Canadian Journal of Law and Technology

Volume 19 | Number 1 Article 7

1-30-2023

Book Review Rethinking the Jurisprudence of Cyberspace

David Cowan
National University of Ireland Maynooth

BOOK REVIEW
Rethinking the Jurisprudence of Cyberspace

Rethinking Law series
Chris Reed & Andrew Murray
Edward Elgar Publishing
Publication Date: 2018
ISBN: 978 1 78536 428 0, 256 pp

Dr. David Cowan[*]

It is a common claim that law is always catching up with technology. This is not entirely fair. The European Union's General Data Protection Regulation[1] (GDPR) could be viewed as a case of technology having to catch up to the law. That said, clearly there are challenges in law and in the legal profession, both in terms of how the law can adapt to changes in the digital world and the disruption of the legal profession. On the former point, there are perhaps three broad schools of thought: existing law is sufficient for adapting to new technological challenges, as it has always done; we need specific laws for the technological challenges we face, because it is a new world; and a third way of inevitable compromise between the two. In *Rethinking the Jurisprudence of Cyberspace* by Chris Reed, Professor of Electronic Commerce Law at Queen Mary University of London, and, Andrew Murray, Professor of Law at the London School of Economics, we have an extremely valuable guide to the jurisprudential and law-making challenges as we journey deeper into the digital world. There are not only the geographical challenges of discerning the relationship between the physical and digital world, but also temporal challenges, both in terms of a constant operating environment and the tendency of law to use the rear-view mirror. This highly-readable volume navigates through the issues by combining depth in legal philosophy with sophistication and nuance in grasping technology.

This is not to say we should view this as a binary challenge——an either/or dilemma for our age. Arguably, we have an opportunity to future-proof both the law and legal system. In this volume, which is part of the Rethinking Law series, Reed and Murray map out some very thoughtful territory, not just for those agonizing over the jurisprudential questions, but happily by also offering extensive practical guidance for legislators and regulators looking to find their way around cyberspace. Technology has its own dedicated followers of fashion, which can confuse debates or create unrealistic timeframes or attributes for

---

[*] Associate Lecturer in Law, National University of Ireland Maynooth.

[1] EC, *Regulation (EU) 2016/676 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, [2016] OJ, L, 119/L.

technology. Artificial Intelligence (AI) is a good example of this. Indeed, it might be hyperbole to say that AI has a great future behind it, but as one consultant, Aditya Kaul, research director at Omdia, explained, "[b]ack in the 1970s, there were predictions that, by 2020, we should have generalized AI by now. We should have been having some moon and Mars bases, and we're nowhere near that."[2] After the awakening years of the 1940s and 1950s there was something of a flatlining, with expert systems being the thing. The first article I wrote on law and technology was about expert systems; and reading this 1984 article[3] the observations I made then seem eerily familiar now. I also recall working on a project with the late AI pioneer Professor Donald Michie,[4] who worked at Bletchley Park with Alan Turing, when he launched The Turing Institute in Glasgow, Scotland. We were filming with the BBC and wanted to show robots putting a ball of paper into a bin, but the programmers were struggling. I informed them this was simply illustrative and asked if they could perhaps just do so by a remote control rather than programming? The disgruntled programmers agreed, and always the pragmatist Michie laughed off the incident. I sometimes think we have progressed little since, but it seems people's imagination still runs away with them. Michie urged greater caution in an interview with me at the time that AI was not, "a race of super-clever Daleks, unfathomable to man, that will eventually dominate the globe. In fact, what AI is about is exactly the opposite: making machines more fathomable and more under the control of human beings, not less."[5] Optimistically, he believed AI seeks to return technology to its "proper place" as servant to society, and together people and machines could "subdue many of the world's afflictions."[6]

However, the last decade or so has seen a new lease of energy with big data and accelerated learning algorithms. Today it is hard to read about a legal tech product being discussed without someone referencing AI, but the AI component is probably analogous to the robot being manually controlled by Michie's programmers. Perhaps I am being hyperbolic again, but certainly AI has not progressed as far as early AI pioneers had expected to happen. If we are not talking about AI in law then we are talking about blockchain, which is famously trusted because it trusts no one and no one can be trusted anyway. It is a libertarian dream of borderless freedom, to which legal orthodoxy might retort there is everywhere a real-world counterpart. Eventually the digital footprint has to reach landfall, or does it? By reaching landfall it is brought into a jurisdiction.

---

2 Aditya Kaul, as quoted in Sooraj Shah, "Why hasn't AI changed the world yet", *BBC* (3 March 2020), online: < www.bbc.com/news/business-51632840 > .

