 481 at 488 and 496). Absent any express statutory definition, "national security" can be construed as "the safety of a nation against threats such as terrorism, war, or espionage" (*Oxford Dictionary of English* 2016) 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 (Wolfers at 481 and 483), 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*? (David A Baldwin "The concept of security" (1997) 23 Review of International Studies 5 at 12, 13 and 15; Wolfers at 484 and 500) Examining the purposes and powers granted under the Intelligence and Security Act 2017 and how the Act addresses "matters of national security", it can 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 (Intelligence and Security Act 2017, ss 3 and 59; DPMC 2017; see also Wolfers at 481, 485 and 489).

Privacy, like national security, is another complex concept that defies precise or easy definition (Penk at 1). While formulating a definitive or universal definition of privacy seems like an impossible task, describing and defining its extent, elements and characteristics has proven less problematic. For example, despite there being no general right to privacy in New Zealand (Penk at 20), there is no question that privacy is a fundamental value (Penk at 5 and 15). It is also much broader than but includes the value of data protection (Penk at 7 and 54). Privacy is intimately related to the human rights goals of individual autonomy, dignity and equality (Penk at 16). Even though privacy has been described as simply "the right to be let alone" (Samuel D Warren and Louis D Brandeis "The right to privacy" (1890) 4 Harvard Law Review 193 at 193 and 205; Penk at 3; see also Koops at 120), it is not merely a negative freedom since it also involves the positive freedom of "self-development" (Bert-Jaap Koops and others "A typology of privacy" (2018) 38 University of Pennsylvania Journal of International Law 483 at 565 and 566). Privacy has been characterized as being composed of distinct yet interdependent elements such as solitude, intimacy, secrecy (or confidentiality) and anonymity (or inconspicuousness) (Koops and others at 564 and 566; see also Ruth E Gavison "Privacy and the limits of law" (1980) 89 Yale Law Journal 421 at 433-434 and 436; Penk at 7 and 27). According to Koops and others, there are possibly nine "ideal types of privacy", namely: bodily, intellectual, spatial, decisional, communicational, associational, proprietary, behavioural, and informational privacy (at 566). 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 (Koops and others at 566; see also Daniel J Solove "Conceptualizing privacy" (2002) 90 California Law Review 1087 at 1099-1124; see also Penk at 8). Regardless of this, privacy is without question a significant principle and value in relation to encryption (Penk at 23).

The principle and value of *right against self-incrimination and criminal procedure rights* also concerns important human rights (Legislation Design Advisory Committee at 32). These so-called rights of the accused or persons charged have legal foundations and bases in statutory law, common law, and international law (Evidence Act 2006, s 60; see also New

Zealand Bill of Rights Act, ss 23(4), 25(d), 25(a) and 27(1); see also Search and Surveillance Act 2012, ss 103(7), 130(2), 136(g) and 138; see also Law Commission *The Privilege Against Self-Incrimination* (NZLC PP25, 1996) at 12-14 and 44; see also International Covenant on Civil and Political Rights, art 14(3)(g); see also Andrew Butler and Petra Butler *The New Zealand Bill of Rights Act* (LexisNexis, Wellington, 2015) at 1430, 1433, 1434, 1437, 1438 and 1439; see also Paul Rishworth and others *The New Zealand Bill of Rights* (Oxford University Press, Oxford, 2003) at 646 and 647). The right against self-incrimination involves "[t]he right of a person not to be compelled by the threat of punishment to answer questions which might incriminate himself/herself" (Butler and Butler at 1430). 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" (1996 at 1; Butler and Butler at 1430 and 1431). 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 (New Zealand Bill of Rights Act 1993, s 23(4); see also Butler and Butler at 1431; see also Rishworth and others at 661). According to Butler and Butler, citing the case of *R v Director of Serious Fraud Office, ex parte Smith* [1993] AC 1 (HL), these two rights, together with other human rights, comprise a bundle of "silence immunities" (at 1431; see also Rishworth and others at 649) including: the right to silence, right not to be compelled to be a witness or to confess guilt, right to a fair trial and right to be presumed innocent until proved guilty according to law, right to justice, and freedom of expression under the New Zealand Bill of Rights Act 1990 (which includes the right not to speak) (Butler and Butler at 1431, 1432, 1437, 1438, 1439 and 1454; see also New Zealand Bill of Rights Act 1990, ss 23(4), 25(d), 25(a), 25(c), 27(1) and 14; see also Law Commission 1996 at 44; Rishworth and others at 647-650; see also Legislation Design Advisory Committee at 24 and 25).

