Osgoode Hall Law Journal

Article 3

Law, Metaphor, and the Encrypted Machine

Lex Gill
Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto

Citation Information

Gill, Lex. "Law, Metaphor, and the Encrypted Machine." *Osgoode Hall Law Journal* 55.2 (2018) : 440-477.
https://digitalcommons.osgoode.yorku.ca/ohlj/vol55/iss2/3

Law, Metaphor, and the Encrypted Machine

Abstract
The metaphors we use to imagine, describe, and regulate new technologies have profound legal implications. This article offers a critical examination of the metaphors we choose to describe encryption technology and aims to uncover some of the normative and legal implications of those choices. The article begins with a basic technical backgrounder and reviews the main legal and policy problems raised by strong encryption. Then it explores the relationship between metaphor and the law, demonstrating that legal metaphor may be particularly determinative wherever the law seeks to integrate novel technologies into old legal frameworks. The article establishes a loose framework for evaluating both the technological accuracy and the legal implications of encryption metaphors used by courts and lawmakers—from locked containers, car trunks, and combination safes to speech, shredded letters, untranslatable books, and unsolvable puzzles. What is captured by each of these cognitive models, and what is lost?

Law, Metaphor, and the Encrypted Machine

LEX GILL*

The metaphors we use to imagine, describe, and regulate new technologies have profound legal implications. This article offers a critical examination of the metaphors we choose to describe encryption technology and aims to uncover some of the normative and legal implications of those choices. The article begins with a basic technical backgrounder and reviews the main legal and policy problems raised by strong encryption. Then it explores the relationship between metaphor and the law, demonstrating that legal metaphor may be particularly determinative wherever the law seeks to integrate novel technologies into old legal frameworks. The article establishes a loose framework for evaluating both the technological accuracy and the legal implications of encryption metaphors used by courts and lawmakers—from locked containers, car trunks, and combination safes to speech, shredded letters, untranslatable books, and unsolvable puzzles. What is captured by each of these cognitive models, and what is lost?

* Lex Gill is a former Research Fellow at the Citizen Lab at the Munk School of Global Affairs and Public Policy, University of Toronto. This article was completed during her term at Citizen Lab. Nothing in this publication reflects the position or views of her current or future employers. The author would like to offer particular thanks to Victor Muñiz-Fraticelli, Mickael E., Henry de Valence, Nicola Dalla Guarda, Tamir Israel, and Gabriella Coleman for their generous feedback on earlier drafts of this work.`

THE METAPHORS WE USE to imagine, describe, and regulate new technologies have profound legal implications. This article offers a critical examination of the metaphors we choose to describe encryption technology in particular, and aims to uncover some of the normative and legal implications of those choices.

Part I provides a basic description of encryption as a mathematical and technical process. At the heart of this article is a question about what encryption *is* to the law. It is therefore fundamental that readers have a shared understanding of the basic scientific concepts at stake. This technical description will then serve to illustrate the host of legal and political problems arising from encryption technology, the most important of which are addressed in Part II. That section also provides a brief history of various legislative and judicial responses to the encryption 'problem,' mapping out some of the major challenges still faced by jurists, policymakers, and activists. While this article draws largely upon common law sources from the United States and Canada, metaphor provides a core form of cognitive scaffolding across legal traditions. Part III explores the relationship between metaphor and the law, demonstrating the ways in which it may shape, distort, or transform the structure of legal reasoning. Part IV demonstrates that the function served by legal metaphor is particularly determinative wherever the law seeks to integrate novel technologies into old legal frameworks. Strong, ubiquitous commercial encryption has created a range of legal problems for which the appropriate metaphors remain unfixed. Part V establishes a loose framework for thinking about how encryption has been described by courts and lawmakers—and how it could be. What does it mean to describe the encrypted machine as a locked container or building? As a combination safe? As a form of speech? As an untranslatable library or an unsolvable puzzle? What is captured by each of these cognitive models, and what is lost? This Part explores both the technological accuracy and the legal implications of each choice. Finally, the article offers a few concluding thoughts about the utility and risk of metaphor in the law, reaffirming the need for a critical, transparent, and lucid appreciation of language and the power it wields.

I. AN ENCRYPTION PRIMER

For computer scientists, the concepts described in this article are both obvious and fundamental. The same cannot be said for the lawyers, politicians, and judges who shape the law as it pertains to encryption technology—at least not universally. An article that seeks to understand what encryption "is" to the law (and what it ought to be) therefore requires a small detour to explain what

encryption "is" in fact. Ludwig Wittgenstein has said that "[i]n mathematics, *everything* is algorithm and *nothing* is meaning," even in moments when "we seem to be using *words* to talk *about* mathematical things. Even these words are used to construct an algorithm."[1] Perhaps in law we struggle with an inverse kind of problem: that everything is meaning and nothing is algorithm—not even the algorithms themselves.

Wittgenstein cautioned against the tendency in philosophy to interfere both in language and mathematics, arguing that it ought to seek out only understanding, to "leave everything as it is."[2] Even if we accept that jurists (unlike Wittgenstein's philosopher) have the latitude to move beyond pure description, they must nonetheless begin by reckoning with mathematical fact. Without a functional understanding of the technology itself, it is impossible to appreciate how the language of the law variously captures, clarifies, distorts, and obfuscates the nature of the encrypted machine. To that end, this Part aims to summarize a small number of basic mathematical concepts which inhabit the mind of every cryptographer, asking the reader to adopt them as his or her own in order to make better sense of the analysis set out in the article that follows.

Encryption is the process of using a cryptographic algorithm (a *cipher*) to transform information (*plaintext*)—such as an ordinary email, text message, or file—into an unintelligible format (*ciphertext*) using a secret (a *key*). Decryption, by contrast, is the process of using that key to revert the ciphertext back to its original form.[3] In other words, encryption encodes a message such that it can only be read by its intended recipient (*i.e.*, whoever has the secret key). The mechanism from which the encryption key is derived can take any number of forms—for example, it might be a passphrase, numeric code, or biometric data (like a fingerprint or a retinal scan). As a security tool, encryption is used to maintain message confidentiality, to authenticate the identity of the sender, and to preserve the integrity of the message.[4]

Cryptography has been used to conceal political and military secrets since at least the time of Julius Caesar, who wrote to Marcus Cicero using a basic

---

1. Ludwig Wittgenstein, *Philosophical Grammar*, Rush Rhees, ed, translated by Anthony Kenny (Oxford: Basil Blackwell, 1974) at 468 [emphasis in original].
2. Andrew W Moore, "Wittgenstein and Infinity" in Oskari Kuusela & Marie McGinn, eds, *The Oxford Handbook of Wittgenstein* (Oxford: Oxford University Press, 2011) 105 at 114.
3. Bruce Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd ed (New York: John Wiley & Sons, 1996) at 1 [Schneier, *Applied Cryptography*].
4. In other words, encryption is used to ensure that the message can only be read by those with the key, to confirm that the sender is who she says she is, and to ensure that the message has not been altered in transit.

cipher "that shifts the alphabet three places to the right and wraps the last three letters *X, Y, Z* back onto the first three letters" (this is called the "Caesar cipher" or "Caesar shift").[5]

JULIUS ———— MXOLXV E (*M*) = (*M* + 3) (modulo 26)
plaintext ciphertext

Cryptanalysis is the study of cryptographic systems in order to find weaknesses in their design or implementation which would allow the analyst to derive a plaintext message from its ciphertext counterpart without the key. For a simple example, note that a "shift" cipher like the one above only has 26 possible keys using a standard Latin alphabet. This makes finding the *right* key easy to guess (even for a human) through exhaustive search ("brute force"). Even when these kinds of substitution ciphers become more complex, they remain relatively trivial to decrypt using statistical frequency analysis, because the ciphertext continues to reveal the linguistic and structural properties of the original plaintext message.[6] Modern cryptographic tools use vastly more sophisticated encryption algorithms, both in order to mitigate that risk and to increase the number of possible keys.[7] As a result, decryption becomes more difficult, time-intensive, and computationally demanding for an adversary.

Note however that in order to remain secure, such systems (no matter how complex the algorithm) require some additional mechanism to safely transmit

---

5. Dennis Luciano & Gordon Prichett, "Cryptology: From Caesar Ciphers to Public-Key Cryptosystems" (1987) 18:1 College Mathematics J 2 at 3.
6. *Ibid* at 6.
7. Conceptually, it may help jurists to understand this methodology by looking to the result when taken to its logical conclusion in the form of the "one-time pad," a form of polyalphabetic cipher invented in 1917. The one-time pad uses a key consisting of randomly selected numbers that is the same length as the plaintext message itself. The result is that for any given one-time pad, it is "equiprobable that a plaintext character is represented by any ciphertext character," eliminating patterns that would otherwise betray the original message (*ibid* at 7). See Dirk Rijmenants, "The Complete Guide to Secure Communications with the One Time Pad Cipher" *Cipher Machines and Cryptology* (22 January 2016) at 2, online: <users.telenet.be/d.rijmenants/papers/one_time_pad.pdf> (the ciphertext generated is theoretically unbreakable and mathematically unsolvable without possession of the key, "regardless [of] any existing or future cryptanalytic attack or technology, infinite computational power or infinite time"). However, one-time pads require the generation and exchange of a new set of key characters for every message sent, making them highly impractical for most purposes. One-time pads also require an additional mechanism for secure transmission of the key, which is why spies were known to exchange them using disposable or self-destructing vehicles, such as flammable booklets. See also Schneier, *Applied Cryptography*, *supra* note 3 at 15-17.

the key itself to the intended recipient of the message. This is the reason that spies were historically known to exchange keys to encrypted messages using fake walnut shells, obscure radio transmissions, false coins, and flammable booklets.[8] In the 1970s, the Diffie-Hellman key exchange algorithm and the development of RSA[9] sought to address this key distribution problem, marking the dawn of *public key cryptography*. In brief, public key cryptosystems allow two parties to establish a shared secret without prior knowledge of each other over a public network.[10] In such systems, a cryptographic algorithm is used to generate a pair of two keys: a *public key* which can be used to encrypt messages for a specific party, and a *private key* which that party can then use to decrypt messages which have been encrypted with the corresponding public key. As an example, imagine two political activists—Ameenah and Benjamin—who need to exchange email correspondence but are concerned about the risk of government surveillance. Using a public key encryption system like Pretty Good Privacy (PGP),[11] Ameenah only needs to know Benjamin's public key (which he can make freely available on the Internet) in order to encrypt an email such that only Benjamin will be able to read it. Upon receipt of Ameenah's email, Benjamin can only decrypt that message using the private key file (which he keeps secret) paired with his public one. Benjamin is then able to respond securely to Ameenah by using her public key to encrypt a message that only she can read. Of course, in many systems this kind of exchange takes place without the awareness or active participation of users themselves: public key cryptography underpins a vast range of modern communications security systems—from PGP to the key exchange and authentication mechanisms of Transport Layer Security (TLS).

