Title: A pluralist and interdisciplinary approach to encryption regulation

Author name and affiliation: Michael Anthony C. Dizon, University of Waikato

Postal address:

Te Piringa Faculty of Law
The University of Waikato
Private Bag 3105
Hamilton 3240
New Zealand

Email: michael.dizon@waikato.ac.nz

Acknowledgments: This article is based on the ENCRYPT and DECIPHER research project that received funding from the New Zealand Law Foundation and the University of Waikato.

A pluralist and interdisciplinary approach to encryption regulation

1. Problem of regulating encryption

Encryption can be defined as a technology that transforms information or data into ciphers or codes for purposes of ensuring its confidentiality, integrity and authenticity. It is able to achieve these purposes by enciphering and deciphering data through the use of cryptographic algorithms and encryption and decryption keys. Possession of or control over these keys is critical to the security and secrecy of the encrypted information. Encryption can be applied to different states and types of data (i.e., data at rest (stored data), data in motion (communications), and data in use (processed data)).

Despite the seemingly straightforward definition and process of encryption, it is an enigmatic technology that poses significant regulatory challenges to law and policymakers. As a dual-use technology, encryption is crucial to preserving the security and privacy of information and communications, but it can also be used for illegal purposes and means and impede criminal investigations. Governments around the world have sought various ways to regulate this technology especially in light of the widespread availability and use of computers and the internet. There have been many proposed encryption regulations since the so-called Crypto Wars in the US in the 1990s when the US government sought to formally regulate the development and use of this technology (Steven Levy *Crypto: How the Code Rebels Beat the Government – Saving Privacy in the Digital Age* (Viking, New York 2001) at 187). This included the development of the Clipper Chip (an encryption device whose encryption keys were held by government escrow agents) (Levy at 226). Recently, the creation of backdoors and ghost protocols in encryption have also been proposed ("International statement – End-to-end encryption and public safety" (12 October 2020) <www.beehive.govt.nz/release/international-statement-end-end-encryption-and-public-safety>), which have been opposed by people from various sectors and industries ("CDT, GPD and Internet Society respond to new statement from Five Eyes alliance" <www.gp-digital.org/news/global-encryption-coalition-responds-to-new-statement-from-five-eyes/>).

While there have been numerous proposals to regulate encryption over the past decades, none have gained much traction or acceptance in liberal democratic states and the vociferous debates about encryption regulation continue unabated. A major issue with these proposed encryption regulations is that they seem to be labouring (whether unconsciously or unwittingly) under a very law-centred mindset. They seemingly assume that the enactment of legislation can definitively solve the issues brought about by new or disruptive technologies

such as encryption. This regulatory approach is captured perfectly in a statement made by former Australian Prime Minister Malcolm Turnbull about how state law trumps the underlying mathematics of encryption. He said, “The laws of Australia prevail in Australia, I can assure you of that. The laws of mathematics are very commendable, but the only law that applies in Australia is the law of Australia” (The Guardian, “New law would force Facebook and Google to give police access to encrypted messages” <https://www.theguardian.com/technology/2017/jul/14/new-law-would-force-facebook-and-google-to-give- police-access-to-encrypted-messages>). The problem with such a narrow and one-sided view of the relationship between law and technology is that it neglects to take into account the many significant non-legal factors and considerations that are necessary in order to properly deal with encryption or any technology for that matter. Focusing solely on state laws and the legal aspects of encryption without sufficient recognition of its technical and social dimensions can result in the adoption of laws and policies that are either ineffective or unacceptable to the relevant stakeholders or society as a whole.

The article submits that a pluralist and interdisciplinary approach is necessary for the development of encryption regulation. This approach requires abandoning or going beyond the dominant, deep-seated legal centralist and instrumentalist mindset that is prevalent in current regulatory thinking and proposals about encryption. There can be much benefit to adopting such a nuanced and multidimensional approach that examines, not just the legal, but also the technical and social dimensions of encryption. Considering the often overlooked technical and social principles and values of encryption can provide much needed context and valuable insights into how to better regulate encryption and technology more generally.

The article is organised into the following parts. Part 2 sets out the concepts of legal centralism and instrumentalism. It discusses the problems with the legal centralist and instrument mindset that pervades current and past proposals to regulate encryption. In Part 3, the article describes what a pluralist and interdisciplinary approach entails. It also explains how this approach can be beneficial to the development of encryption regulation. Part 4 illustrates how the application of a pluralist and interdisciplinary approach makes it possible to recognise critical technical principles and social values concerning encryption. It explains why taking account of these principles and values can help produce more appropriate and better-grounded encryption laws and policies. Part 5 concludes with a brief summary of the findings and further thoughts on the future of technology regulation.