3 See David Cowan, "Old traditions die hard" (1984) Legal Workings 37-41, DEC User.

4 On 7 July 2007 Professor Michie was killed in a car crash. See J A N Lee, "Computer Pioneers", online: *Computer Society, Institute of Electrical and Electronics Engineers* < history.computer.org/pioneers/michie.html > (for his biography). See also, Donald Michie, *On Machine Intelligence*, 2nd ed, (Chichester: Ellis Horwood, 1986).

5 David Cowan, "The optimistic prophet: Donald Michie", (1985) Computer Talk at 15.

6 *Ibid.*

Reed and Murray take us a step back to examine questions of law and authority, which has been undermined by technology. In Part One, the authors identify three key cyberspace lawmakers: the state(s); non-state transnational and technological rule makers; and communities, meaning private lawmakers. The theme of authority runs throughout, though not without its Gemini twin legitimacy. States are conventionally assumed to have comprehensive authority to regulate within their borders and activities beyond its borders which have effects internally. However, the authors highlight this is simplistic in cyberspace, particularly given the lack of practical authority a state may have over a cyberspace user.

The question marks over legitimacy take on an interesting dimension in cyberspace, where the community of users is much greater than the population of a state. States have an extended cyberspace community, and its citizens have digital imprints and data selves around the world. This raises further questions over the exact relationship between the individual and the state in a digital world. Reed and Murray argue the axiom that nation-states have unlimited authority to make rules comes under challenge in cyberspace. In a borderless digital world, it is less obvious who can make the rules and why citizens of cyberspace should obey them. Equally, who should regulate cyberspace? The authors suggest it may be a question of developing a new 'decentralized, emergent law' whereby collective action of cyber users create common standards through mutual coordination and consent, eventually leading to cyberspace governing institutions.

In Part Two of this volume, Reed and Murray dive more deeply into how rules work with a focus on control, competition and conversation, including outlining normative competition in Cyberspace, place of networks and nodes. Control is thoroughly examined though the traditional lens of law as a system of imperative commands enforced through coercion backed by authority. Starting with the assertion by Johnson and Post[7] that law's primary role is to control how others behave, Reed and Murray pose the question used as the title of a 2006 book by Goldsmith and Wu: *Who Controls the Internet*?[8] The answer from Goldsmith and Wu, shared by Lawrence Lessig, was a Hobbesian discourse based on law's ability, as Lessig puts it, to achieve control through threats. This brings us inevitably to the discussion of code as a control mechanism. Though Lessig's regulatory model and "pathetic dot" thesis have had little influence on regulators and has not always been deeply explored in the academy, he does offer a lot of food for thought. Lessig may be giving the wrong answers, but he is asking the right questions and, as the authors note, such discussions were not obvious topics at the time.

---

[7] David R Johnson & David Post, "Law and Borders: The Rise of Law in Cyberspace"(1996) 48:5 Stan L Rev 1367, DOI: < 10.2307/1229390 > .

[8] Jack Goldsmith & Tim Wu, *Who Controls the Internet?: Illusions of a Borderless World* (New York: Oxford University Press, 2006).

Drawing on behavioral insights, Reed and Murray conclude that "obedience to the actual provisions in the law will only happen if the law becomes entrenched as part of the normative landscape within which its community operates" and code, they suspect, "might work in a similar way."[9] Building on this, the authors explain "the community will identify a conflict between the demands of code and the community's existing norms, and will collectively decide that those norms are to be preferred to code's prescriptions."[10] Pressure can then be applied by the community users for coders to bring code and norm closer together. Turning to normative competition in cyberspace, they argue that users are more likely to change behaviour in accordance with social norms rather than legal norms or rules. While social norms have lesser sanctions than legal norms——ostracism rather than imprisonment for instance——there is greater likelihood of detection in the former due to the distributed nature of the detection mechanism. Norms, the authors explain, are naturally pluralistic and they explore three competing theories of social normative compliance: rational choice theory, evolutionary theory, and social rationality theory. Notably, in cyberspace communities there are "chosen communities"[11] with strong loyalty bonds, and they reflect us and our specific interests. Nicholas Negroponte,[12] co-founder of the MIT Media Lab, also expounded that in cyberspace geography and time are meaningless, which creates unique communities that are normatively connected rather than temporally or geographically.

Reed and Murray suggest persuasion is a better policy in cyberspace or perhaps a reality check on the practicalities of enforcement. The past year has thrown up good examples of such dynamics. The Covid-19 experience of passing legislation and regulations to promote what governments see as good behaviours to manage the pandemic has been met with varying levels of adoption by citizens. In normative terms cyberspace, the authors note, is "uniquely noisy" with a variety of actors each clamouring for attention and obedience, a space wherein "only the loudest voices are heard and paid attention to."[13] The 2020 US presidential elections are fertile ground for any researchers to develop that train of thought. Reed and Murray add that other normative claims on such actors, who are members of various communities in cyberspace, suggests that "[i]deally the lawmaker would understand at least the broad outline of the authority claims of those other communities' rules, and attempt to craft its own authority claim to be as little incompatible as possible."[14]

---

9 Chris Reed & Andrew Murray, *Rethinking the Jurisprudence of Cyberspace* (Cheltenham: Edward Elgar Publishing, 2018) at 102.