In general, these 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" (Rishworth and others at 646). The Law Commission itself enumerates the reasons why the right against self-incrimination is a necessary part of a free and democratic society (1996 at 20; see also Butler and Butler at 1434-1435; Rishworth and others at 659). 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 (Law Commission 1996 at 29). 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 (Law Commission 1996 at 30; see also Rishworth and others at 646).

In addition, the right can prevent "inhumane treatment and abuses in criminal investigations" as well as "unwarranted intrusions from the State" (Law Commission 1996 at 30). 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" (Law Commission 1996 at 30; see also Rishworth and others at 647). This conforms to the principle that "[n]atural justice operates at its highest level in the case of criminal trials, with strict procedural requirements" (Legislation Design Advisory Committee at 25). Finally, the right against self-incrimination "protects some innocent defendants from conviction" (Law Commission 1996 at 30). 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.

It is worth noting that freedom of expression is not included among the fundamental principles and values of encryption in this article. Freedom of expression is undoubtedly important in a networked society and encryption can enable the exercise of this right (UN Human Rights Council "Report of the Special Rapporteur on the promotion and protection of the right of freedom of opinion and expression" (2017) at 1). In the United States, encryption and freedom of speech is considered an important issue (see Richard Post "Encryption Source Code and the First Amendment" (2000) 15 Berkeley Technology Law Journal 713; see also Lee Tien "Publishing Software as a Speech Act" (2000) 15 Berkeley Technology Law Journal 629). 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. 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.

The *right against unreasonable search and seizure* is critical for balancing human rights with law enforcement values (New Zealand Bill of Rights Act 1993, s 21). It is considered a "'broad and general right' which protects an amalgam of values including property, personal freedom, privacy and dignity" (Butler and Butler at 916 and 940). It preserves others values such as "liberty, dignity, bodily integrity, privacy, and the right to peaceful enjoyment by people of their property" (Legislation Design Advisory Committee at 100). The right against unreasonable search and seizure generally protects individual persons

from “unwarranted state intrusions…. [or] interferences with [their] person, property, correspondence, personal information or electronic communications” (Butler and Butler at 916; see also Rishworth and others at 418 and 421). The kind of state interference contemplated here normally concerns law enforcement and other activities involving penal liability (Butler and Butler at 925, 932 and 935; see also Rishworth and others at 418). 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” (Butler and Butler at 932 and 935). 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” (Butler and Butler at 904). The right “should extend not only to the interception of mail… but also the electronic interception of private conversations, and other forms of surveillance” (Butler and Butler at 904). 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 (Butler and Butler at 916-917; see also Rishworth and others at 419-420; see also Legislation Design Advisory Committee at 100). 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” (Butler and Butler at 974 and 941; see also Rishworth and others at 420; see also Penk at 20). It is worth pointing out that, unlike other jurisdictions, the right against unreasonable search and search does not give rise to a separate or distinct general right to privacy in New Zealand (Butler and Butler at 904, 919 and 920).

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 in New Zealand law (Butler and Butler at 61; Legislation Design Advisory Committee at 21 and 24). The Legislation Design Advisory Committee expressly provides in its Guidelines that “[n]ew legislation should respect property rights” (at 24). As explained by the Committee, “[p]eople are entitled to the peaceful enjoyment of their property (which includes *intellectual property* and *other intangible property*)” (at 24). 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" (New Zealand Bill of Rights Act 1993, s 27(1); see also US Constitution, fourteenth amendment). Of course, like other rights, property rights are never absolute and are subject to reasonable control as provided for by law (New Zealand Bill of Rights Act 1993, s 5; see also Legislation Design Advisory Committee at 21 and 24).