Cryptography plays a role in almost every conceivable application of modern electronic communications technology: it secures web traffic, maintains the confidentiality of files on a network, and protects electronic banking systems, for example. Encryption technology takes many forms, and is used both to secure data against interception as it travels over a network ("in transit") and from being

8. Rijmenants, *supra* note 7.
9. The Diffie-Hellman exchange was a secure public key exchange method first published in 1976, and RSA was one of the first public-key cryptosystems (and it continues to be widely used). They originated from, respectively, Whitfield Diffie & Martin E Hellman, "New Directions in Cryptography" (1976) 22:6 IEEE Transactions on Information Theory 644; Ron L Rivest, Adi Shamir & Leonard Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems" (1978) 21:2 Communications of the ACM 120.
10. Schneier, *Applied Cryptography*, *supra* note 3 at 4.
11. See the description of Phil Zimmerman's "Pretty Good Privacy" in Schneier, *Applied Cryptography*, *supra* note 3 at 584-85.

compromised while stored ("at rest") on physical device (like a USB drive, laptop, or mobile device). Different legal and practical implications follow depending on which party applies the encryption and controls the private key or the mechanism (such as a passphrase) from which it is derived. Some service providers choose to design communications systems so that they retain the ability to decrypt their users' data. For example, data transmitted between a user's phone and a social media company's servers may be both encrypted in transit and encrypted at rest on the company's servers. But so long as the company retains the ability to decrypt that information—for example, in order to conduct analytics, to provide more personally targeted advertising, to otherwise monetize the data, or because the firm is required to do so by law—the secrecy of the information continues to depend, on some level, on choices made or risks faced by the intermediary. By contrast, many communications systems are now designed such that *only* the sender and the intended receiver are able to access the plaintext version of the message, a model known as *end-to-end encryption*. As a result, when Ameenah and Benjamin use an end-to-end messaging application like Signal,[12] their private keys never leave their respective devices. A message can be encrypted for Benjamin on Ameenah's phone, and decrypted by Benjamin on his phone, but there is no third party—including Signal's developers—with the power to access that message.[13] End-to-end encryption has become the standard for other popular mobile messaging applications such as iMessage and WhatsApp, preventing third parties—including law enforcement and intelligence agencies—from intercepting users' private communications.

While modern cryptographic systems have become increasingly sophisticated, their security continues to rely on the same basic mathematical principle: the ciphertext becomes exponentially more difficult to decrypt as the length of a key increases.[14] Cryptosystems are meant to be designed in conformity with what is known as Kerckhoffs' Principle, such that they remain secure even if everything about how they work—except the private key—is publicly known and known by the adversary.[15] This is the case for all modern encryption systems: they are secure because the number of possible keys is unfathomably large and almost computationally impossible to guess—not because there is any particular secrecy

12. Signal, Open Whisper Systems, online: <signal.org>.
13. In fact, companies like Signal often go to great lengths to design systems such that they limit the exposure of user data. See *e.g.* Letter from Brett Max Kaufman to Special Agent Tracy J Minnich (14 July 2016) on Open Whisper Systems (Signal), online: <signal.org/bigbrother/documents/2016-10-04-eastern-virginia-subpoena-response.pdf>.
14. Schneier, *Applied Cryptography*, *supra* note 3 at 352.
15. Auguste Kerckhoffs, "La cryptographie militaire" (1883) 9 J des Sciences Militaires 5 at 12.

in their design. To provide a sense of scale, the Advanced Encryption Standard (AES) encrypts data by applying a series of substitutions and permutations to 128-bit blocks of plaintext using 128, 192, or 256-bit keys.[16] A 256-bit key has approximately 1077 potential combinations, a number only slightly smaller than the number of atoms in the observable universe. Even using a powerful supercomputer, attempting to guess the key to an AES-encrypted message through brute force would take in the order of millions of billions of years.[17] As Bruce Schneier has explained, "there is an enormous inherent mathematical advantage in encrypting versus trying to break encryption," rendering defence "so much easier than attack that attack is basically impossible."[18] This mathematical truth is what makes encryption such an extraordinary problem for the law.

II. ENCRYPTION AND THE STATE

"Cryptography rearranges power," explains Philip Rogaway, "it configures who can do what, from what. This makes cryptography an inherently political tool."[19] As discussed in Part I, revealing the plaintext form of a properly encrypted message, file, or device is a practical impossibility without the right secret key. As a result, while the state can (and does) exploit other vulnerabilities in networks, computers, and people, it cannot practically circumvent modern encryption using brute force alone. In principle, properly implemented strong cryptography therefore allows the possibility for information to exist entirely beyond the reach of law enforcement and intelligence agencies.

Consequently, encryption raises certain philosophical problems: even in liberal democracies, the idea of a space entirely beyond government control sits poorly with courts and policymakers. This is in part because cryptography is math, and is therefore functionally agnostic: it secures the information of activists, lawyers, financial institutions, and politicians in precisely the same way as it does for child predators and terrorists. In doing so, encryption frustrates the work of law enforcement and national security agencies that seek to use

16. United States National Institute of Standards and Technology for Federal Information Processing Standards Publication 197, "Announcing the Advanced Encryption Standard (AES)" (26 November 2001), online: <csrc.nist.gov/publications/fips/fips197/fips-197.pdf>.
17. Schneier, *Applied Cryptography*, *supra* note 3 at 151.
18. Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (New York: WW Norton, 2015) at 344.
19. Phillip Rogaway, "The Moral Character of Cryptographic Work" (Essay delivered as the IACR Distinguished Lecture at Asiacrypt, Auckland, New Zealand, 2 December 2015) at 1, online: <web.cs.ucdavis.edu/~rogaway/papers/moral-fn.pdf> [emphasis omitted].

private information stored on devices or communicated in transit as evidence or intelligence. For example, law enforcement may face challenges in accessing evidence stored on an encrypted hard drive, on the servers of an intermediary, or in encrypted text messages between an accused person and a third party. Encrypted voice calls between persons of interest may make a traditional wiretap futile, and encrypted web traffic will prevent an individual's online activities from being monitored or analyzed. Courts and legislators have been (and will continue to be) called upon to provide "solutions" to these problems, confronting complex issues of constitutional law and human rights in the process.[20]

Over the last forty years, states worldwide have introduced a constellation of legal and policy responses in response to the challenges raised by encryption technology, including both legal measures and covert practices. These practices include: (1) controlling and restricting the public use, distribution, and export of encryption technology; (2) compelling, persuading, or enlisting commercial actors, academics, and others in efforts to weaken consumer software, publicly available encryption tools, and encryption standards in order to facilitate government access to data, whether systematically or on a case-by-case basis; (3) compelling service providers to surrender the unencrypted form of otherwise encrypted information or devices, or to give up control of a secret key (or the mechanism from which that key is derived, such as a password) in order to allow government authorities to decrypt the data themselves; or (4) compelling or requiring individuals to surrender the unencrypted form of otherwise encrypted information or devices, or to give up control of a secret key (or the mechanism from which that key is derived, such as a password) in order to allow government authorities decrypt the data themselves.

Beginning in the 1970s, the emergence of public key cryptography represented the first challenge to "government's longstanding domestic monopoly on the use of electronic ciphers and its ability to prevent encryption from spreading around

20. For a more detailed analysis of this history and these legal issues in Canada, see Lex Gill, Tamir Israel & Christopher Parsons, "Shining a Light on the Encryption Debate: A Canadian Field Guide" (May 2018) Joint Research Publication, The Citizen Lab (University of Toronto) and the Canadian Internet Policy and Public Interest Clinic (University of Ottawa), online <citizenlab.ca/wp-content/uploads/2018/05/Shining-A-Light-Encryption-CitLab-CIPPIC.pdf>.

the world."[21] By the early 1990s, however, digital technology had become so ubiquitous that legislators, law enforcement, and intelligence agencies began to perceive the widespread use of cryptographic tools as a significant threat. This anxiety resulted in a White House proposal for a device called the "Clipper Chip"—the first public attempt to mandate the insertion of what is often referred to as a government *backdoor* into the devices of ordinary consumers.[22] The Clipper Chip relied on a system of *key escrow,* wherein the government proposed to securely store a copy of each chip's unique key, and used a classified encryption algorithm intended to allow the public some of the commercial benefits of modern encryption while affording law enforcement and intelligence agencies the ability to access information in plaintext form. The proposal raised a host of privacy and civil liberties concerns, and involved serious vulnerabilities baked into its design: the consensus among security researchers was that there was no way to implement a key escrow system without fundamentally compromising user security.[23] The Clipper Chip was ultimately rejected following widespread public mobilization, as were subsequent attempts to revive key escrow.[24]

During the same era, the United States government became increasingly concerned that encryption technology would be used overseas in ways that compromised American interests. To manage the spread of cryptographic tools, "all products using encryption were controlled under the International Traffic in Arms Regulations (ITAR) and listed on the U.S. Munitions List (USML)" until 1996.[25] These controls limited the availability of high-quality cryptographic tools outside the United States, and in some cases criminalized researchers and computer scientists who ran afoul of export regulations (for example, by uploading cryptographic algorithms to the Internet).[26] This battle played out in a series of court cases in which the courts found that the distribution of cryptographic

21. Danielle Kehl, Andi Wilson & Kevin Bankston, "Doomed to Repeat History? Lessons from the Crypto Wars of the 1990s" (June 2015) Open Technology Institute Cybersecurity Initiative at 3, online: New America <static.newamerica.org/attachments/3407-doomed-to-repeat-history-lessons-from-the-crypto-wars-of-the-1990s/Crypto%20Wars_ReDo.7cb491837ac541709797bdf868d37f52.pdf>.
22. *Ibid* at 5.
23. *Ibid* at 11; see also Hal Abelson et al, "The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption" (27 May 1997), online: Columbia University Academic Commons <hdl.handle.net/10022/AC:P:9130>.
24. Kehl, Wilson & Bankston, *supra* note 21 at 7-8.
25. *Ibid* at 12.
26. *Ibid*.

source code was subject to First Amendment protection.[27] Throughout the late 1990s export restrictions were gradually relaxed, largely due to pressure from industry actors frustrated by the need to create weakened, export-grade versions of commercial software, as well as to concerns that the regulations would ultimately compromise the ability of American technology firms to compete in a global market.[28] The last of the major restrictions were reversed by early 2000, marking the end of what had come to be known as the "Crypto Wars."[29]

However, the battle over the future of encryption technology was far from over. Beginning in the 1990s, attempts to draft an international "Internet Bill of Rights" have consistently recognized an explicit right to use encryption,[30] which is curious if only because encryption is so explicitly teased out from other rights it enables (such as freedom of expression, privacy, and security). In 2006 the Association for Progressive Communications (APC) wrote that "people communicating on the Internet must have the right to use tools which encode messages to ensure secure, private and anonymous communication," and in 2014, a coalition based at the United Nations Internet Governance Forum (IGF) set forth that "everyone has the right to use encryption technology to ensure secure, private and anonymous communication."[31] These declarations are but one indication that encryption continues to occupy a central place in the minds of those working toward human rights, including freedom of expression and privacy, in the digital sphere. Indeed, in many countries, public use of encryption products remains greatly restricted or simply banned outright. In places like China, India, Senegal, Egypt, and Pakistan, access to encryption tools remains highly controlled or even criminalized, and even where it is allowed, government

