International Internet Law

by Joanna Kulesza
Routledge, New York, 2012
ISBN 978-0-415-67468-3 (print) or 978-0-203-12325-6 (e-book)
Price: $135.00, pp. 160

Translated by Magdalena Arent and Wojciech Wotoszyk

Reviewed by Jennifer Harris
Journal of High Technology Law
Suffolk University Law School

“[T]he process of regulating legal and social consequences of technological solutions always falls behind technological innovations and their implementation. This applies to the internet as well, if not most of all.”¹

The world has approximately 2.5 billion internet users.² The internet, like the environment, does not stop at a country’s borders, and needs, like the environment, to be governed by at least some comprehensive international law. Yet unlike treaties held on international environmental law or even the sharing of outer space, there is no International Internet Law yet to resolve the overlapping of jurisdiction and opinion in the internet’s worldwide reach. This book, written by

---

¹ Joanna Kulesza, International Internet Law, ix (Routledge 2012).
Joanna Kulesza and the fourth book in the Routledge Research in IT and e-commerce Law series, proposes such a law.

Jurisdiction is one of the most difficult things to determine when a network is worldwide. Kulesza uses the word “aterritorial” to describe the internet. The World Wide Web consortium’s Internet Governance Project defines the internet as “the global data communications system formed by the interconnection of public and private networks using Internet Protocol (IP), TCP (“Transmission Control Protocol”) and the protocols required to implement IP internetworking on a global scale, such as DNS and packet routing protocols.” This is more than just http and content. To date, only a patchwork of attempts to regulate this hardware-supported, non-jurisdictional framework exists, and it comes from all directions.

For example, the Council of Europe Convention on Cybercrime defines offenses and “unifies terminology,” but is essentially optional. ICANN, or the Internet Corporation for Assigned Names and Numbers, which has the authority to administer DNS code sequences (to entities such as ccTLDs or gTLDs) is located in California and, until recently, was governed by California law. Nations themselves feel differently about what constitutes a crime and, relatedly, what types of content should be blocked. The United States and many others consider

---

3 Joanna Kulesza is an assistant professor in the Department of International Law and International Relations, Faculty of Law and Administration, at the University of Lodz, Poland. She is the author of three monographs, including International Internet Law, and over twenty peer-reviewed articles in English and Polish. She is currently the Membership Committee Chair of the Global Internet Governance Academic Network (GigaNet). For more information, see [http://unilodz.academia.edu/JoannaKulesza](http://unilodz.academia.edu/JoannaKulesza).
cyberattacks a form of warfare to which a physical response is acceptable, but other nations believe as long as they maintained due diligence, cyberattacks originating within them should not bring repercussions.

Kulesza is a proponent of a fairly open internet and the ideas and commerce that can be exchanged over such an internet. The failure to create an International Internet Law, she believes, will result in the “Balkanization” of internet law or the effect described as “splinternet.” Not only would countries each have their own internet laws, but free transmission could be prevented: in 2008 Russia blocked Georgia’s internet in a dispute, and unwittingly also disabled the network in Armenia. Kulesza wishes to see the development of a global Internet and “the information society that is to form the basis for a global knowledge-based economy.”4 Like most of us, she believes the benefits of a global internet outweigh the burdens.

This book is divided into four chapters, packaged between a Preface and a Summary, dense with information in small text. The first two chapters, “The Limits of State Competence,” and “Scope and Sources,” address the problems with internet governance today, the first broadly by laying out principles underlying jurisdiction in public and private international law, the second by pinpointing certain areas that could use uniform international regulation, such as trademark law

---

4 See Kulesza, supra note 1, at 159.
in regard to domain names, fair use under copyright law, e-commerce contracts, and cybercrime. The third chapter, “Examples of Current National Practice,” summarizes how far various nation-states\(^5\) presume their law reaches into people’s privacy, issues of file sharing, and content monitoring or censorship. In the fourth, “From International Governance to International Internet Law,” the author discusses existing ideas on what to do and offers a solution, further outlined in her Summary.