With respect to *secrecy of correspondence* or communications, while it is covered by the right against unreasonable search and seizure, it remains a distinct value that is expressly mentioned in the law and is worth analyzing separately because of the unique elements and issues it raises especially in the context of digital communications and electronic surveillance (Butler and Butler at 944 and 949). It is integral for preserving privacy, confidentiality, anonymity, aspects of freedom of association, anonymous speech, and freedom of expression (see UN Human Rights Council).

Trust is not commonly mentioned in most non-technical literature on encryption. But it plays an important moderating and balancing role for the other principles and values cited above (see Michael Anthony C Dizon "The value of trust in encryption" (2023) 4 IEEE Transactions in Technology and Society 343). Trust can be described as "an individual's willingness to depend on another… because of the characteristics of the other" (D. Harrison McKnigh and Norman L Chervany "Trust and distrust definitions" in R Falcone, M Singh and YH Tan (eds) *Trust in Cyber-Societies* (Springer, Germany, 2001) at 1). The three general types of trust are dispositional, interpersonal and institutional (McKnight and Chervany at 40). Dispositional trust relates to "the extent to which one displays a consistent tendency to be willing to depend on general others across a broad spectrum of situations and persons" (McKnight and Chervany at 38). On its part, interpersonal trust is about a person's willingness to depend on specific "other people, either personally, as in trusting behavior and trusting intentions, or their attributes, as in trusting beliefs" (McKnight and Chervany at 38). When it comes to interpersonal trust or trusting beliefs about persons, trust is based on "cognitive perceptions about the attributes or characteristics of the trustee. Often, people trust behaviorally because of inferences about the trustee's traits" (McKnight and Chervany at 36). In this case, the four characteristics of trustworthiness are competence, benevolence, integrity, and predictability (McKnight and Chervany at 41). Institutional trust is where "one believes, with feelings of relative security, that favorable conditions are in place that are conducive to situational success in a risky endeavor or aspect of one's life" (McKnight and Chervany at 37). Institutional trust is the outcome of two conditions: structure assurance and

situational normality (McKnight and Chervany at 37). There is structural assurance when "one securely believes that protective structures – guarantees, contracts, regulations, promises, legal recourse, processes, or procedures – are in place that are conducive to situational success" (McKnight and Chervany at 37). Situational normality exists when "one securely believes that the situation in a risky venture is normal or favorable or conducive to situational success" (McKnight and Chervany at 38).

Categorization

Interestingly, the 10 fundamental principles and values of encryption have been categorized in the New Zealand context. In relation to law enforcement powers, the Law Commission groups them into two general categories: "human rights values" and "law enforcement values" (Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at 37). 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) (Law Commission 2007 at 38, 39, 40 and 41.). 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" (Law Commission 2007 at 42). 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 reasonable expectation of privacy) (Law Commission 2007 at 42; see also Law Commission *Review of Search Surveillance Act 2012* (NZLC R141, 2017) at 49; see also Koops at 121).

This categorization of principles and values into human rights values vis-à-vis law enforcement values is reasonable and analytically useful. For the purposes of this article though, it would be helpful to rename the categories to "human rights and freedoms" and "law enforcement and public order goals" 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 and criminal procedure rights; 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 goals. Information security and trust deserve special attention. 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 goals. The same can be said about trust, which bolsters and mediates the other encryption principles and values. Like information security, it sits across both categories.

The table below illustrates the basic categorization 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 messy and complex than this table represents. Nevertheless, this table is useful as an analytical tool to normatively and logically categorize such discrete concepts. The intricate relations and interconnections between and among the principles and values are further elaborated in Part 2 of this article.

Figure 1. Categories of encryption principles and values