27. Annette Vee, "Text, Speech, Machine: Metaphors for Computer Code in the Law" (2012) 2 Computational Culture, online: <computationalculture.net/article/text-speech-machine-metaphors-for-computer-code-in-the-law>. See especially *Bernstein v United States Department of State*, 922 F Supp 1426 (ND Cal 1996) [*Bernstein*].
28. Kehl, Wilson & Bankston, *supra* note 21 at 14.
29. *Ibid* at 17.
30. See Lex Gill, Dennis Redeker & Urs Gasser, "Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights," Berkman Klein Center for Internet & Society Research Publication No 2015-15 (Cambridge, Mass: Harvard University, 2015) at 2, online: <ssrn.com/abstract=2687120>.
31. Association for Progressive Communications (APC), *Internet Rights Charter* (Johannesburg: APC, 2006); The Internet Rights and Principles Coalition (IGF), *Charter of Human Rights and Principles for the Internet* (United Nations: IGF, 2014).

agencies nevertheless maintain "overall authority to review and approve all standards, techniques, systems and equipment."[32]

In Canada, the United States, and much of the west, a choice has generally been made to avoid imposing legal obligations on service providers that would require them to design weaknesses into their software that would facilitate government access to encrypted data (*i.e.*, "backdoors"). As a result, governments have generally had to find ways to make individuals reveal encrypted data themselves on a case-by-case basis—either by compelling surrender of their private key or by compelling them to decrypt the data personally. In the United Kingdom for example, since 2007 Part III of the *Regulation of Investigatory Powers Act* (IPA) has given various actors (from judges to high-level police and border authorities) both the power to compel decryption and to criminally charge individuals for non-compliance.[33] The IPA gives those actors authority to compel decryption in three broad circumstances: "in the interests of national security, for the purpose of preventing or detecting crime, or in the interests of the economic well-being of the United Kingdom."[34]

In the United States and Canada by contrast, no equivalent statutory power to compel decryption exists. Instead, because decrypting a device usually involves the surrender of a password or passphrase (which only exist in the defendant's mind), attempts to compel decryption have generally been found to engage the defendant's right against self-incrimination, with certain exceptions. In the United States, Fifth Amendment protection arises in the case of (1) testimonial disclosure which is (2) compelled and (3) which could result in criminal liability.[35] While there is no US Supreme Court jurisprudence yet on this particular issue, following a careful review of existing case law the Congressional Research Service concluded that "there is a strong argument that the Fifth Amendment would bar the government from compelling an individual to disclose his passcode to the government."[36] What constitutes "testimonial disclosure" has invariably become a problem of metaphor, however, as will be discussed in greater detail in Part V.

---

32. Article 19, *Right to Online Anonymity: Policy Brief* (London: Article 19, 2015) at 29-30, online: <www.article19.org/data/files/medialibrary/38006/Anonymity_and_encryption_report_A5_final-web.pdf> [Article 19].
33. *Regulation of Investigatory Powers Act 2000* (UK), c 23, ss 49-56 [*RIPA*].
34. *Ibid*, s 32.
35. Brendan M Palfreyman, "Lessons from the British and American Approaches to Compelled Decryption" (2009) 75:1 Brook L Rev 345 at 354.
36. United States Congressional Research Service, "Encryption: Select Legal Issues," by Richard M Thomson II & Chris Jaikaran, Report No 7-5700 (CRS, 3 March 2016) at 12.

Canada's position on the issue can be traced back as far as 1998, when John Manley (then Minister of Industry) claimed that "warrants and assistance orders also apply to situations where encryption is encountered," though this position seems to have been later abandoned and "is not supported by any case studies, proposed or passed legislation, or case law in Canada."[37] The Supreme Court of Canada has yet to address the problem directly, though there are a few criminal cases in which the accused's right to refuse provision of a password appears to have been taken for granted. In *R v Boudreau-Fontaine*, the most relevant appellate case to the compelled decryption issue in Canada, the Court of Appeal of Quebec found that police who had ordered a man to enter his laptop password as part of an investigation into the breach of his probation conditions violated his right to silence, his "right to be presumed innocent, the right not to be conscripted against oneself, and the protection against self-incrimination."[38] As in the United States, the question of whether being forced to disclose a private key or to decrypt a device would garner the same protection against self-incrimination as traditional testimony under the *Charter* depends on whether a key can be properly characterized as "testimonial" in nature.[39] In the most thorough Canadian article on the subject, Nicole Dalla Guarda has argued that it likely would—and moreover that the centrality of the right against self-incrimination to Canadian law makes it unlikely that compelled decryption, "either through the conduct of state actors or through legislation, could ever be justified under ss. 1 or 24(2) of the Charter."[40]

Notably in *R v Fearon*—a case concerning the warrantless search of cell phones incidental to arrest—the Supreme Court appeared to reject the idea that whether a phone is password-protected should have a significant bearing on its user's expectation of privacy.[41] While the problem goes beyond the scope of this article, it is worth stating that digital technology raises a curious legal question about how to characterize the relationship between the protection against unreasonable search and seizure and the rights to silence and against

37. N Dalla Guarda, "Digital Encryption and the Freedom from Self-Incrimination: Implications for the Future of Canadian Criminal Investigations and Prosecutions" (2014) 61:1 Crim LQ 119 at 121; Industry Canada, "Canada's Cryptographic Policy: Speaking Notes for the Honourable John Manley Minister of Industry to the National Press Club" (1 October 1998), online: <www.ic.gc.ca/eic/site/ ecic-ceac.nsf/eng/gv00119.html>.
38. *R c Boudreau-Fontaine*, 2010 QCCA 1108 at para 39, 93 WCB (2d) 47.
39. Guarda, *supra* note 37 at 124, 133.
40. *Ibid* at 137.
41. *R v Fearon*, 2014 SCC 77 at para 53, [2014] 3 SCR 621 (demonstrating that because the phone was not password-protected in this case, the issue remained unexplored).

self-incrimination. The result is that it may not be immediately obvious how an individual's reasonable expectation of privacy over a device should alter the scope of their rights as an accused person, if at all.[42] In any case, it is sufficient to state that the Canadian position on compelled decryption remains somewhat unfixed, and the limited American jurisprudence has suggested a narrowing tendency.

Beyond the possibility of compelled decryption on a case-by-case basis, technological change has increased the perceived urgency of the encryption debate, and provoked a renewed calls in western countries for government "backdoors" or "lawful access" schemes. Whereas in the past, the use of encryption tended to require the intentional deployment of specialized software, large-scale commercial implementation of strong cryptography has now become standard practice in securing web traffic, instant messaging, and physical devices such as mobile phones and hard drives. As a result, where law enforcement and other state agencies had previously been able to access or intercept with relative ease plaintext data and communications between parties (whether lawfully or not), the widespread proliferation of strong encryption has made that task increasingly difficult. Following the 2013 Snowden disclosures regarding the National Security Agency (NSA)'s domestic electronic surveillance activities, many technology companies doubled down on efforts to secure their products from eavesdroppers, including both criminals and governments alike.

In response, a new government narrative has emerged which employs the rhetorical shorthand of "Going Dark."[43] Its proponents argue that strong encryption compromises both legitimate intelligence-gathering activities and law enforcement's ability to secure evidence in criminal investigations. Others have sought to reassure political leadership regarding the risk of cold cases, claiming that—to the contrary—we now live in a "golden age of surveillance."[44] Peter Swire

---

42. See the discussion on the inverse question in *R v Jones*, 2017 SCC 60 at paras 16-34, [2017] 2 SCR 696.
43. See Valeria Caproni, "Going Dark: Lawful Electronic Surveillance in the Face of New Technologies" (Statement before the House Judiciary Committee, Subcommittee on Crime, Terrorism, and Homeland Security, Washington, DC, 17 February 2011), online: <archives.fbi.gov/archives/news/testimony/going-dark-lawful-electronic-surveillance-in-the-face-of-new-technologies>.
44. Matt Olsen, Bruce Schneier & Jonathan Zittrain, *Don't Panic: Making Progress on the "Going Dark" Debate* (Berkman Center for Internet & Society, Harvard University, 2016) at 9-15, online: <cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf>; Peter Swire & Kenesa Ahmad, *"Going Dark" Versus a "Golden Age of Surveillance"* (Stanford Center for Democracy & Technology, 2011), online: <web.archive.org/web/20120108160041/https://www.cdt.org/blogs/2811going-dark-versus-golden-age-surveillance>.

has argued that even where encryption has resulted in a loss of access to specific information in specific contexts, those losses are more than offset by massive gains in the form of new material never before available to law enforcement.[45] Rogaway has described the "Going Dark" narrative as "a brilliant discourse of fear: fear of crime; fear of losing our parents' protection; even fear of the dark," and has advanced a competing set of propositions rooted in a surveillance studies framework.[46]

Nevertheless, recent technological developments emerging alongside this narrative have reignited calls for encryption backdoors from major political figures in the United States, including one in the form of an ill-fated legislative proposal from US Senators Burr and Feinstein.[47] The legal dispute concerning a court's ability to compel Apple (under the *All Writs Act*) to assist in the decryption of a device in the FBI's possession[48] was an attempt to circumvent encryption through judicial means instead.[49] Intelligence agencies in the United States and the United Kingdom have also covertly sought to insert backdoors into commercial encryption software, and have lobbied bodies such as the National Institute of Standards and Technology (NIST) to introduce weak links into public encryption standards[50] (Canada's Communications Security Establishment (CSE) has assisted in similar efforts).[51]In Canada, the federal government conducted two major public consultations in the fall of 2016, one on cybersecurity and another

45. Swire & Ahmad, *supra* note 44 at 4.
46. Rogaway, *supra* note 19 at 26.
47. Dianne Feinstein, "Intelligence Committee Leaders Release Discussion Draft of Encryption Bill" (13 April 2016), online: <www.feinstein.senate.gov/public/index.cfm/press-releases?ID=EA927EA1-E098-4E62-8E61-DF55CBAC1649>.
48. *In re An Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300*, 2016 US Lexis 20543 (CD Cal).
49. For a thorough legal analysis of both of these developments, see Thomson & Jaikaran, *supra* note 36.
50. Association for Progressive Communications, "The right to freedom of expression and the use of encryption and anonymity in digital communications" (2015) Submission to the United Nations Special Rapporteur on the Right to Freedom of Opinion and Expression at 11, online: <www.ohchr.org/Documents/Issues/Opinion/Communications/AssociationForProgressiveCommunication.pdf>; James Ball, Julian Borger & Glenn Greenwald, "Revealed: how US and UK spy agencies defeat internet privacy and security," *The Guardian* (6 September 2013), online: <www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security>.
51. See Christopher Parsons & Tamir Israel, "Canada's Quiet History of Weakening Communications Encryption," Telecom Transparency Project and Canadian Internet Policy and Public Interest Clinic (7 August 2015), online: <www.telecomtransparency.org/canadas-quiet-history-of-weakening-communications-encryption>.

on national security. The former identified encryption as a major challenge facing law enforcement,[52] and the latter, while billed as an attempt to reform some of the more controversial aspects of the *Anti-terrorism Act, 2015* (former Bill C-51), dedicated an entire section of its accompanying background paper to the perceived need for new lawful access powers, including the ability to circumvent encryption. While the paper appeared to acknowledge that neither the power to compel an individual nor an intermediary to decrypt data currently exists in Canadian law, it failed to illuminate the government's perspective vis-*à*-vis the potential *Charter* issues such powers could raise.[53] In short, from recent legislative proposals in the United States to the ongoing national security consultation in Canada, any potential "right" to encryption is far from won—and in that battle, metaphor remains a persuasive weapon.