The jurisdictional differences on conflict of law decisions and the filtering issue in China and Singapore are notable. The United States and European Union appear at first to have similar ideologies, but cases such as the “Yahoo Nazi Memorabilia Case” show that freedom of speech is more extensively interpreted in America.\(^6\) The discussion of China and Singapore’s filtering methods shows that China relies mostly on hardware and surveillance by ISPs, whereas Singapore, while maintaining its reputation as an Asian media hub, uses a low-tech word search filter and defamation suits by the government that run into the hundreds of thousands of dollars. Kulesza here remains very low-key with regard to

---

\(^5\) Kulesza often refers to sovereign nations as “states.”

\(^6\) Yahoo! Inc. v. La Ligue Contre le Racisme et l’Antisemitisme, 433 F.3d 1199 (9th Cir. 2006) (en banc) (reversing 169 F.Supp. 2d 1181 (N.D. Cal. 2001)) (cert. denied, 547 U.S. 1163 (2006)). A Paris court imposed a fine on Yahoo! for allowing an auction of Nazi memorabilia. The District Court, Northern District of California, found for petitioner on First Amendment grounds and refused to order Yahoo! to block its content or to order any collection of a fine imposed by the French court. The 9th Circuit confirmed U.S. jurisdiction of the case but, in dismissing, offered no resolution regarding the conflict of laws.
compromise, suggesting that perhaps everyone could agree that they want to filter child pornography or instructions on how to create weapons of mass destruction.

In her final chapter, “From International Governance to International Internet Law,” Kulesza postulates that the world needs a framework on internet usage worldwide. She reviews the work of various authors on the cutting edge of the debate surrounding internet governance, whose ideas vary from maintaining nationality of content in cyberspace, giving the status of “common heritage of mankind” to the most necessary and basic of web resources, and creating separate “areas” of cyberspace populated by “netizens,” governed with their own laws but residing apart. With regard to ethics, she suggests a “jus internet,” meaning, simply, internet law, but implying, by using the latin, a just basis in social norms.

She argues that this overarching internet law makes sense to adopt because, even without sanctions, it will pay off in countries’ accountability through community. Finally, she proposes an Internet Framework Convention to create and summarize principles covering International Internet Law, not yet including an accountability mechanism, although Additional Protocols could define norms and obligations. A reader senses that she would like to see an international treaty, but has decided the world is not ready yet.

Kulesza summarizes at great length the real problems with internet usage, conflict of laws, and privacy, but I would have enjoyed more discussion on the
solution side. Kulesza appears overly optimistic and unrealistic at times. For example, she believes international governing law “pays off,” but simply because of mutual reciprocity where, as in Wikipedia, members obey the rules because “their power is the power of the community.” Given that, for example, the United States and China are diametrically opposed to each others’ views on filtering, the desire for such community itself may be lacking. Or she states that “the current challenge is the actual identification of the ethical rules that cyber-communities obey,” when in reality, Internet users may follow a code of ethics, or they may follow none. This idealizes the internet, as many people who tend to work in a medium wish to extoll the virtues of that medium.

Judges may be interested in this book, and it would be a great reference for anyone in the world looking to begin dialoguing on the international internet, for example, diplomats or United Nations ambassadors. However, I do not recommend this book for the lay reader. It reads like a dissertation thesis that was turned into a book, and upon researching the author’s biography, I found out this was exactly the case. The author’s knowledge is encyclopedic but this does not make this book accessible. The latin is pro forma, the text is cramped, and the part

---

7 Kulesza, supra note 1 at 151-52.
8 Kulesza, supra note 1 at 152.
9 Kulesza, supra note 1 at 152.
10 To find the information, go to this webpage, and click: “View on translate.google.com”: http://www.academia.edu/2024924/Miedzynarodowe_prawo_Internetu (last visited November 13, 2012).
most interesting to a lay reader, i.e., the author’s own argument and personal opinion, is sacrificed in place of thesis-type analysis of existing law.