BOOK REVIEW

RETHINKING CYBERLAW: A NEW VISION FOR INTERNET LAW

Jacqueline Lipton

Cheltenham, UK: Edward Elgar, 2015. 164 pp. ISBN: 978-1-78100-217-9. £65.

It is not difficult to guess the grand ambition from the title of *Rethinking Cyberlaw: A New Vision For Internet Law*. The primary goal of Jacqueline Lipton (David L. Brennan Chair in Law and the Director of the Center for Intellectual Property Law and Technology at the University of Akron School of Law in the US) is to establish an informed debate about the extent to which the focus, metaphors and narratives in cyberlaw are important and helpful in thinking about the challenges posed by innovations and new technologies in a highly networked environment. As she observes: "it is important to move the debate away from questions about *whether* cyberlaw is a distinct field toward what the field actually comprises" (p.13).

Lipton's quest to re-assess the scope of cyberlaw is informed by two factors: first, we have over two decades of precedents from which we can identify key issues and themes relevant to the present environment; second, that the world now is vastly different from the technological landscape in the early 1990s. It is worth recalling that discussions during that earlier period were directed at the characteristics of hardware and software as redefining the principles of social ordering and democracy.[1] The debates and arguments about the adequacy of law and whether there was a need for a separate law often revolved around metaphors and narratives such as "cyberspace", "code is law", "Internet Law", and "Cyberlaw".[2] Cyberlaw's genealogy may at first glance seem strangely out of place with the expansion of the digital landscape, emergence of personal data as a driver of innovation and economy, and smart technologies. Search engine rankings, social logins, cloud markets and blockchains are some of the innovations transforming economic and social activities. "Google" is now a verb. IBM Watson merely hinted at the capabilities of machines to learn, engage and act autonomously. The digital landscape of peer-to-peer systems employed by Napster and Grokster bear little semblance to the complex web of affordances, apps and plugins available today that enable content to be shared and interactions to take place seamlessly. Finally, the emergence of internet elites, whose business models give them control over upstream and downstream markets, have started to raise concerns about competition, innovation and manipulation.[3] The continued growth of online intermediaries such as Google and Facebook also coincides with personal data emerging as an asset of economic value. Indeed, Facebook, the leading

[1] L Lessig, "The Law of the Horse: What Cyber Law Might Teach" (1999) 113 *Harvard Law Review* 501-549.
[2] J Cohen, "Cyberspace as/and Space" (2007) 107 *Columbia Law Review* 210-256.
[3] See European Commission, "Antitrust: Commission Sends Statement of Objections to Google on Comparison Shopping Service" (2015) available at http://europa.eu/rapid/press-release_MEMO-15-4781_en.htm (accessed 17 Sep 16).

social networking site, had profits in the first quarter of 2016 that exceeded $2 billion.[4] Is there a role for cyberlaw when policymakers are trying to prepare society and their economies for the Fourth Industrial revolution?

Rethinking Cyberlaw answers this question in the affirmative. The book is particularly engaging in respect of the argument that topics and issues that are peripheral to the study of cyberlaw should either be excluded or given less focus (pp. 3-8). According to Lipton, early cyberlaw scholarship was understandably keen to avoid the strictures of legal essentialism and formalism and instead projected law inter-temporally, or as she puts it – "in terms of how the internet might impact human behaviour and how courts and legislatures might respond to online problems…") (p. 2). Lipton concludes that with the benefit of hindsight, we can draw on the extensive legal resources during the past two decades and "reframe cyberlaw in light of the realities of modern regulation" (p. 3) and use two key concepts – information and intermediaries – "toward developing a cyberlaw that contributes something more useful to the future evolution of legal principles as they apply to online conduct" (p. 3).