III. METAPHOR AND THE LAW

There is a rich body of literature examining the relationship between metaphor and cognition, much of which finds its intellectual roots in George Lakoff and Mark Johnson's seminal work *Metaphors We Live By*. Lakoff and Johnson argued that metaphors go beyond mere aesthetic, idiomatic, or descriptive tools, and that they "have the power to define reality."[54] Metaphors simultaneously shape and reproduce the ways in which we understand the world around us, and guide our ability to navigate shared meaning within it. They create cognitive bridges between disparate subjects, mapping existing knowledge about a familiar and concrete source domain onto unfamiliar, abstract, or novel concepts.[55] This unconscious capacity to transpose old cognitive models onto new subjects is

52. Public Safety Canada, "Security and Prosperity in the Digital Age: Consulting on Canada's Approach to Cyber Security," Consultation Workbook (Ottawa: Public Safety Canada, 2016), online: <www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-scrty-prsprty/index-en.aspx>.
53. Public Safety Canada, "Our Security, Our Rights: National Security Green Paper," Background Document (Ottawa: Public Safety Canada, 2016) at 55, online: <www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-scrt-grn-ppr-2016-bckgrndr/ntnl-scrt-grn-ppr-2016-bckgrndr-en.pdf>.
54. George Lakoff & Mark Johnson, *Metaphors We Live By*, 2nd ed (Chicago: University of Chicago Press, 2003) at 157.
55. Cornelius Puschmann & Jean Burgess, "Metaphors of Big Data" (2014) 8 Intl J Comm 1690 at 1696.

a fundamental component of human reasoning; cognitive scientist Douglas Hofstadter has called analogy "the very blue that fills the whole sky of cognition."[56]

Yet the metaphors we use in law are far from neutral. To the contrary, they are emotionally and ideologically loaded devices with extraordinary normative force, with the power to "help the imaginary become real or true."[57] The strategic deployment of a conceptual metaphor may subtly move the goalposts of a given argument, or it may change the game entirely, by obfuscating certain characteristics and emphasizing others.[58] In the words of Sara Watson, metaphors "prime us to take for granted the ways we think about things," allowing us to alter the terms of a debate and rewrite the rules of political possibility.[59] Metaphors reconfigure meaning.

There is perhaps no context where this is more apparent than in the language of the law. In *Legal Fictions*, Lon Fuller famously wrote that "metaphor is the traditional device of persuasion," and that in its absence, the law's "power to convince and convert" is fatally compromised.[60] Legal reasoning works explicitly by adapting old principles to novel facts: it operates through analogy, by way of precedent. The law is also highly conceptual, with an internal logic that tends to divorce words from their ordinary meanings, elevating them to abstract and even metaphysical categories. These categories have boundaries, but those are neither immediately apparent from the view of common sense nor fixed across time. Law needs metaphor, because everything new is folded into the law by reference to that which came before.

One type of "legal fiction" described by Fuller are those rhetorical devices that we know to be "false statements," but which are nevertheless "recognized as having utility."[61] We adopt these falsehoods because they are expedient, provide some functional benefit, or serve to preserve the internal coherence of the law. For example, whether in the common or civil law tradition, one of the most powerful

---

56. Douglas R Hofstadter, "Epilogue: Analogy as the Core of Cognition" in Dedre Gentner, Keith J Holyoak & Boicho N Kokinov, eds, *The Analogical Mind: Perspectives from Cognitive Science* (Cambridge: MIT Press, 2001) 499 at 499, quoted in Kailash Awati & Simon Buckingham Shum, "Big Data Metaphors We Live By," *Medium* (14 May 2015), online: <medium.com/@kailashawati/big-data-metaphors-we-live-by-98d3fa44ebf8#.jkzvkjuh5>.
57. Sally Wyatt, "Danger! Metaphors at Work in Economics, Geophysiology, and the Internet" (2004) 29:2 Sci Tech & Human Values 242 at 244.
58. Jonas Ebbesson, "Law, Power and Language: Beware of Metaphors" (2008) 53 Scandinavian Stud L 259 at 260.
59. Sara M Watson, "Data is the New '___'," Dis Magazine (2018), online: <dismagazine.com/discussion/73298/sara-m-watson-metaphors-of-big-data>.
60. Lon L Fuller, "Legal Fictions" (1930) 25:4 Ill L Rev 363, 513 & 877 at 380.
61. *Ibid* at 369.

legal categories we have is that of personhood, to which the law has decided certain rights and obligations may attach that do not attach to non-persons. The construct of legal personhood is what allows us to accept that a corporate entity 'is' a person for the law's purposes, and by extension to accept that it has special characteristics, such as the ability to make legally recognizable decisions, to own and owe property, and to exercise certain rights.[62] Yet we know that the boundaries for inclusion in the legal category of 'personhood' are neither fixed nor rooted in some kind of objective external reality. Battles over the abolition of slavery and toward women's suffrage have often been framed as exercises toward a redefinition of 'personhood' in the law. Legal questions regarding the precise moment a fetus becomes a "person" or whether corporate "persons" have the same rights (such as political speech) as flesh-and-blood persons are similarly illustrative. Metaphors are therefore instrumental in negotiating the boundary points of legal category, and in so doing they both reconfigure and distort relationships, rights, obligations, and identities.

The metaphors chosen by a court or legislature will effectively determine the validity of certain arguments, delimit the boundaries of acceptable debate, and reshape what we understand to be both "logical" and legal in a given situation. Yet there is also a risk that over time the fact that a term is metaphor at all becomes less apparent, allowing a concept to gradually shift from intellectual shorthand to established truth. As Stefan Larsson writes,

> When the metaphors are not perceived as metaphors, the conceptions behind will be perceived as the only possible alternative for the purpose of a given regulation. Any attempted revisionary arguments will then be framed within the prevailing conception, no matter what arguments are produced. …. This means that legal decisions, as well as legislation, are framed and conceptualized in a particular way without us even seeing alternative frames or conceptualizations.[63]

In other words, the more entrenched a metaphor is, the more difficult its underlying assumptions are to challenge or uproot. As Fuller wrote, the mind is willing to go to great lengths "to preserve a comforting and persuasive analogy."[64]

---

62. Ebbesson, *supra* note 58 at 262.
63. Stefan Larsson, "Metaphors, Law and Digital Phenomena: The Swedish Pirate Bay Court Case" (2013) 21:4 Intl JL & IT 354 at 366 [Larsson, "Pirate Bay"].
64. Fuller, *supra* note 60 at 382.

IV. METAPHOR AND TECHNOLOGY

Metaphor plays a special role for the law wherever technology is concerned, for at least two reasons. The first is that the pace of legal change lags far behind that at which technology develops, and as such both courts and policymakers have little choice but to adopt a reactive stance. In this way, metaphor provides a critical shorthand, narrowing the gap between the world in which we live in and the world for which the law was written. "The most typical way this happens," explain Tim Hwang and Karen Levy, "is that judges and regulators think about whether a new, unregulated technology is sufficiently like an existing thing that we already have rules about," and then transpose the existing conceptual framework onto the unregulated phenomenon.[65] In other words, metaphor offers a powerful conceptual "bridge" to transition between old and new in the law.[66]

The second reason for the special role of legal metaphor where new technology is concerned is the fact that, as Judith Donath explains, "information is fairly formless"—and as such, aspects of the digital environment may demand a greater degree of metaphor than more material legal subjects.[67] Larsson explains how those formless technological experiences are translated into a materially recognizable cognitive object using the term *skeumorph* (the "reuse of old concepts for new phenomena"), using words and iconography that bind physical letters to email, film photography to pixelated imagery, and so on.[68] When the law is faced with a problem that has a complex technical dimension, Larsson explains that we are often faced with countless "skeumorphic" terms. He provides the example of copyright litigation over The Pirate Bay, a website which "is found in a 'domain' name, relying on 'torrents' to be found by a search 'engine,' taking place in a 'swarm' and has nowadays moved into using 'magnet' 'links.'"[69] The formless quality of the digital space means that "we are inevitably surrendering to a conceptual reuse that is massive."[70] As a result, communicating the salient aspects of a given technical reality to a courtroom or legislature may become an

---

65. Tim Hwang & Karen Levy, "'The Cloud' and Other Dangerous Metaphors," *The Atlantic* (20 January 2015), online: <www.theatlantic.com/technology/archive/2015/01/the-cloud-and-other-dangerous-metaphors/384518/>.
66. Stefan Larsson, *Metaphors and Norms: Understanding Copyright Law in a Digital Society*, vol 36 (Lund: Lund University Press, 2011) at 101 [Larsson, "Metaphors and Norms"].
67. Josh Dzieza, "A History of Metaphors for the Internet," *The Verge* (20 August 2014), online: <www.theverge.com/2014/8/20/6046003/a-history-of-metaphors-for-the-internet>.
68. Larsson, "Pirate Bay," *supra* note 63 at 355, 362.
69. *Ibid* at 363.
70. *Ibid*.

act of double or even triple translation. Metaphor, while imperfect, provides a common language.

Some would argue that the whole history of technology law is a history of metaphor. After all, the conceptual infrastructure of North American telecommunications law has its roots in legal principles that were drawn by analogy from railway regulation and interstate commerce—ideas which themselves originated in even earlier technologies and earlier analogies.[71] Harmeet Sawhney, Venkata Ratnadeep Suri, and Hyangsun Lee explain how the same framework captured by the US *Interstate Commerce Act* was applied for all subsequent "point to point technologies" involving the flow of materials and information, including "petroleum pipelines, trucking, civil aviation, and telecommunications"—breaking down only with the advent of broadcast media.[72] The way they describe this process over time is highly illustrative:

> In the first-order stretching somewhat forced connections are made between technologies. For instance, radio was linked to railroads via the telegraph and telephone connections. In other words, it would have been difficult to establish a connection between railroads and radio because there is little similarity between them. The telegraph and telephone allowed for the establishment of this connection because they were similar to railroads and also to radio but in different ways. The similarities between railroads and telegraph and telephone networks are rather immediate because they all are composed of nodes and links. On the other hand, the similarities between telegraph and telephone networks and radio rest on the fact they are electronic means of communication. The telegraph and telephone served as intermediaries in linking railroads to radio. This stretched framework functioned as long the new technology was employed in ways that mimicked the old one.[73]

There are countless instances where metaphor has shaped the law's understanding of a new technology, and the political implications of those choices have been profound—particularly since the advent of the Internet. The term "cyberspace" itself is deeply metaphorical, and was originally coined by William Gibson in a work of science fiction (he called it "a consensual hallucination").[74] Cyberspace invokes a shared virtual geography, a dimension of spatiality, of place. But if what happens on the Internet occurs within a discrete

---

71. Harmeet Sawhney, Venkata Ratnadeep Suri & Hyangsun Lee, "New Technologies and the Law: Precedents via Metaphors" (2010) 2:3 Eur J Leg Stud 38.
72. *Ibid* at 39.
73. *Ibid* at 47.
74. William Gibson, *Neuromancer* (London: Harper Collins, 1984). See also Mark Graham, "Geography/Internet: Ethereal Alternate Dimensions of Cyberspace or Grounded Augmented Realities?" (2013) 179:2 Geographical J 177 at 180.