2. Trouble with legal centralism and instrumentalism

A principal problem with past and current proposals to regulate encryption is that they implicitly and unknowingly adhere to and espouse a legal centralist and instrumentalist mindset to regulation. Legal centralism is the belief in the primacy or predominance of state law in controlling or shaping people's behaviours and attitudes. It subscribes to the idea that (John Griffiths "What is Legal Pluralism" (1986) 24 Journal of Legal Pluralism & Unofficial Law 1 at 3-4)

> law is and should be the law of the state, uniform for all persons, exclusive of all other law, and administered by a single set of state institutions. To that extent other, lesser normative orderings, such as the church, the family, the voluntary association and the economic organization exist, they ought to be and in fact are hierarchically subordinate to the law and institutions of the state.

Closely aligned with legal positivism, legal centralism considers state law to be the exclusive or predominant legal order within the territories or geographic boundaries of nation-states. From the perspective of legal centralism, only laws that are enacted by nation-states and those normative orders that are formally recognised by the state (e.g., state law officially recognising indigenous or customary law as having legal effect) can be considered law. It sees law simply as "a command backed up by the threat of sanction" from and by the state (Lawrence Lessig *Code version 2.0* (Basic Books, New York, 2006) at 340).

When it comes to technology regulation, legal centralism often goes hand-in-hand with instrumentalism, which is the notion that technology is always subject to the supremacy of human agency, and that it can be simply manipulated to achieve desired goals. It holds the view that "technology is a simple tool – an instrument of the social, political, or economic group or individual that chooses to develop or use a certain technology" (Arthur Cockfield and Jason Pridmore "A Synthetic Theory of Law and Technology" (2007) 8 Minnesota Journal of Law, Science & Technology 475 at 479). Instrumentalism views technology as both a regulatory target and a regulatory tool. As a target, technology is considered infinitely malleable and ultimately subject to human control, especially by the state. As a tool, technology is seen as an effective means to steer or compel persons towards stated objectives or desired ends. The latter is also called techno-regulation, which involves the "deliberate employment of technology to regulate human behaviour" (Ronald Leenes "Framing Techno-Regulation: An Exploration of State and Non-State Regulation by Technology" (2011) 5 Legisprudence 143 at 149).

The problem with legal centralism and instrumentalism in general and as they apply to encryption regulation is that they fail to recognise that: there are multiple normative orders aside from state law that significantly influence and affect people's actions in the networked

information society; and that technology cannot be easily controlled or manipulated because it is neither silent nor neutral and it actually embodies people's and society's deeply-held principles and values (Batya Friendman (ed) *Human Values and the Design of Computer Technology* (Cambridge University Press, Cambridge, 1997)). Principles and values are conceptions or beliefs of individuals or groups of the desirable whether in relation to modes of behaviour or end-goals (Clyde Kluckhohn and others "Values and value-orientations in the theory of action" in T Parsons and EA Shils (eds), *Toward a General Theory of Action* (Harper Torchbooks, New York, 1951) at 395; Milton Rokeach *The Nature of Human Values* (The Free Press, New York, 1973) at 7-8). These principles and values are therefore crucial considerations when regulating encryption or any technology. Proposed encryption regulations such encryption bans, mandatory key escrow, mandated backdoors in encryption, compelled decryption, or forced disclosure of encryption keys have been problematic and opposed by various stakeholders because they contradict and disregard the attendant technical and social principles and values concerning encryption (Harold Abelson and others "Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications" MIT Computer Science and Artificial Intelligence Laboratory Technical Report (6 July 2015)). One way to take cognisance of and properly address these principles and values is to adopt a legal pluralist and interdisciplinary approach to encryption regulation.