The introductory chapter in *Rethinking Cyberlaw* merits careful reading and reflection since much of the discussion in later chapters pursues the ideas in a nuanced manner. The chapter begins by providing a context and an overview of why cyberlaw curricula as currently constituted, and cyberlaw scholarship, continue to overemphasise all aspects of "cyber". Lipton feels that the sheer range of issues and topics covered in cyberlaw contributes to the subject lacking intellectual coherence and thereby creates problems of manageability.[5] Lipton questions whether there is really a need for cyberlaw courses to continue giving prominence to issues relating to extraterritorial reach of laws, legislative competence and regulation of network infrastructure.

The next four chapters aim to vindicate Lipton's vision with a discussion of topics "that have caused the most media attention and that have come to the fore in cyberlaw casebooks and syllabi" (p. 158): (i) copyright; (ii) trademarks; (iii) defamation; and (iv) privacy and online victimisation. Lipton's primary goal in these chapters is directed towards emphasising two essential characteristics that she argues should now be the focal point of cyberlaw curricula: information flows and online intermediaries. When considering both concepts, Lipton stresses that the interplay between the modalities of regulation and law should also figure more prominently, particularly in strengthening areas where social norms are being outpaced by technological innovations. Given the emergence of information and online intermediaries as drivers of mobile interactions, innovation and the economy, Lipton suggests that a "reconceptualised cyberlaw field could serve to organize the judicial and legislative developments from disparate areas of law that relate to intermediaries into a more cohesive framework" (p. 12).

---

[4] D Seetharaman, "Facebook Posts Strong Profit and Revenue Growth" (2016) available at http://www.wsj.com/articles/facebook-posts-strong-profit-and-revenue-growth-1469650289 (accessed 17 Sep 16).

[5] See also E Goldman, "Teaching Cyberlaw" (2008) 52 *St. Louis University Law Journal* 749-764.

Each chapter follows a standard narrative – a quick summary of legal concepts is followed by a commentary on key cases and arguments and concludes with suggestions on how cyberlaw scholarship should now be reconfigured. As an example, the chapter "Digital Copyright Law" takes the reader through conceptual, technological and policy issues in considerable detail. Lipton uses cases to highlight the critical tensions raised when proprietary rules for the protection of intellectual property works become situated in an infrastructure where free flow of information is the default engineering construct. While accepting that an understanding of legal and regulatory responses to the application of established copyright rules and norms is needed, Lipton suggests that the implications of law for online intermediaries, the adverse impact on start-ups, and creation of innovative business models and services and reduction of consumer choice merit equal attention and discussion. (pp. 68-71).

Chapter 3, which is devoted to trademark law, is compact and full of recommendations. The discussion leaves readers with a series of questions where there are no easy answers: why is secondary rather than primary liability given very little space (p. 87); is there scope for expanding fair use for online intermediaries; what are the unintended consequences of overprotecting interests of intellectual property rights holders; can a more coherent framework be created for EU and US approach to trade mark liability; and does the Uniform Domain Name Dispute Resolution Policy offer lessons for cyberlaw? Some readers may find the questions and coverage engaging. Equally, readers may wish to consider whether these are failings endemic in cyberlaw scholarship, or whether cases such as *Google France v Louis Vuitton*[6] are just another illustration of proprietary entitlements trumping innovation opportunities (pp. 93-94). In sum, Chapters 2 and 3 (as well as the following Chapter 4) reinforce the question whether judicial responses tend to preserve the status quo of protecting intellectual property rights rather than give serious weight and consideration to the financial resources available to promoting innovative services (pp. 82-83).