10 *Ibid.*

11 *Ibid.* at 107.

12 Nicholas Negroponte, *Being Digital* (London: Hodder & Stoughton, 1995) at 164—171.

13 Reed & Murray, *supra* note 9 at 137.

14 *Ibid.* at 138.

Another important discussion revolves around the platforms and gatekeepers of cyberspace. There is some concern, and rightly so, about the concentration of power amongst technology companies and platforms. As the *New York Times* reported last year Apple, Amazon, Alphabet, Microsoft and Facebook rose thirty-seven percent in the first seven months of 2020 to "constitute 20 percent of the stock market's total worth, a level not seen from a single industry in at least 70 years."[15] Such concentration makes these near-monopolies strong gatekeepers and lawmakers, and we face a number of challenges in taming the beasts, which are hungrily fed on user data and clicks. However, optimistically the authors also note, citing the cases of the 2002 AOL/Time merger and the declining younger generation user base of Facebook, "the very plasticity of cyberspace's communication allows new players to gain market share rapidly, which can quickly lead to the loss of gatekeeper strength for the established players." The recent Facebook and GDPR fines are ways the EU is also seeking to manage these threats. Another question of concentration to add is whether we want social media platforms controlling free speech. The widely reported curbs on U.S. President Donald Trump's social media activities put in stark contrast the conflict between the power of the platform and the power of the president, not forgetting that the platforms themselves have their own cabals of decision-making and a profound financial interest in controversy as a driver of data and clicks. Irrespective of one's feelings about the Trump presidency, it leaves open the question of where this debate leaves democratic control. The exit of Trump may have shut down the issue for now, but it surely remains a live issue.

A final theme to note is an idea central to western democratic ideals, namely the rule of law, which is ripe for review in the digital age. Reed and Murray start their assessment with Dicey and examine how the rule of law can be reinterpreted for cyberspace. They offer a revised rule of law laundry list, a digital Dicey so to speak: law should be known in advance, public, general, clear, stable and certain, and applied to all.[16] The authors conclude, "[t]he message of this book is that the legitimacy, efficacy and normative acceptance of law norms in the online environment are predicated upon their acceptance by the community and by the individual within that community," which they think of as "a form of legal reception theory" where the text is an interpretive act set against the individual's cultural background.[17] This may narrow the scope of legal systems to the individual, thereby reasserting the law in cyberspace. Their afterword leaves us with the thought that "lawmaking authority in cyberspace has to be assessed at the level of individual rules of law, not at the law system level."[18] They also offer an elevator speech for the book[19] comprising four broad points:

---

[15] Peter Eavis & Steve Lohr, "Big Tech's Domination of Business Reaches New Heights", New York Times (19 August 2020), online: <www.nytimes.com/2020/08/19/technology/big-tech-business-domination.html>.

[16] See Reed & Murray, *supra* note 9 at 200—224.

[17] *Ibid*. at 228.

1. Law has two main sources of authority: constitutional and community acceptance of a rule.
2. Cyberspace jurisprudence concerns itself exclusively with the second of these.
3. Laws compete for authority in cyberspace with other laws as well as social and other norms.
4. Lawmakers can "certainly weaken" their claims by not establishing legitimacy and by impairing the rule of law via authority claims beyond their bounds.[20]

Reed and Murray conclude, "in the crowded normative landscape of cyberspace, 'Which of these laws ought to be obeyed?' We think we are now closer to answering that question."[21]

Indeed, they have been very helpful with their analysis of a range of concerns that need to be addressed if we are to take the challenges in law posed by technology seriously. This may form the basis of any notion we might have, as a set of societies, to develop a social contract for the digital age. The social contract of the enlightenment was one founded on privilege and handed down by an elite to the working man. A new social digital contract might be founded on enhanced access bringing together all areas of society and recognizing diversity, thereby achieving a true social legitimacy. This, it appears to me, is the struggle societies currently face and the self-realization that technology offers a way for this new kind of social contract, and our lawmakers in cyberspace must take a humbler approach by requesting our attention. It is this humbler approach that Reed and Murray suggest that might drive lawmakers to persuade users more broadly as to the legitimacy of laws and for users in turn to consider the demands law makes. In other words, a legal path may exist to support the creation of a more collaborative digital society.

---

[18] *Ibid*. at 231.

[19] See *ibid*. at 234.

[20] See *ibid*. at 234—235.

[21] *Ibid*. at 235.