3. Benefit of pluralism and interdisciplinarity

3.1 Legal pluralism

A foundational concept of a pluralist and interdisciplinary approach to encryption regulation is legal pluralism. It has been described as "the presence in a social field of more than one legal order" (Griffiths at 1). It advances the view that there is not one but many laws or normative orders in any socio-technical field or activity. Legal pluralism is similarly a response to legal centralism because it "rejects the idea that only the state can be considered the source of 'legal' rules. Any social field is full of normative material. Some originate within the field itself, some from fields external to it, and some from smaller social fields which are more or less included within it" (Griffiths at 34). As Griffiths further explains, "The descriptive theory of legal pluralism is, thus, the theory of normative heterogeneity entailed by the fact that social space is normatively full rather than empty, and of the complexity of the working of norms entailed by such heterogeneity" (at 34). Von Benda-Beckmann further expounds on how legal pluralism is (Franz von Benda-Beckmann "Who's Afraid of Legal Pluralism" (2002) 47 Journal of Legal Pluralism 37 at 72):

> an outcome of social processes, as a context for social interaction, as being reproduced in interactions in different interaction settings and locales, etc. Only then can be seen to what extent, and in which socio-political or geographical spaces, legal forms are plural, individuals are "multilegal" and objects and social relationships "multi-normative", and to what extent one can generalize from any such layer or interaction setting for the wider existence and significance of plural legal constellations.

From a legal pluralist perspective, "there is not one single law but a network of laws" (Boaventura De Sousa Santos "Law: A Map of Misreading. Toward a Postmodern Conception of Law" (1987) 14 Journal of Law and Society 279 at 281).

While legal pluralism is admittedly a complex concept, it is essentially a recognition of the multiple and plural legal and normative orders that exist in any given field or situation. In practical terms, it is mainly about having a less state law-centred view of law and regulation and being open to the presence of other normative orders that influence people's behaviour (Michael Anthony C. Dizon "Laws and Networks: Legal Pluralism in Information and Communications Technology" (2011) 15 Journal of Internet Law 1). Normative here means a prescription of what persons ought to do or else (Richard T Morris, "A typology of norms" (1956) 21 American Sociological Review 610 at 610).

Interestingly, the existence of plural legal and normative orders has been widely accepted in the field of law and technology. The most influential and well-known theory in technology law, Lawrence Lessig's theory of the four modalities of regulation (Lessig at 123), subscribes to the concept of legal pluralism. Lessig believes that there are four modalities of regulation that control people's behaviours in cyberspace and in the real world: law, norms, market and architecture. According to Lessig, all four modalities have significant effects on people's conduct. Lessig's theory is noteworthy because it considers law to be only one of the four regulatory modalities. Other modes of regulation such as social norms and technology (as part of or as subsumed in architecture) also significantly influence people's actions and decisions. To illustrate, even in the routine activity of driving, people are subject to these plural regulatory modalities: law (speed limits), norms (driving etiquette), market (fuel tax and petrol prices), and technology or architecture (speed humps and speed cameras). From a legal pluralist perspective, Lessig's theory is evidently an expression or description of the plural normative orders present in a digitally connected world that includes the: legal (law), social (norms), economic (market) and technological (architecture). It could be said that Lessig's theory repudiates legal centralism and espouses a legal pluralist approach to technology regulation.

3.2 Interdisciplinary method

Studying plural normative orders naturally calls for an interdisciplinary research method that examines the legal, technical and social dimensions of a problem. Such an approach means focusing on the relevant (1) laws and legal rules, (2) technical principles and codes, and (3) social norms, values and other rules of behaviour. This requires drawing on the fields of technology law, science and technology studies (STS), and socio-legal studies. A hybrid approach that analyses the legal, technical and social dimensions together and at the same time can be very useful. For instance, it makes sense for doctrinal legal research on applicable technology laws to be done in conjunction with the collection and evaluation of empirical social data of persons who are or will be affected by these regulations. The fields of STS and socio-legal studies are particularly relevant to the study of plural normative orders because they both emphasise the mutual shaping between and among law, technology and society (Weibe E Bijker, Thomas P Hughes and Trevor J Pinch (eds) *The Social Construction of Technological Systems: New Directions in the Sociology of History of Technology* (The MIT Press, Cambridge, 1987)).

Furthermore, a pluralist and interdisciplinary approach to technology regulation is valuable because it focuses on the complex and multifaceted interactions between the legal, technical and the social domains. Lessig himself explains how the "interaction among these modalities is dynamic" (Lessig at 130) and why "we need a more general understanding of how regulation works – one that focuses on more than the single influence of any one force such as government, norms, or the market, and instead integrates these factors into a single account" (Lessig at 121). Having an integrated interdisciplinary approach is critical because when it comes to regulating a technology like encryption, "policy choices are available either through technology itself, through laws that cause technology to exclude possible options, or through laws that cause users to restrict certain actions" – that is, through technical, legal or social means (Joel R Reidenberg "Lex Informatica: The Formulation of Information Policy Rules Through Technology" (1998) 76 Texas Law Review 553 at 569).