Chapters 4 ("Online Defamation and other Harmful Speech") and 5 ("Digital Privacy and Cyber-Victimization") provide two further opportunities for Lipton's to illustrate her claims regarding the continued salience of cyberlaw and the need for much greater engagement with the role of online intermediaries in a global context. Newcomers to cyberlaw scholarship will find Chapter 4 informative – staple US judicial and legislative interventions are recounted in sufficient detail and highly accessible. Non-US readers may wonder why policy and judicial developments elsewhere are not given more coverage. The OECD, for example, published in 2011 an important document, *The Role of Internet Intermediaries in Advancing Public Policy Objectives*, which addresses some of the tenets of Lipton's broad thesis – business models, trust, balancing economic, cultural and innovation challenges, multi-stakeholder engagement and responsive models of governance.[7] US readers may also benefit from integrating some

[6] *Google France SARL and Google Inc. v Louis Vuitton Malletier SA*, [2010] EUECJ C-237/08, C-237/08 (ECJ).
[7] OECD, *The Role of Internet Intermediaries in Advancing Public Policy Objectives* (2011) available http://www.keepeek.com/Digital-Asset-Management/oecd/science-and-technology/the-role-of-internet-intermediaries-in-advancing-public-policy-objectives_9789264115644-en#.V9q7brU-Y00 (accessed 17 Sep 16).

recent jurisprudence from the European Court on Human Rights in Strasbourg.[8] Finally, the conclusion in both Chapters 4 and 5 could be updated to take into account of developments in the EU. As is well-known, the EU continues to pursue an activist role in pursuing its single market agenda. More specifically, as part of the Digital Single Market Strategy initiative, the European Commission launched a "Public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy."[9] Some of the responses, which have now been made publicly available, would complement the conclusions reached in Chapter 4.

Chapter 5 is devoted to the ability of individuals to manage their privacy and misuse/abuse of information. The complex issues of privacy, victimisation and control over personal data are condensed into 13 pages. It is true that online intermediaries have a role to play. There is, however, a wider dimension which scholars such as Sherry Turkle, Helen Nissenbaum and Jack Balkin have pointed out. Affordances and new technologies, when embedded in social relations, may lead to good as well as bad outcomes – revenge porn, peer victimisation, harassment and trolling come to mind. The law is sometimes the least efficient mechanism for shaping social norms that have been outpaced by new technologies. Cyberlaw in its reconceptualised form may make an important contribution in helping change social attitudes, which undermine trust and respect for human dignity. The final chapter (Chapter 6) reinforces the goals and aims outlined in the introductory chapter.

Lipton's book is not intended to provide a capacious resource for lawyers and law students. Readers may probably agree with Lipton's vision for a reconceptualised cyberlaw. I do not interpret *Rethinking Cyberlaw* as implying that cyberlaw as originally conceptualised has no place in law schools or scholarship. Where I probably depart from endorsing Lipton's vision enthusiastically is in relation to the importance she attaches to the core concepts as providing an intellectual and policymaking compass for cyberlaw. The reason for this is simple. It is difficult to think of many concepts that have emerged as a prism for understanding the evolving role of law. A recurring cyberlaw theme, for example, in discussions about sovereignty, intellectual property, free speech and privacy was the evolution of social norms and economic relationships in an environment mediated by technology and their disruptive consequences for established legal, economic and social ordering. Cyberlaw is sufficiently well-developed as a discipline and a metaphor to help us better reflect on cultural, institutional and political engagement with affordances and innovations that make up the Internet of Things. [10] *Rethinking Cyberlaw* is a bold attempt to explore what it is we do when we study and research cyberlaw. There is space for both visions.

---

[8] See e.g. *MTE v Hungary* [2016] ECHR 135; *Delfi v Estonia* [2015] ECHR 586.
[9] European Commission, "Public Consultation on the Regulatory Environment for Platforms, Online Intermediaries, Data and Cloud Computing and the Collaborative Economy" (2015) available at https://ec.europa.eu/digital-single-market/en/news/public-consultation-regulatory-environment-platforms-online-intermediaries-data-and-cloud (accessed 16 Sep 16).
[10] R Calo, "Robotics and the Lessons of Cyberlaw" (2015) 103 *California Law Review* 513-564.

Joseph Savirimuthu
Senior Lecturer in Law, School of Law and Social Justice, University of Liverpool

DOI: 10.2966/scrip.130316.x