"place," what kind of place is it? What are its topological features? Who belongs there, who controls it, and where are its borders?[75] Mark Graham has explained cyberspace as being "conceived of as both an ethereal alternate dimension which is simultaneously infinite and everywhere … and as fixed in a distinct location, albeit a non-physical one."[76] Others have declared that the image of a 'universal' cyberspace is a falsehood entirely, and that the Internet, unevenly distributed itself, simply reflects and reinforces existing global power relations.[77] Nevertheless, the metaphor is persistent, and its assumptions are apparent through decades of legal debate related to the exercise of jurisdiction on the Internet—a debate which arguably remains utterly unresolved in certain fundamental ways.

And if 'cyberspace' was the dominant metaphor developed and imagined by 1990s cyberpunks, its chief competitor is surely the "information superhighway"—a phrase (coined in the 1970s by Al Gore) which had a pervasive impact on early government forays into Internet regulation. In her own discussion of technological metaphor, Sally Wyatt draws her readers' attention to an article by Virginia Postrel published in a 1998 issue of *Wired* to illustrate the point.[78] In that piece, Postrel criticizes infrastructural metaphors like the "information superhighway" and "bridge[s] to the future," arguing that they embed a specific ideological agenda: that "the future must be brought under control, managed, and planned … It represents technocracy, the rule of experts."[79] The debate over net neutrality in the mid-2000s has often been retold by scholars as a similar conflict of metaphor, one perhaps most famous for the comic failure of Senator Ted Stevens's claim that the Internet was just "a series of tubes."[80] While that analogy failed to take hold, Al Gore's "superhighway" was subject to a powerful extension by Tim Wu, who first developed the principle of network neutrality by

---

75. John Perry Barlow, "A Declaration of the Independence of Cyberspace" (1996), online: <www.eff.org/cyberspace-independence>. Arguably those are the questions John Perry Barlow sought to answer when he wrote: "Governments of the Industrial World, you weary giants of flesh and steel ... You are not welcome among us. You have no sovereignty where we gather" (*ibid*).
76. Graham, *supra* note 74 at 180.
77. *Ibid* at 180.
78. Wyatt, *supra* note 57 at 251. See especially Virginia Postrel, "Technocracy R.I.P.," *Wired* (1 January 1998), online: <www.wired.com/1998/01/postrel>.
79. Postrel, *supra* note 78.
80. "Your Own Personal Internet," *Wired* (30 June 2006), online: <www.wired.com/2006/06/your-own-person>; Ed Felten, "Taking Stevens Seriously" (17 July 2006), *Freedom to Tinker* (blog), online: <freedom-to-tinker.com/blog/felten/taking-stevens-seriously>.

arguing against a system that would allow "fast lanes" and slow ones.[81] The net neutrality principle—and its corresponding metaphor of the Internet as a kind of public infrastructure—has been an important bulwark against corporate control of online expression, and an instrumental guarantor of the right to receive and impart information online.[82]

The last twenty years of digital copyright law have been similarly coloured by metaphor, where analogies to print and physical media remain stubbornly dominant despite a legal context fundamentally transformed by technology.[83] For example, The Pirate Bay has been subject to a great deal of litigation and as a consequence, a vast barrage of metaphors that aim to describe the website's function.[84] They have included terms like 'platform,' 'search engine,' 'bulletin board,' and 'assemblage'—distinct categories of Internet service subject to different kinds of treatment by the law. For example, the label of 'platform' strategically folds The Pirate Bay into an area of law that is generally reluctant to assign liability to intermediaries and service providers, whereas other terms (like 'publisher') would tend to increase the website's perceived involvement in the copyright infringing activities of its users.[85] In each of these instances, we see new ways in which metaphors "are instructive not for their realism, but for the way they direct our focus to certain social and political phenomena."[86]

Computer code itself is subject to shifting and transient conceptual metaphors which are both dependent on context and ideologically loaded. Annette Vee, for example, has analyzed the legal treatment of code in the United States by grouping it into the three interrelated categories of text, speech, and machine —which together, she argues, form "a set of ontologies for code."[87] She demonstrates that in the context of copyright law, computer

---

81. Tim Wu, "Why You Should Care About Network Neutrality," *Slate* (1 May 2006), online: <www.slate.com/articles/technology/technology/2006/05/why_you_should_care_about_network_neutrality.html>.
82. See *e.g.* Federal Communications Commission, Press Release, "Chairman Pai Circulates Draft Order to Restore Internet Freedom and Eliminate Heavy-Handed Internet Regulations" (21 November 2017), online: <apps.fcc.gov/edocs_public/attachmatch/DOC-347868A1.pdf> (in the United States, where the current administration has moved to repeal net neutrality rules, it has positioned itself in opposition to "heavy-handed" Internet regulation, "utility-style regulations," and "micromanaging the Internet" in a similar vein).
83. Larsson, "Pirate Bay," *supra* note 63 at 377.
84. *Ibid* at 368-372.
85. *Ibid*.
86. Daniel J Solove, *The Digital Person: Technology and Privacy in the Information Age* (New York: New York University Press, 2004) at 28.
87. Vee, *supra* note 27 at 1.

code's textual and literary dimensions are emphasized—whereas in the realm of patent theory, software's "functionality" and its machine-like qualities are foregrounded. Similarly, where the US government has sought to censor or criminalize code, its expressive elements have been defensively invoked to secure its constitutional protection under the First Amendment. Yet the law struggles to untangle each of these distinct stories from the other, particularly because separating the "the expressive from the functional," or "speech" from "conduct" is often impossible in computing.[88] Vee illustrates this element by pointing to the legal battle over a piece of software called DeCSS, which was popularized to circumvent restrictive digital rights management (DRM) technology. While hackers and activists reproduced the code in the form of haikus and artwork to emphasize its literary dimensions and strengthen First Amendment arguments, the entertainment lobby denounced it as a "digital crowbar."[89] Vee captures an important feature of legal metaphor in her analysis when she explains that "each legal metaphor for code offers a different paradigm for where code can go, what it can do, and who is allowed to write and circulate it."[90] She recognized that a metaphor, even once entrenched, remains context-dependent: a technical term may have entirely different semantic implications from one area of the law to another. Indeed, what computer code 'is' to the law *remains* in flux—a point comically illustrated by Jonathan Schwartz, one of Google's key witnesses in the intellectual property case *Oracle v Google*, who desperately tried to explain an Application Programming Interface (API) to a judge as though it were as an item on a breakfast menu in 2016.[91]

'The cloud' is perhaps one of the most frequently discussed technological metaphors, both due to its conceptual ubiquity and because of the commercial, political, and legal implications that flow from its popular adoption. However, it has also been subject to sustained criticism for its ability to obscure the technological infrastructure to which it refers, distorting the reader's understanding of data's physicality and locality. As the now-trite saying goes, there is no "cloud" after all, just someone else's computer—or perhaps more accurately, just someone else's "millions of hard drives, servers, routers, fiber-optic cables,

88. *Ibid* at 4.
89. *Ibid*.
90. *Ibid*.
91. Sarah Jeong, "In Oracle v. Google, a Nerd Subculture Is on Trial," *Motherboard (Vice)* (12 May 2016), online: <motherboard.vice.com/read/in-google-v-oracle-the-nerds-are-getting-owned>. See *Oracle v Google*, 750 F (3d) 1339 (Fed Cir 2014).

and networks."[92] Yet 'the cloud' imposes the model of a "single, virtual object,"[93] one which is "weightless and intentionally vague"[94] and that we understand to be "just *there,* atmospheric and part of the environment."[95] The metaphor hides the vast physical, electrical, and computational infrastructure housed in data centres overseas, just as it negates "the infrastructure of labour" enabling the existence of these digital networks.[96] Tung-Hui Hu has described the cloud as "a cultural fantasy of participation and security" which confuses and distorts traditional notions of sovereignty and jurisdiction and which "hides its physical location by design."[97] At the same time, he argues that because 'the cloud' as a metaphor obscures relationships of power, it lends itself to a covert resurgence of sovereign authority: "the cloud grafts control onto an older structure of sovereign power, much as fiber-optic networks are layered or grafted onto older networks."[98] Intuitively, the metaphor also transforms how we understand the individual: once information has been surrendered to 'the cloud,' there is a sense that it has become depersonalized, disembodied, harder to locate—it becomes somewhere else and someone else's. From distorting property law constructions of ownership and control, to reconfiguring legal tests for jurisdiction, this metaphor has legal implications.

Even beyond 'the cloud,' the world of digital metaphor is rife with references to the natural form—from bugs and viruses to webs and mice.[99] The language we have adopted to understand data seems particularly prone to these kinds of analogies. "Big data" in particular often takes the form of an unstoppable natural force: courts and the popular press alike adopt the language of data "torrents," "oceans" "deluges" "tsunamis" and "waves."[100] In those moments where the party holding the data fails to maintain control of it, we even refer to it as a 'spill' or a 'leak.' This metaphor, that "big data is a force of nature to be controlled,"[101] is meant to emphasize the enormous volume and tremendous analytical power of the information at stake, but also tends to obscure its relationship to the

92. Tung-Hui Hu, *A Prehistory of the Cloud* (Cambridge, Mass: MIT Press, 2015) at x.
93. *Ibid*.
94. Dzieza, *supra* note 67.
95. Hu, *supra* note 92 at ix.
96. *Ibid* at xii.
97. *Ibid* at xvi, 4.
98. *Ibid* at xvi.
99. See *e.g.* Sue Thomas, *Technobiophilia: Nature and Cyberspace* (New York: Bloomsbury Academic, 2013).
100. Watson, *supra* note 59.
101. Puschmann & Burgess, *supra* note 55 at 1698.

human beings who collect, manage, and exploit it. As Deborah Lupton explains, these words "suggest an economy of digital data and surveillance in which data are collected constantly and move from site to site in ways that cannot easily themselves be monitored, measured or regulated."[102]

A close link is the image of data as a resource to be extracted from the natural world and transformed, exploited, and monetized.[103] It is what Cornelius Puschmann and Jean Burgess describe as the "nourishment/fuel to be consumed" metaphor of big data.[104] These industrial analogies, like data 'mining,' 'refining,' and 'raw data'—along with declarations in the popular press announcing that "data is the new oil"[105]—suggest the need for large-scale processing.[106] More troublingly, they divorce data from the very human beings from which it originates, transforming its analysis into a commercial activity that can be "obscured, specialized, and distanced" from public scrutiny.[107] Following the Snowden revelations, these same patterns were mirrored in words used to describe government surveillance, signaling the exploitation of a natural resource (sweep, harvest, gather, scoop, glean, pluck, trap) and evoking the language of industry (mine, dig, burrow).[108] Nautical themes (dragnet, trawling, tentacles, harbour, net, inundated, leviathan) and biological and medical elements (hemorrhaging, implanting, infect, ingest, inject, stethoscopic) also featured prominently when public discourse around surveillance was analyzed.[109] Yet in the face of the enormous privacy and civil liberties implications of big data analytics, the natural resource metaphor in particular has become a lightning rod for criticism. As Hwang and Levy have written:

> Just as the history of resource exploitation in America—from westward expansion through the Gold Rush, and beyond into modern-day debates about water and

---

102. Deborah Lupton, "Swimming or drowning in the data ocean? Thoughts on the metaphors of big data" (29 October 2013), *This Sociological Life* (blog), online: <simplysociology.wordpress.com/2013/10/29/swimming-or-drowning-in-the-data-ocean-thoughts-on-the-metaphors-of-big-data>.
103. Puschmann & Burgess, *supra* note 55 at 1698.
104. *Ibid* at 1700.
105. Watson, *supra* note 59.
106. *Ibid*.
107. *Ibid*.
108. Deji Bryce Olukotun, "Sweep, Harvest, Gather: Mapping Metaphors to Fight Surveillance," *The Millions* (10 April 2014), online: <themillions.com/2014/04/sweep-harvest-gather-mapping-metaphors-to-fight-surveillance.html>.
109. Julia Fleischaker, "Mapping the language we use to describe surveillance," *Melville House* (11 April 2014), online: <www.mhpbooks.com/mapping-the-language-we-use-to-describe-surveillance>.