Many proposed encryption regulations are problematic because they are working under a legal centralist and instrumentalist mindset that conceives of the state and state laws as the preeminent regulator and mode of regulation. However, legal, technical and social problems brought about by emerging or disruptive technologies such as encryption cannot be solved through legal solutions alone. Socio-legal researchers are very much aware of the limitations of state law when it comes to dealing with technical change and social upheaval. As Moore says, "Legislation is often passed with the intention of altering the going social

arrangement in specified ways. The social arrangements are often effectively stronger than the new laws" (Sally Falk Moore "Law and Social Change: The Semi-Autonomous Social Field as an Appropriate Subject of Study (1973) 7 Law & Society Review 719 at 723). It makes sense then to adopt a legal pluralist and interdisciplinary approach to encryption regulation that goes beyond the examination of applicable laws and also considers the technical and social dimensions of the problem, particularly the critical technical principles and social values involving encryption.

4. Importance of technical and social principles and values

Utilising a pluralist and interdisciplinary approach makes it possible to observe and analyse important principles and values that are at the core of the technical and social orders that influence encryption. Understanding and taking account of these principles and values can provide crucial insights and much needed guidance to the development and implementation of encryption regulation.

4.1 Technical principles

When proposing or developing encryption regulations, a critical technical principle concerning the development, access to and use of encryption must be taken into account – the secrecy and security of keys. This is the second principle of Auguste Kerckhoffs' classic statement of the six principles of cryptography (Auguste Kerckhoffs "La cryptographic militaire" (1883) 9 Journal des sciences militaires 5). It is considered "one of the underlying principles for many modern cryptographic systems" (Jason Andress *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice* (Syngress Press, Amsterdam, 2011) at 69). Based on this principle, encryption should be secure even though everything about it is public knowledge (save for the keys) (Andress at 69). It is a "fundamental premise in cryptography… that the sets… are public knowledge. When two parties wish to communicate securely using an encryption scheme, the only thing that they keep secret is the particular key pair" – specifically, the decryption or private key (Alfred J Menezes, Paul C van Oorschot and Scott A Vanstone *Handbook of Applied Cryptography* (CRC Press, Florida, 1996) at 14). It is a guiding principle in the development and use of encryption that "cryptographic algorithms should be robust enough that, even though someone may know every bit of the system with the exception of the key itself, he or she should still not be able to break the encryption" (Andress at 69).

For persons involved in the development and implementation of encryption such as cryptologists and information security professionals, it is axiomatic that encryption and decryption keys are kept safe and private from unauthorised parties (Menezes at 14). This is

so because, “According to this principle, the security of a cryptosystem must be based entirely on the secret keys” (Hans Delfs and Helmut Knebl *Introduction to Cryptography: Principles and Applications* (Springer, Berlin, 2015) at 4). This means that “the security of the system should reside only in the key chosen” (Menezes at 14). The implication is that “the objectives of information security [must] rely solely on digital information itself ” – the key (Menezes at 3). Keys are therefore the linchpin of the privacy and security of encryption and need to be safeguarded.

The technical principle of the secrecy and security of keys should be a significant regulatory consideration. Keeping keys private and protected is essential for the security of encryption and any related system that implements it. Proposals for mandatory key escrow or similar systems where users’ keys are required by government to be deposited with a trusted third party potentially weaken or contravene this vital principle. Since encryption keys are the cornerstone of the privacy and security of encryption, their secrecy and inviolability should be protected as a matter of policy.

Knowledge of this technical principle can also be useful for regulators and law enforcement. The keys can be one of the principal targets of a criminal investigation since whoever holds the keys has access to and control over the encrypted data or communication. Specific powers and procedures under the Search and Surveillance Act 2012 such as search and seizure and production orders can be utilised by law enforcement officers to gain access to or control over these keys, and thereby the encrypted data. Nonetheless, it is worth emphasising that the secrecy and security of keys plays a crucial role in ensuring the integrity of encryption and the data and information systems that it protects. Therefore, the use of the power to compel disclosure of access information like encryption keys from providers should be used judiciously and sparingly. The production or disclosure of encryption keys should not be required if it undermines the integrity of a product or service or substantively affects and places at risk the security and privacy of other users or members of the general public who are not the subject of the investigation.

