Principles and values of encryption: Relevance and influence on information technology law and policy (Part 2)

ORDER AND RELATIONSHIPS BETWEEN PRINCIPLES AND VALUES

Part 1 of this article examined the definitions and categorization of the 10 principles and value of encryption: (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. To further explore these principles and values, focus group interviews were conducted with three groups of stakeholders (i.e., the general public, businesses and government) who were asked to rank and order them. Each focus group was given 10 cards with each card having one principle and value printed on it. The participants spread the cards on the table and worked together to prioritize and organize them. During the exercise, they were also asked to explain the meaning or significance of each principle and value to them and why they ordered the principles and values in the way they did. In this way, the exercise provided an express visual representation of the relative importance the participants placed on the different encryption principles and values, as well as the dynamic connections and interactions between and among them. The three groups of stakeholders had distinct ways of prioritizing and conceptualizing and they followed their own logic or reasoning for organizing and presenting the encryption principles and values.

According to businesses

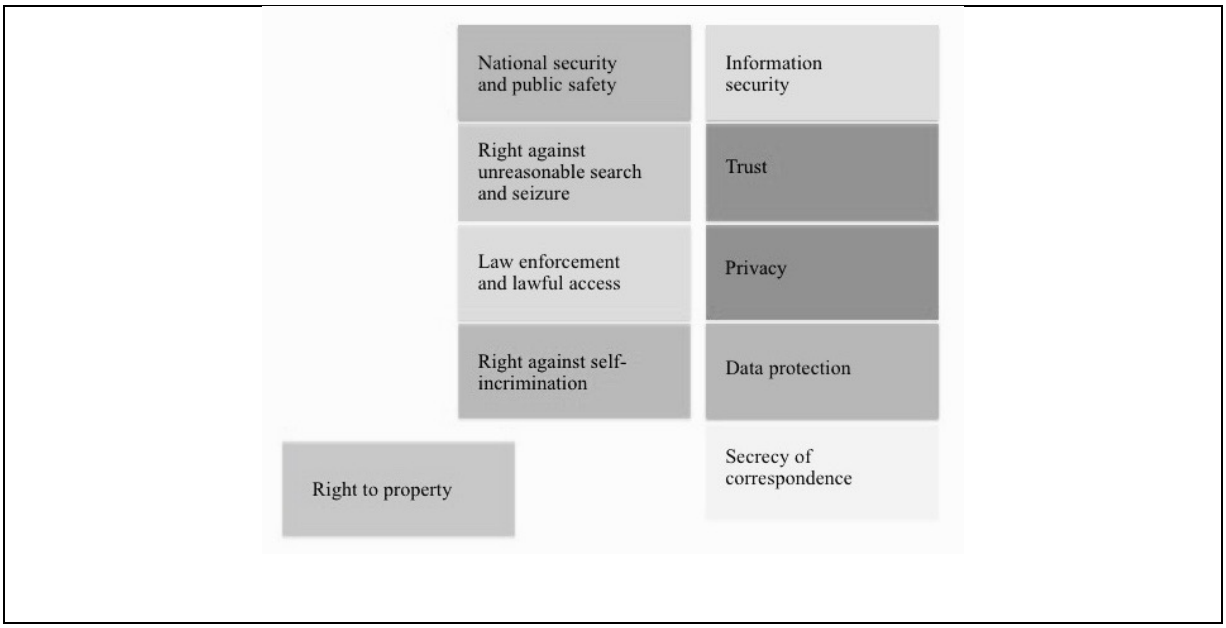
A focus group of business people arranged the principles and values in a fairly straightforward manner (see figure below). They were sorted into two columns: one for those connected with national security and law enforcement and another for information security. "They're two strands, aren't they?" notes Provider Q, one is about "government and nation" and the other pertains to the "commercial" or "private sector". Provider N agrees, "Yeah, it's kind of a big bracket thing". Provider P explains 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.

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 and criminal procedure rights. On the right column, the

participants put information security at the highest level followed by trust, privacy, data protection and secrecy of correspondence.

Figure 2. Organization of principles and values by business



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". Provider O agrees, "This is up there". 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". 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".

> 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.

Provider O says, "national security and public safety is the same as law enforcement [and covers] right against unreasonable searches". But with respect to right against unreasonable

search and seizure, “I would probably put that one near the bottom,” comments Provider N. Provider O concurs, together with criminal procedure rights. 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”.