> air rights—involves the appropriation of resources that belonged to someone else, online data collection policy treats personal information as a natural, inexhaustible good—ripe for exploitation in the name of economic growth and private gain.[110]

Jer Thorpe goes even further to subvert this narrative by extending it to its logical outgrowths: "where oil is composed of the compressed bodies of long-dead micro-organisms, this personal data is made from the compressed fragments of our personal lives. It is a dense condensate of our human experience."[111] By contrast, in a 2015 talk Maciej Ceglowski aimed to invert the metaphor entirely, asking listeners to "imagine data not as a pristine resource, but as a waste product, a bunch of radioactive, toxic sludge that we don't know how to handle."[112]

The examples above touch all dimensions of the law—from the philosophy of jurisdiction, to contract and intellectual property, to deep constitutional problems of privacy, freedom of expression, and the rule of law. They are presented here not merely to act as a survey of existing literature, but instead to demonstrate the force with which metaphor shapes the social, political, and legal rules assigned to particular technologies. And, while the power of metaphor to distort reality should not be overlooked, we should also avoid discounting its functional utility. As Vee explains, "whatever their function in legal discourse, metaphors can illuminate the unstable identities for technologies when they are new—before their uses become well-worn grooves through culture and communication."[113] And it is clear that the law's approach to cryptographic tools is in need of such illumination on multiple fronts. As Jeffrey Kiok explains, "there is no historical analogue that matches encryption in the constitutionally relevant ways," and the appropriate legal metaphors remain unfixed.[114]

We must exercise caution, however, because once folded into the law, what Larsson calls the "conceptual path dependence" of a metaphor becomes jurisprudentially entrenched and difficult to escape.[115] When new technologies inherit old legal metaphors, they also inherit old rules, models, and limitations. This becomes problematic where the new technology is used in or behaves in

---

110. Hwang & Levy, *supra* note 65.
111. Jer Thorpe, "Big Data Is Not the New Oil" *Harvard Business Review* (30 November 2012), online: <hbr.org/2012/11/data-humans-and-the-new-oil>.
112. Maciej Cegłowski, "Haunted by Data" (Lecture delivered at the Strata + Hadoop World Conference, New York City, 1 October 2015), online: <idlewords.com/talks/haunted_by_data.htm>.
113. Vee, *supra* note 27 at 1.
114. Jeffrey Kiok, "Missing the Metaphor: Compulsory Decryption and the Fifth Amendment" (2015) 24:1 BU PILJ 53 at 76.
115. Larsson, "Pirate Bay," *supra* note 63 at 376.

ways which could not have been anticipated by looking to that which came before. This failure to conform to the paradigm set out by the old metaphorical infrastructure can lead to a break down in the logic of the law, which Sawhney, Suri, and Lee have called "a metaphor vacuum."[116] As will be discussed in Part V below, the legal treatment of encryption technology is characterized by precisely this kind of problem.

V. THE ENCRYPTED MACHINE

As discussed in Part II**,** modern encryption raises both practical and theoretical problems in areas such as criminal evidence, national security, and constitutional law.[117] They range from fairly straightforward procedural issues to larger philosophical questions about the appropriate limits of state power. In practice of course, these questions are deeply interrelated and hard to untangle from one another.

This Part explores some of the possible metaphors which have historically been advanced to describe the process or result of encryption, but begins by offering a few thoughts on methodology. When attempting to unpack the normative implications of a given metaphor, we need to look carefully at the mechanics of its implicit arguments. How, for example, does it explain, ignore, or transform the specific component parts of the technology? If one says that "encryption is a cat," what parts of the cat make up the plaintext, the ciphertext, the key, and the act of production or technological mechanism from which that key is derived? As Vee has recognized in her study of metaphors for code, it is also essential to recognize that the law rarely settles on a singular analogy for all cases—rather, it develops various cognitive models for a given technological concept depending on its legal and factual context.[118] That choice will be shaped by the political and legal debate in which it is embedded. For example, as discussed in Part II, one of the earliest legal treatments of encryption took place in the context of arms regulation—with the underlying assumption that if encryption was a kind of weapon, it ought to be controlled as one. Later, restrictions on the distribution of cryptographic algorithms were challenged by the argument that code (including cryptographic code) had an expressive dimension which made it more like a kind of speech—protecting cryptographer Daniel Bernstein's "right to circulate his

116. Sawhney, Suri & Lee, *supra* note 71.
117. Though it also likely has a number of private law implications far beyond the scope of this article.
118. Vee, *supra* note 27.

algorithm as freely as he might 'speak' it."[119] Yet while they may have latent power and utility, neither of these two metaphors will necessarily translate perfectly to contexts beyond the debate over export controls for cryptographic products. Indeed, different fact scenarios and uses for encryption may require different metaphors entirely. For example, A. Michael Froomkin (one of the earliest writers to explore cryptographic metaphor) described four possible modes of imagining the component parts of encrypted communication—as a car, language, house, or safe.[120] Whether or not they are ultimately desirable and accurate rhetorical tools, it is possible to see how the first two may be more appropriately applied to describe the process of encryption in transit between two parties, whereas the latter two seem best positioned to describe the data at rest. Similarly, the appropriate metaphor may differ depending on the specific technical tool in question. For example, email encrypted using PGP is often distinguished from unencrypted email by comparing postcards to sealed envelopes—an idea which builds analogy on the back of existing "skeumorphic" conceptions of email as postal mail. While this metaphor may have some utility in describing a single encrypted email (though problematically, it continues to replicate the 'container' problem discussed below) it is far less appropriate to explain the nature of a hard drive with full-disk encryption, or the concept of encrypted network traffic.[121] Finally, the choice will also depend on motive. Hypothetically, law enforcement concerned about accessibility of evidence may be more concerned with cultivating metaphors that describe the paradigmatic model of an encrypted machine at rest, whereas intelligence agencies engaged in large-scale network surveillance may be inclined toward thinking about the data in transit.

In the words of Charlotte Linde, "people in power get to impose their metaphors," so we ought to look carefully at what metaphors those people choose.[122] The analogy most frequently advanced by law enforcement to describe the encrypted machine has been the idea of the device as a locked 'container,' which takes various forms depending on context. Former Federal Bureau of Investigation (FBI) Director James Comey has likely been the most persistent advocate of this metaphor, for example using the analogy of un-openable "car trunks" and "apartments" in reaction to Apple and Google's decision to

119. *Ibid* at 3 referring to *Bernstein*, *supra* note 27.
120. A Michael Froomkin, "The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution" (1995) 143:3 U Pa L Rev 709 at 861.
121. See Paul Ohm, "The Rise and Fall of Invasive ISP Surveillance" 2009:5 U Ill L Rev 1417 at 1453.
122. Lakoff & Johnson, *supra* note 54 at 157.

introduce mobile device encryption by default.[123] Comey's cognitive model for the encrypted machine hinges on the idea of devices like computers and mobile phones as enclosed physical spaces—as houses, closets, and vehicles full of evidence robbed from the hands of law enforcement.[124] Here we see certain parallels to the discussion of 'cyberspace' above, as well as to Josephine Wolff's study of the language used in computer security, in which she describes burglary as one of three core metaphors of the field.[125] She writes that

> [c]omparisons of Internet crime to burglary draw on this notion of breaking into a protected space and apply it to a domain in which both the ideas of "breaking" and "entering" have a much less physical manifestation … Many descriptions and explanations of how computer networks should be defended derive from these analogies to protecting houses against burglars and fortifying medieval castles. In many ways however, the burglar metaphor fails to provide meaningful guidance … [as] some of its central assumptions about the nature of theft and the best ways to stop burglars do not map neatly from castles onto computers.[126]

Yet this metaphorical deficit has not stopped the language of an encrypted device as box, room, or home from dominating either the public encryption debate or the courtroom rhetoric of law enforcement. In one of the hearings over the San Bernardino shooter's iPhone, Comey even proclaimed that the FBI was simply "asking Apple to take the vicious guard dog away and let us pick the lock."[127] At the same time, the narrative has been subversively adopted by critics of the policies which the 'container' metaphor otherwise tends to support. For example, the non-governmental organization Article 19 has described encryption backdoors as the equivalent of "requiring locksmiths to produce weak door locks

123. Kashmir Hill, "FBI Director says Apple and Google are Putting their Customers 'Beyond the Law,'" *Forbes* (13 October 2014), online: <www.forbes.com/sites/kashmirhill/2014/10/13/fbi-director-says-apple-and-google-are- putting-their-customers-beyond-the-law>.

124. James B Comey, "Expectations of Privacy: Balancing Liberty, Security, and Public Safety" (Address delivered at the Center for the Study of American Democracy Biennial Conference, Kenyon College, Gambier, Ohio, 6 April 2016), online: www.fbi.gov/news/speeches/expectations-of-privacy-balancing-liberty-security-and-public-safety [Comey, "Expectations of Privacy"].

125. Josephine Wolff, "Cybersecurity as Metaphor: Policy and Defense Implications of Computer Security Metaphors" (Paper delivered at the TPRC Research Conference on Communication, Information, and Internet Policy, American University, Washington College of Law, 31 March 2014) at 6, online: <papers.ssrn.com/sol3/papers.cfm?abstract_id=2418638>.

126. *Ibid*.

127. Spencer Ackerman, Sam Thelma & Danny Yadron, "Congress tells FBI that forcing Apple to unlock iPhones is 'a fool's errand,'" *The Guardian* (1 March 2016), online: <www.theguardian.com/technology/2016/mar/01/apple-fbi-congress-hearing-iphone-encryption-san-bernardino>.

and deadbolts in order to facilitate governments' access to private homes," and a coalition of cryptographers has employed the analogy of "keys under doormats."[128] Of course, 'backdoor' is itself a metaphor.

At the heart of Comey's analogy—one which has been adopted by courts and commentators alike—is the aspiration that digital and physical evidence be treated identically by the law, even where they exhibit fundamentally different characteristics.[129] As others have explained however, the container metaphor fails to represent the technical process of encrypting data. This is because, as explained in Part II, encryption does not create a 'barrier' between the outside world and the plaintext. There is no intelligible data hidden 'inside' an encrypted file or machine—rather, encryption renders data unintelligible, transformed, and rearranged by a mathematical process.[130] There can be no plaintext version of the data somehow enclosed within, because (to quote Gertrude Stein) there's no "there" there at all.