Another important technical principle that needs to be reckoned with is the inherently adversarial nature of encryption (Kerckhoffs). Encryption has historically been a cat-and-mouse game between cryptography and cryptanalysis. It is a “centuries-old battle between codemakers and codebreakers” (Simon Singh *The Code Book: The Secret History of Codes and Codebreaking* (Fourth Estate, London,1999) at ix). The development of encryption can be characterised as a race between those who seeks to preserve the secrecy and security of their information and those who set out to break it. This adversarial nature arises from the

fact that the technology of encryption embodies competing dualities: encoding vs decoding, ciphertext vs plaintext, confidential vs accessible, and unintelligible vs readable.

In the context of encryption, parties are portrayed as either friends or adversaries (Delfts and Knebl at 6). Adversaries are individuals or entities who attempt to prevent the parties from securely and secretly communicating by discovering meaningful information, corrupting information in transit, masquerading as a legitimate party, or denying communications between parties (Menezes at 496). An adversary, who can either be passive or active, is also called an enemy, attacker or eavesdropper (Menezes at 13 and 14). An adversary is considered one of the expected and unavoidable dramatis personae in encryption.

The adversarial nature of encryption has significant implications on regulation. The security and integrity of encryption demands constantly anticipating and guarding against possible attacks. As Rivest states, "cryptographers must also consider all the ways an adversary might try to gain by breaking the rules or violating expectations" (RL Rivest, "Foreword" in Alfred Menezes, Paul van Oorschot and Scott Vanstone *Handbook of Applied Cryptography* (CRC Press, Florida, 1996) at xxi). In light of this, encryption laws and policies should prioritise innovation in cybersecurity and encourage continuous improvements to strengthen encryption since these are essential to stay ahead of this constantly evolving technological conflict or competition. Furthermore, it is vital for law and policymakers to avoid proposing or adopting regulations that have a direct effect or unintended consequence of impeding or dissuading developers and providers from keeping their encrypted data, devices and systems secure and resilient against known, unknown and future attacks. For example, frequent calls by governments on technology companies to create backdoors in encryption are seemingly unmindful of the adversarial nature of this technology. This critical principle must therefore be taken into account when proposing or developing encryption laws and policies.

4.2 Social values

The use of a pluralist and interdisciplinary approach can also help disclose important social values concerning encryption. Based on 10 focus groups interviews conducted with members of the general public, businesses and government in the country, of the 10 fundamental principles and values associated with encryption (i.e., data protection, information security, privacy, national security and public safety, right against self-incrimination and other rights of persons charged, right against unreasonable search and seizure, right to property, secrecy of correspondence, law enforcement and lawful access, and trust), the participants considered privacy, data protection and information security to be the

most important ones. For participants then, encryption is integral to information security and they consider it is necessary for the protection of privacy and data protection. Furthermore, they consider trust to be an all-important principle and value of encryption.

Participants understand that encryption is essential for information security. Most people are aware that this technology protects the confidentiality, integrity and authenticity of data. Given the primacy given to information security, any proposed encryption regulation should recognise that critical role of encryption in preserving this socio-technical principle and value. Thus, the development and use of encryption should be encouraged as a matter of law and policy. This is crucial because safeguarding information security is an important responsibility of persons both in the private and public sectors. For example, it is the legal duty of many providers and businesses to protect the privacy and data of their customers and users under data protection laws such as the Privacy Act 2020. The widespread use, implementation and development of encryption, including the use of encryption by default, should be actively promoted since these are necessary to protect computers and data from misuse, abuse or improper disclosure.

It is worth pointing out that the protection of other principles and values involving encryption depend on information security. Information security underpins the protection of a whole host of property, privacy and other rights of persons. For instance, privacy and data protection cannot be effectively ensured in an online or digital environment without encryption. Secrecy of correspondence of electronic communications relies on encryption. In certain respects, protecting national security and public safety is reliant on the security of critical information infrastructures and government-held data from external threats.

In the same vein, encryption regulations that undermine or weaken information security (whether intentionally or as an unintended effect) should be avoided. As a standard practice, businesses and providers should spend their time and resources improving the security of their products and services rather than weaken them. This recommendation springs from the very definition and nature of encryption. From a technical standpoint, encryption is geared towards the protection of information security by providing the appropriate level of security and being resistant to attacks. Furthermore, information security should be considered an ongoing and evolving process. The continuous development and improvement of encryption and other aspects of information security should be supported. The need for constant security improvement is connected to the adversarial nature of encryption. Since new ways are always being found or developed to break encryption or breach information security, it is imperative that the security of computers and data be

continually strengthened and improved. Because of the inherent difficulties of keeping data and information system secure because of the presence and actions of adversaries, proposed encryption regulations should not inhibit or dissuade developers and providers from enhancing the security of their products and service especially if they are subject to a legal duty to protect the privacy and security of their users.