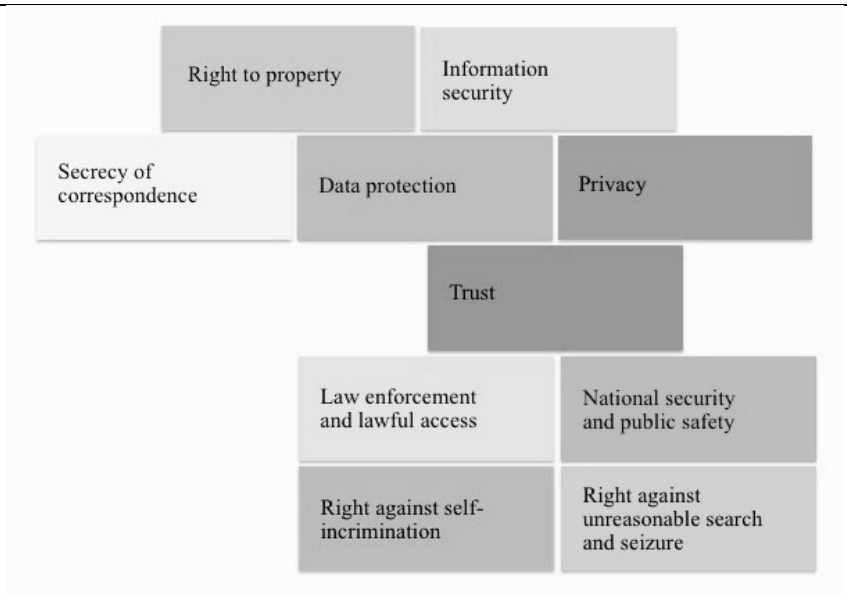
Notably, the focus group participants from business set apart right to property from the others. For them, it does not seem to fit within the two columns of national security and information security. Provider Q sees right to property “in terms of intellectual property”. Provider O agrees, “It’s a very intellectual [right or] power”.

For the general public

A focus group of members of the general public also organized the principles and values of encryption into two clusters: privacy and national security (see figure below). The first cluster includes information security, data protection, privacy, secrecy of correspondence, and right to property. The second cluster contains law enforcement and lawful access, national security and public safety, right against self-incrimination and criminal procedure rights, 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 clusters. 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”. 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].

Figure 3. Organization 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?"

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].

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.

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.

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.

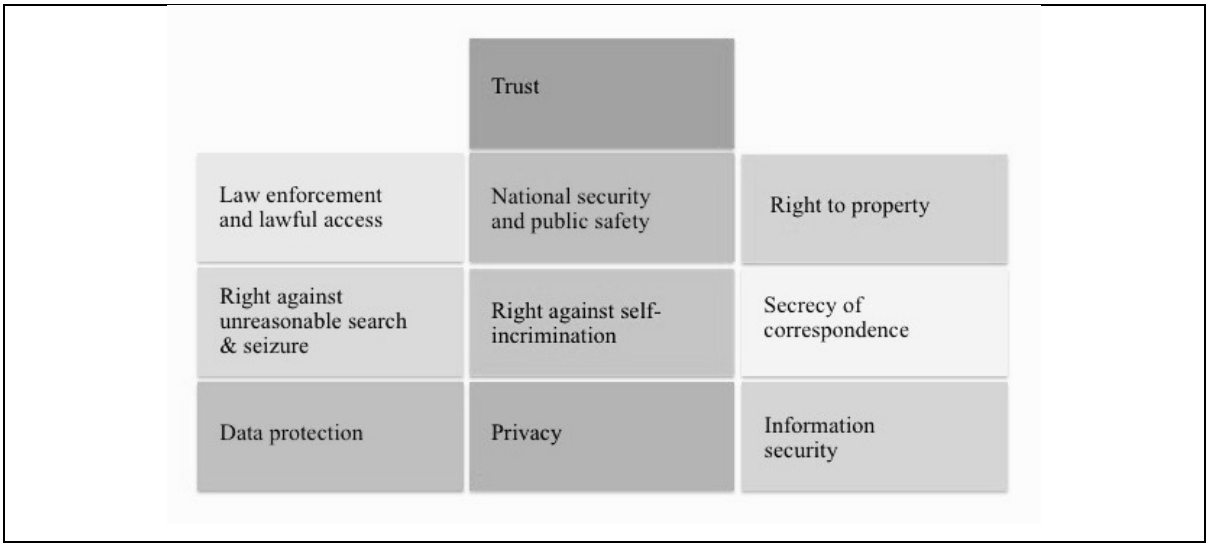
User F believes trust is important, but, at the moment, "there is no trust between these two [clusters of principles and values] actually". User I states, "I think if there was a protocol so that you knew when things are happening, then potentially, but I'd be very wary to say yes". A number of the focus 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".

View of government

A focus group of representatives from government had a more formal and structured approach to organizing 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 and criminal procedure rights, 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.

Figure 4. Organization of principles and values by government



The focus group participants from government have a mainly 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?". 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". Regulator E continues, "data protection… is about… integrity, ensuring the information that is stored and retrieved is the same information". 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.

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". 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".

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

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.

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. 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 and criminal procedure rights] 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, [criminal procedure rights]… sits sort of in the middle between the two [halves].

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". Regulator E reiterates the significance of the privacy-related principles and values at the foundation of the structure:

> 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.

For regulators, trust is an exceedingly important value. "It is a balance of trust," Regulator B explains, "So, I think it is important, how do we continue to grow a trust model that the community and society can buy into". Regulator H similarly believes, "I think we need to keep managing that balance". But finding that balance can be hard according to Regulator E, "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". Regulator E further notes that while it is one thing to "say I trust… this technology. The broader stroke being I trust society and institutions". Regulator B remarks, "I think that from a technology side… 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?" Regular E concurs, "You cannot legislate trust. And that is a very fundamental concept in encryption and in information systems security".