But it would be unfair to attribute this misunderstanding entirely to Comey. While the FBI's use is certainly opportunistic, the idea of 'containers' is at the heart of many so-called skeumorphs we use to understand our devices (encrypted and otherwise) on a day-to-day basis. As Kiok explains:

> The kind of language people use when talking about computers (e.g., files and folders) and the language that encryption companies often use to describe what their products "do" (e.g., creating encrypted "containers," encrypting a "file" or "folder," or using a "key" to "unlock" encrypted media) can cause people to improperly analogize how encryption software actually works.[131]

In this light, it is unsurprising that the cognitive model has a certain commonsensical resonance with judges and politicians. Nevertheless, metaphors in law and policy can be intentionally weaponized toward a specific legal purpose or vision, revealing both the "design intentions," as well as "the political assumptions and aspirations" of those who use them.[132] In this instance, the concept of device-as-container functionally serves to weaken the self-incrimination argument against compelled decryption, and perhaps to challenge certain conceptions of privacy more generally. It serves two dual functions: it obfuscates the testimonial

---

128. Article 19, *supra* note 32 at 30; Harold Abelson et al, "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications" (2015), online: <www.schneier.com/academic/paperfiles/paper-keys-under-doormats-CSAIL.pdf>.
129. See Comey, "Expectations of Privacy," *supra* note 124.
130. Kiok, *supra* note 114 at 54.
131. *Ibid* at 58.
132. Wyatt, *supra* note 57 at 244-45.

aspect of disclosing a private key, and it rejects the notion that there is any qualitative difference in the kind or scope of information stored on digital devices compared to what might otherwise be physically stored or discovered.

The images selected to substantiate the FBI's metaphor of enclosure (car, apartment, box) are not accidental: after all, Fifth Amendment protection is meant to extend only to "expression of the contents of an individual's mind," not to the contents of their glove compartment.[133] It is essential to recall that various courts, including the US Supreme Court, have determined that surrendering the key to a strongbox fails to engage one's rights against self-incrimination because it is "non-testimonial," whereas providing the combination to a locked safe (a "product of the mind") engages those rights. So, the logic follows, the more a computer is "like" a lockbox (and consequently the more a private key is "like" a physical key), the easier it will be for the state to compel an individual to decrypt a device.[134] And, while the courts in the United States may have largely accepted the argument that the disclosure of a *password* is a testimonial act, the metaphor of locked containers arguably remains the dominant narrative in public and political discourse. The narrative is emblematic of a larger worldview which struggles to tolerate the idea of space beyond the law's reach, captured by Comey's declaration that there is in fact "no such thing as absolute privacy in America. There is no place outside the reach of judicial authority."[135]

Even the 'combination safe' analogy is only an improvement insofar as it helps to capture the testimonial nature of an alphanumeric password or passphrase, "because a combination is something that is in one's mind."[136] It fails, as does the locked container analogy, to say much about whether the data we keep in combination safes (or cars or closets or boxes) is qualitatively different in any way from the kinds of things one might keep on their mobile phone or laptop. Moreover, it continues to mislead its audience in suggesting that a plaintext version continues to exist somewhere 'within' the 'safe,' replicating the same technical inaccuracies as described above.[137] The biggest problem with the safe

133. *Doe v United States*, 487 US 201 at 210 (1988) [*Doe*]. See also James Comey, "Even Our Memories Are Not Absolutely Private in America" (Address delivered at the Boston Conference on Cyber Security, Boston, 8 March 2017), online: <www.c-span.org/video/?c4662211/even-memories-absolutely-private-america-james-comey-head-fbi>. Comey is quick to point out that "even our memories are not absolutely private" in the case of immunity orders where testimony is compelled in the same speech (*ibid*).
134. Kiok, *supra* note 114 at 77; Thomson & Jaikaran, *supra* note 36 at 9.
135. Comey, "Expectations of Privacy," *supra* note 124.
136. Kiok, *supra* note 114 at 77.
137. *Ibid*.

metaphor, however, is that it maintains a "conceptual path dependence"[138] which remains fixated on the nature of the 'testimony'—*i.e.*, the act of key production, or the mechanism from which the private key is derived. That fixation serves to potentially exclude deeper questions—from the purpose of constitutional protection against self-incrimination to the scope of state power, the limits of the right to privacy, and the concept of individual liberty.

Indeed, by taking a step back, this distinction between 'testimony' and 'non-testimony' can seem arbitrary from the perspective of an outsider. For example, a 2014 decision by a Virginia court found that forcing a man to unlock a cell phone using his fingerprint failed to engage his right against self-incrimination, as the fingerprint itself was deemed 'non-testimonial.'[139] In *Doe*, the court reviewed case law affirming that "to furnish a blood sample; to provide a handwriting exemplar, or a voice exemplar; to stand in a lineup; and to wear particular clothing" had all been found to be non-testimonial.[140] The image of an individual's face, which mobile phone companies have been experimenting with as a mechanism to unlock a mobile device, appears to be similarly non-testimonial—as are likely to be all other forms of biometric identification, including retinal scans.[141] Gestures and pattern locks, by contrast (because they are stored only within the defendant's mind) have been declared as 'testimonial' as an alphanumeric password,[142] despite being potentially less secure for general use.[143] It must also be recalled that regardless of whether a device is secured using an alphanumeric password, a passphrase, a fingerprint, a gesture, or even a facial scan as the mechanism from which the key is derived, encrypting the device involves precisely the same kind of mathematical transformation in all cases. The ciphertext is just as computationally difficult to decrypt in the key's absence, and the user presumably expects that her data is equally secure and equally private.[144] This process of categorization implicitly accepts that the correct way to determine whether an accused's right against self-incrimination should apply—potentially a

138. Larsson, "Pirate Bay," *supra* note 63 at 376.
139. *Commonwealth of Virginia v David Charles Baust*, 89 Va Cir 267 (Va Cir Ct 2014).
140. *Doe*, *supra* note 133.
141. Vivek Mohan & John Villasenor, "Decrypting the Fifth Amendment: The Limits of Self-Incrimination in the Digital Era" (2012) 15 J Const L 11 at 20-24.
142. *Ibid*.
143. See *e.g.* Adam J Aviv et al, "Smudge Attacks on Smartphone Touch Screens" (Proceedings of the 4th USENIX Conference on Offensive Technologies, 2010), online: <www.usenix.org/legacy/event/woot10/tech/full_papers/Aviv.pdf>.
144. Which is an observation likely to have some bearing on the relationship between the protection against unreasonable search and seizure and arguments related to self-incrimination.

determining factor in their imprisonment or worse—is whether a metaphorical abstraction of a technical process (the mechanism from which the key is derived) is sufficiently similar to the separate metaphorical abstraction of forced speech (testimony). Ultimately, this is not likely to be the right approach.

Perhaps most troubling of all, the courts' reliance on the distinction between 'testimony' and 'non-testimony' has the effect of putting the constitutional liberties of those who use encryption software at the mercy of opaque commercial interests and in the hands of those who make design decisions about consumer electronics. It is not hyperbolic to say that a decision by a major company like Google, Apple, Facebook, or Microsoft to move away from passphrase-based keys and toward biometric ones could fundamentally erase the protection against compelled decryption under the Fifth Amendment for large numbers of people.[145] Vivek Mohan and John Villasenor also raise the problem that digital analysis of non-testimonial biometric measures such as "eye movement, position, and gaze (as well as heart rate, respiration, and facial expression)" may increasingly be used to infer information about a 'testimonial' passphrase, lessening the computational burden of conducting a brute force attack and rendering the protection for 'testimonial' keys mostly worthless.[146] While perhaps judicially expedient, and while the distinction between what is and is not 'testimonial' conforms tightly to the internal logic of the law, it fails to present a particularly principled or coherent approach to the issue of self-incrimination.

Instead, it may be worthwhile to reexamine earlier metaphors encryption as an act of 'speech' or a kind of 'language.'[147] Recall that in early cases such as *Bernstein*, US courts accepted the argument that cryptographic source code was expression protected under the First Amendment.[148] Since that time, there have been various instances where parties or interveners sought to emphasize the expressive and speech-like aspects of the act of production (*e.g.*, the passphrase) in order to emphasize its 'testimonial' nature. At the same time, speech metaphors have also crept into descriptions that give the *process* of encrypting an expressive dimension, as well as into descriptions of the ciphertext itself as a kind of expressive work. This idea was captured by Shari Steele and Danny Whitener in 1996 when they wrote that "prohibiting the use of a particular form of cryptography for

145. For a broad discussion of biometric access codes entering the market, see *e.g.* Alex Hern, "Google aims to kill passwords by the end of this year," *The Guardian* (24 May 2016), online: <www.theguardian.com/technology/2016/may/24/google-passwords-android>.
146. Mohan & Villasenor, *supra* note 141 at 26-27.
147. Vee, *supra* note 27 at 3-4.
148. *Bernstein*, *supra* note 27.

the express purpose of making communication intelligible to law enforcement officers is akin to prohibiting someone from speaking a language not understood by law enforcement officers."[149] Others have experimented with framing the right to use encryption as "a right to be able to limit to whom one imparts one's ideas," captured metaphorically as a "right to whisper."[150] In an amicus brief submitted by the American Civil Liberties Union (ACLU) and the Electronic Frontier Foundation (EFF) in the case of *Commonwealth of Massachusetts v Leon Gelfgatt*, the interveners argued that an order compelling an individual to decrypt a file is akin to an order to explain, transform, or translate it.[151] They argued that an individual could not be asked by the court to turn information that is incomprehensible into information that could put him or her in prison without running directly counter to the essential core of Fifth Amendment rights against self-incrimination. The analogy they chose is novel:

> Being compelled to decrypt a computer drive is like being forced to create, for the benefit of someone standing on the steps of the Boston Public Library, an English translation of every single literary book written in Braille. Doing so would not simply communicate the translator's access to and ability to translate the Braille works, though it would do that. It would also create new versions of those works: English translations revealing the number, length, and contents of all the books in the library's Braille collection.[152]

Kiok rejects the 'language' or 'translation' metaphor on the basis that "generally, more than one person knows a language … [I]f a person can read Spanish, the Government cannot prove that that person knows the contents of every Spanish-language text."[153] However, he acknowledges the conceptual value in the argument that "the fact that only an individual defendant can 'speak' the 'language' of encryption has testimonial significance, because it allows the Government to prove sole control of the encrypted media."[154] Recall that the process of disclosing that which decrypts a device can (depending on how one

149. Shari Steele & Daniel J Weitzner, "Chipping Away at Privacy," (16 April 1993) online: Electronic Frontier Foundation <w2.eff.org/Privacy/Key_escrow/Clipper/clipper.summary>. See also Kehl, Wilson & Bankston, *supra* note 21 at 14.
150. LEAP Encryption Access Project, "The Right to Whisper," online: <leap.se/en/about-us/vision>.
151. *Commonwealth of Massachusetts v Leon Gelfgatt*, 11 NE (3d) 605 (Mass 2014) (Brief for Amici Curiae the American Civil Liberties Union Foundation of Massachusetts, the American Civil Liberties Union Foundation and the Electronic Frontier Foundation in support of the Defendant-Appellee, 2013 WL 6002864).
152. *Ibid* at 4.
153. Kiok, *supra* note 114 at 76-77.
154. *Ibid* at 76.