This recommendation is supported by the *Apple v FBI* case where the US Federal Bureau of Investigation (FBI) sought to compel Apple through a court order to create a modified version of its mobile operating system for use to unlock the San Benardino shooter's iPhone. When Apple refused, the FBI was still able to gain access to the shooter's iPhone with the help of a third-party vendor. Further, after an internal investigation, the US Department of Justice came to the conclusion that the FBI should have first tried to find and exhaust all technical means available to them before seeking to legally compel a company like Apple to render technical assistance (US Department of Justice, Office of the Inspector General "A Special Inquiry Regarding the Accuracy of FBI Statements Concerning its Capabilities to Exploit an iPhone Seized During the San Bernardino Terror Attack Investigation" (March 2018)). It is also notable that there is a company selling a device called GrayKey to law enforcement that allows the latter to access any locked iPhone (Matt Burgess, "UK police are buying top secret hacking tech to break into iPhones" Wired <https://www.wired.co.uk/article/police-iphone-hacking-grayshift-graykey-uk>). These technical developments show that encryption is not foolproof and technical workarounds are possible and are always being developed. The continuous improvement and testing of the security of information systems and devices is a necessary part of information security. Information security is indeed a central principle and value that should be considered in any law and policy discussion about encryption.

In addition to information security, participants consider privacy and data protection to be the topmost principles and values concerning encryption. Encryption naturally involves privacy and data protection. This technology protects data whether it is at rest (stored data), in motion (communications) or in use (processed data). In today's information-rich and data-driven world, there is no other technology that is as essential and intrinsically linked to privacy and data protection as encryption. Given the indispensability of encryption for preserving privacy and data protection, providers and users should have the freedom to develop, access and use encryption. Moreover, encryption should be widely available and used by default. Encryption is an essential element of the principle of privacy by design. Any laws and policies that seek to curb the development and use of encryption or limit the choice

or availability of this technology should not be pursued. For instance, a ban on the use of encryption by the general public will not only be infeasible, but it would effectively deny them of their right to protect their privacy and personal data. The use of encryption inescapably involves a person's reasonable expectation of privacy. As such, any direct or indirect interference with the use of encryption for privacy and data protection must be based on lawful grounds and must comply with the general standard of reasonableness.

Finally, a pluralist and interdisciplinary approach reveals the paramount importance of trust in encryption. People will not use encryption if they do not trust the technology itself or they distrust the persons who develop, provide or regulate it. There is lack of trust if encryption is considered unsafe or insecure. This is a major reason why mandatory backdoors in encryption have been vehemently opposed by users and providers alike because backdoors do not engender trust in the technology, the government, or whoever can gain access (including malicious actors and cybercriminals). Aside from trusting the technology of encryption, there must also be trust in the providers of the encrypted products and services as well as the regulators who seek to regulate or control encryption.

Encryption is founded and relies on the principle and value of trust. It is imperative then that any proposed encryption regulation should be assessed from the viewpoint of its trustworthiness. People should ask: Does the proposed regulation strengthen, maintain or weaken trust in encryption and between the relevant parties? Proposed powers and measures that diminish or break trust should be abandoned while those that help maintain or build trust in encryption should be explored, examined or adopted. Trust should be a core consideration when developing or implementing encryption laws and policies.

5. Consideration of legal, social and technical dimensions

It is evident from the above discussion that the complex problem of regulating encryption cannot be resolve through law or legal means alone. It is necessary then to do away with the belief in the supremacy of the state and the notion that state law is sole form and means of regulating behaviour. By going beyond this legal centralist and instrumentalist mindset, it becomes possible to recognise the plural normative orders in a digital networked world. Further, it allows for greater understanding of the critical technical and social principles and values that can help contextualise and enlighten the difficult matter of encryption regulation.

More generally, when proposing and developing technology laws and policies, it is vital to examine not just the legal, but also the technical and social dimensions of the technology sought to be regulated. This can be accomplished by using a pluralist and

interdisciplinary approach that seeks to find, understand and take into account the fundamental principles and values of the subject technology.