BALANCE AND RECONCILE PRINCIPLES AND VALUES

Based on the preceding discussion, it is clear that encryption is a complex and multifaceted technology. Despite this complexity, focusing on the principles and values of encryption provides a clear, grounded and useful framework for observing and analyzing 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 article to put forward specific or detailed legislative proposals on how to regulate encryption, the observations from and analysis of encryption principles and values can be productively used to inform and guide the development and improvement of relevant information technology laws and policies on encryption in New Zealand and other jurisdictions.

Conflicts and correspondences

Encryption is a complicated technology that embodies conflicting principles, values and interests. It has a dialectic quality and there are always at least two opposing sides to any issue or matter raised by encryption. 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 characterized 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 a practical matter, encryption can also be equally used for legitimate and illicit purposes (e.g., as a crucial means to protect privacy or to conceal the commission or evidence of a crime). Even the principles and values of encryption have been classified into the two seemingly opposing categories: human rights and freedoms versus law enforcement and public order goals. Further, there is the perennial conflict between private rights and public interests. It is this dual character of encryption that makes this technology and the problems that it raises hard to address from the perspective of law and policy.

Despite the inherently contradictory nature of encryption and the difficulties that it engenders, balancing and reconciling these conflicts is conceptually possible. As this article has shown, principles and values are a useful starting point for finding solutions to address the encryption dilemma because it makes clear what they 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 encryption principles and values 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 seemingly incongruent principles and values. 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 government data and 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 explained earlier, 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.

Complex relations and possible connections between privacy and national security

Examining conflicts and correspondences can be applied to the clash between privacy and national security. The conflict between privacy and national security is a familiar fixture

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 categorization, ranking and organization of encryption principles and values.

The focus group participants on the whole recognize the opposition 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?" Highlighting the tension between the two principles and values, Provider B emphasizes, "That's the governments job [national security], the individual's job [privacy]". According to Regulator H, the conflict 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". 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.

But despite the ostensible contestation 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". Provider D believes that "they're complementary. From the start, I think they're complementary. You can't really get one without the other". 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]". 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".

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". 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]". 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.

Regulator B similarly relates how

> 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.

Based on an analysis of the focus group interviews, a possible balance can be achieved through trust. Trust is a paramount principle and value of encryption. Aside from straddling both categories of human rights and freedoms and law enforcement and public order goals, it can act as an intermediary that intercedes between, balances and reconciles the other principles and values with each other. Regulator P explains that trust "kind of underlies all of" the other principles and values. Provider B agrees, "Trust is the number one thing for encryption" because "when you encrypt, you must trust". Regulator B relates how "if you talk about… protection of your data, your private information, security, integrity, confidentiality, I think it… [goes] down to this layer" of trust. According to Regulator E, "[i]f we look at all these conversations, everything boils down to 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". 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". From a law and policy perspective, trust can therefore act "as an essential criterion for evaluating whether a balance can be or has been struck among the contending private and public interests" (Dizon 2023 at 350).

Consideration of principles and values in encryption regulation

Taking into account principles and values can help provide guidance and direction to the development of encryption laws and policies whether in New Zealand or 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 device), the knee-jerk reaction of some government actors is to consider banning or prohibiting the use of encryption altogether. Based on the principles and values of encryption, 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 objective 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. The security and safety of computers, data and information systems rely on encryption. Encryption is essential for the effective and efficient 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 lens 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 state 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 right to property 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 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 (zero trust security model). 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.

The power to demand decryption already exists in New Zealand and is contained in the Budapest Convention on Cybercrime. Under the NZ Search and Surveillance Act 2012, 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 and criminal procedure rights. 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 (Michael Anthony C Dizon and Peter John Upson "Laws of encryption: An emerging legal framework" (2021) 43 Computer Law & Security Review 105635 at 12-13). One proposal that has not been widely discussed or considered in New Zealand and other countries is the grant of expanded investigatory powers to law enforcement including the express power 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 the 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. 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 on the part of 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.

PRINCIPLES AND VALUES IN INFORMATION TECHNOLOGY LAW AND POLICY

As discussed above, there are 10 fundamental principles and values concerning encryption. These principles and values are further categorized into human rights and freedoms and law enforcement and public order goals. They also have varying meanings and significance to different groups of stakeholders (the general public, businesses and government). The relationships between and among the principles and values are complex and conflict-ridden especially across the two categories (i.e., human rights versus 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. It is possible to balance and reconcile the principles and values with each other and this can inform and guide the development and direction of encryption regulation and information technology law as a whole.

The resolution of the encryption dilemma and its consequent problems will require further research, public deliberation, democratic debate, and ultimately difficult law and policy decisions on the part of all stakeholders involved. Whatever laws, regulations and rules on encryption are finally enacted, the key is to recognize 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.