looks at it) communicate self-incriminating information on at least two levels: first through the disclosure of potentially incriminating communications data stored on a device (such as files, images, or messages), and second because there is evidentiary value in the demonstration that one is able to decrypt a particular device in the first place (to extend the metaphor, to show that one knows *how* to translate the book, or that one speaks the right language to do so).[155]

Speech and translation metaphors help to solidify the testimonial dimension of disclosure. And, in terms of comparison to the container metaphors described earlier, the idea of translating an undecipherable book is also much closer to the actual mathematical process involved in decryption; rather than alluding to some hidden plaintext version, it makes the idea of transformation more salient and obvious. It is also possible that describing the abstract *process* of decryption as translation could ultimately represent a subtle cognitive shift that lessens the focus on the specific nature of key and allow us to imagine instead what has happened to the data itself. The idea that the ciphertext has some expressive value in its own right is also potentially useful, at least in the ongoing debate surrounding government-imposed backdoors (though not necessarily to the self-incrimination tests set out by the Fifth Amendment or Canadian *Charter* jurisprudence as they stand today). Nevertheless, because the ease of decrypting a device (if one knows what protects the private key) roughly approximates the ease of opening a locked container (rather than the difficulty of translating a library of Braille) courts may find this distinction less compelling than technical experts do.[156]

Others have attempted to capture the process of transformation that encrypted data undergoes by using the 'shredder' metaphor. Whereas in the 'container' analogies the type of key derivation mechanism seems to matter most, and in the 'translation' metaphor the process of encryption and decryption seems most important, the 'shredder' metaphor creates a vivid mental image of the ciphertext itself. In this model, the metaphorically shredded documents are in the hands of the state, but cannot be reassembled or understood without the specific assistance and knowledge of the accused.[157] The Electronic Frontier Foundation has made a closely related argument, describing the ciphertext both as "confetti

155. *Ibid*.
156. There is a link here to the "substantial cognitive content" argument. See Thomson & Jaikaran, *supra* note 36 at 13.
157. See Kiok, *supra* note 114 at 74.

made from a shredded document" and "like the pieces of a jigsaw puzzle."[158] Again, this model is an improvement on the container analogy insofar as it negates the false impression that encryption creates an enclosed space:

> An encrypted drive is similar to a massively (if not impossibly) complex jigsaw puzzle, with billions of individual pieces and no clues about how to assemble them. There is no barrier that prevents a person from opening the box and inspecting the pieces inside, but that inspection does not reveal what the assembled puzzle would depict. While trial and error would theoretically enable solving such a puzzle, in practice its immense complexity would mean that only a person who already knows what the final image is supposed to look like, or who has numbered the pieces and remembers their correct ordering, could put the pieces together and complete the puzzle.[159]

This is likely the most accurate metaphorical representation of encryption as a mathematical process, and, like the idea of 'translation,' emphasizes the coercive dimension at play. At the same time, this analogy does not entirely address the present legal preoccupation with the testamentary value of the mechanism used to decrypt the ciphertext. It continues to function for passphrases and numeric combinations, but it is unclear whether the 'puzzle' analogy would afford any greater protection in the case of devices using traditionally 'non-testimonial' mechanisms such as a fingerprint.

Finally, all of these metaphors potentially fail to appreciate the intimacy and particular nature of the information at stake in our personal devices. If at the core of the common law constitutional protection against self-incrimination is the belief that the contents of one's mind should be protected from government reach unless disclosed voluntarily, then it may be worth taking a closer look at the nature of the plaintext itself. Notably, the American case law has failed to find that the *contents* of an encrypted device are protected by the Fifth Amendment, hence the emphasis on the testimonial act which discloses the key.[160] However, as the Supreme Court of Canada acknowledged when describing the heightened expectation of privacy associated with personal computers in *R v Vu*, these devices simply cannot be imagined as "containers" like cabinets or cupboards. Rather they "give police access to vast amounts of information that users cannot control, that they may not even be aware of or may have chosen to discard and which

158. *United States v Apple MacPro Computer*, 851 F(3d) 238 (3d Cir 2017) (Brief of Amici Curiae Electronic Frontier Foundation and American Civil Liberties Union in support of Appellant, 2016 WL 1529869 at 6) [*Apple Mac Pro Computer* Amicus Brief in Support of the Appellant].

159. *Ibid* at 8.

160. Thomson & Jaikaran, *supra* note 36 at 7.

may not be, in any meaningful sense, located in the place of the search."[161] The EFF and ACLU have similarly explained that "our computers, phones, and other electronic devices contain a catalogue of information as diverse as the thoughts in our mind."[162] Indeed, this idea goes back as far as the 1940s, to Vannevar Bush's now-classic essay entitled "As We May Think."[163] In that piece, Bush proposed a device he named the *memex*, a kind of mechanical file library that allowed the user to catalogue and link together all of his or her records, private thoughts, and communications. Despite the fact that the memex is comparatively crude when held against modern computers or mobile devices, he did not hesitate to imagine the machine's relationship to its user as "an enlarged intimate supplement to his memory."[164] Potentially, by reconfiguring the encryption equation in a way that places contextual emphasis on the plaintext, we are able to better emphasize our relationship to the devices and their role in our lives better. This perspective highlights the intimate practical and philosophical relationship between self-incrimination and privacy rights where digital evidence is concerned. In this final model—'machine as externalized memory'—precise legal categories are backgrounded and the constitutional stakes are allowed to take center stage.

As a final aside, while the idea of an encrypted machine as 'container' determines what the metaphorical key is to the law, it also has implications for the evolution of the "foregone conclusion" doctrine in the United States, which allows governments to compel decryption where key disclosure fails to add to the sum of information already known to government.[165] Some federal circuit courts have introduced limitations to this doctrine through the "reasonable particularity" standard, which requires the state to have specific knowledge of particular files on a given machine, rather than allow decryption on a broader or more generalized basis.[166] Dan Terzian—himself an advocate of the less restrictive approach to compelled decryption—applies the container analogy to describe the issue as follows:

> But for other courts, knowing that the unencrypted version exists isn't enough. Instead the government must also know particular files exist on that version. This method silently shifts the inquiry; facing the government's demand for a car (the unencrypted hard drive), these courts required knowledge of what's in the glove

161. *R v Vu*, 2013 SCC 60 at para 24, [2013] 3 SCR 657 [*Vu*].
162. *Apple Mac Pro Computer* Amicus Brief in Support of the Appellant, *supra* note 158 at 3.
163. Vannevar Bush, "As We May Think," *The Atlantic* (July 1945), online: <www.theatlantic.com/magazine/archive/1945/07/as-we-may-think/303881>.
164. *Apple Mac Pro Computer* Amicus Brief in Support of the Appellant, *supra* note 158 at 3.
165. Thomson & Jaikaran, *supra* note 36 at 8.
166. Mohan & Villasenor, *supra* note 141 at 20-21.

> compartment (particular files). The shift is subtle, but the effect profound. Courts requiring only knowledge that the unencrypted version exists will always find a foregone conclusion, whereas courts requiring knowledge of the particular files usually won't.[167]

Metaphor connected to the spatiality, location, and storage of data also raises issues for the reasonable particularity standard—issues which are in many ways similar to those applied to 'big data' or 'cloud' metaphors described in Part IV. "It is quite possible for the government to show knowledge of existence, possession, and authenticity without specifying the technologically problematic 'location' of such information," Kiok explains, arguing that to require this latter element creates unnecessary confusion.[168]

VI. CONCLUDING THOUGHTS

Metaphor is not a mere descriptive tool: it is a persuasive device fraught with the possibility to distort, manipulate, or obfuscate reality. Courts and legislators must therefore take a disciplined approach to understanding technical concepts in order to ensure that they are awake to the political and legal implications of their legal choices. In this light, many scholars have argued for the abandonment of technological metaphor altogether. For example, Kiok has said specifically in the context of encryption and the Fifth Amendment that

> courts and commentators should be hesitant to analogize encryption to older technology, and instead should engage in a fact-specific inquiry that focuses on exactly what type of encryption is being used, the testimonial nature of the act of production of a password or decrypted material, and what the government can prove it already knows about the material it is seeking. Inapt analogies and inexact information yield "bad" law. Prosecutors and defense counsel should ensure that experts who understand the issues of encryption testify to a judge in a cogent and coherent way that puts the testimonial issue squarely before a court.[169]

Yet divorcing ourselves from metaphor in the law entirely is both an impractical and a philosophically tenuous proposal. First, it ignores the practical benefit of metaphor, both in its ability to "operationaliz[e] legal theories" effectively and in its capacity translate complex technological problems into

---

167. Dan Terzian, "Forced Decryption as a Foregone Conclusion" (2015) 6 Cal L Rev Circuit 27 at 27-28.
168. Mohan & Villasenor, *supra* note 141 at 22.
169. Kiok, *supra* note 114 at 79.

legally meaningful language.[170] In Fuller's words, "[i]t is easy to say, 'Fictions are makeshifts, crutches to which science ought not to resort.' So soon as science can get along without them, certainly not! But it is better that science should go on crutches than to slip without them, or not to venture to move at all."[171]

Perhaps more importantly, we miss the point that imagining legal reasoning in the absence of technical metaphor implicitly assumes that there remains some fixed, inherent logic to the legal rules and categories at all. In reality, those categories (whether 'testimony,' or 'personhood') are generally themselves abstractions, with boundaries that shift over time and place, embedded with metaphor all the way down. We must therefore remain skeptical about the extent to which it is possible for jurists and judges to "achieve a 'metaphor-free' understanding of the technology."[172] Instead, courts and policymakers ought to strive first to understand the technical, mathematical, or scientific concepts at play as scientists themselves do—in full recognition that "scientific" thinking has its own problems of metaphor and category—and take a critical stance when examining the fictions we then use to translate those concepts into law. Expert testimony is one element of that process, as is a commitment to nuanced, fact-specific reasoning and more rigorous professional development of technological literacy among jurists.

There is no doubt that metaphor will continue to shape the way the law understands encryption, and those understandings in turn may have a transformative impact on our substantive legal and political rights. This power is perhaps most clearly demonstrated in the fields of criminal evidence and constitutional law, but may have broader implications in the long view of technology law as both a discipline and tradition. We must work to "see through" these metaphors, appreciating those instances where they illuminate, while recognizing when they may mislead. For as long as encryption offers the promise of carving out "a space free of power's reach," jurists have an obligation to find metaphors big enough to speak to that greater truth.[173] This demands a serious engagement with both text and meaning: a critical, transparent, and lucid appreciation of language and the power it wields.

---

170. Peter J Smith, "New Legal Fictions" (2007) 95 Geo LJ 1435 at 1439.
171. Rudolf von Jhering, *Geist des römischen Rechts* (Leipzig: Breitkopf & Härtel, 1865) vol 3 at 297, cited and translated in Fuller, *supra* note 60 at 364.
172. Stephanie A Gore, "'A Rose by Any Other Name': Judicial Use of Metaphors for New Technologies" [2003]:2 U Ill JL Tech & Pol'y 403 at 438.
173. Rogaway, *supra* note 19 at 27.