

UC Irvine

UC Irvine Journal of International, Transnational, and Comparative Law

Title

Transnational Legal Ordering of Data, Disinformation, Privacy, and Speech

Permalink

<https://escholarship.org/uc/item/6512h6s3>

Journal

UC Irvine Journal of International, Transnational, and Comparative Law , 6(1)

Authors

Kaye, David

Shaffer, Gregory C.

Publication Date

2021-05-27

Transnational Legal Ordering of Data, Disinformation, Privacy, and Speech

David Kaye* & Gregory Shaffer**

This symposium addresses the governance of digital privacy and speech in two ways. First, it assesses the impact of regulation in one area on issues outside of it. Second, it shows how regulatory processes are transnational in scope, involving different forms of transnational legal ordering.

The symposium was held on September 11, 2020, marking the nineteenth anniversary of 9-11. Many readers will remember precisely where they were on that momentous day. In a strange way, 9-11 brought people around the world together, at least for a moment. Yet 9-11 occurred just before the world of connectivity changed in massive ways. It was only five years or so before the creation of YouTube, Twitter, and Facebook. So much has changed since 9-11, including the nature of information and how we share it, risks to privacy, challenges to democracy, and contestation over the ownership of data. We are pressed to think in new ways about the implications of regulation of information, privacy, and speech both domestically and transnationally, and how these different substantive areas interact.

Processes of transnational legal ordering begin with struggles over the framing of a problem that actors wish to be ordered through legal mechanisms.¹ That is the case with the issues of data privacy and speech in the broader global context. Is the problem to be defined in terms of individual privacy protection? Of social access to information? Of the integrity of political processes in light of disinformation campaigns? Of property rights and innovation? Of the free flow of data? Or otherwise? The framing of the problem shapes legal norms to address relevant state and non-state practices. Struggles over defining it implicate what is and what is not ordered through law.

* David Kaye is Clinical Professor, University of California, Irvine School of Law.

** Gregory Shaffer is Chancellor's Professor, University of California, Irvine School of Law. We thank my research assistant and the Editor-in-Chief of the journal, Allyson Myers, as well as the other journal members for their work.

1. TRANSNATIONAL LEGAL ORDERS 7-8, 38 (Terence C. Halliday & Gregory Shaffer eds., 2015).

Lawmaking occurs at multiple levels, from the international to the regional to national and sub-national levels. It involves both public lawmaking and rulemaking by private actors, including by companies creating and operating social media platforms. It encompasses both the extraterritorial application and impact of national law, and the deterritorial development and application of private rulemaking. Transnational legal ordering comprises the development, resistance, interaction, settlement, and unsettlement of these norms across different levels of social organization. Rulemaking by private bodies can feed back into shaping the understanding of public law, just as public law shapes private rule application and practice. There are, in short, multiple sites for the propagation of norms. What becomes “law” involves the dynamic development of norms across these sites, involving diagnostic struggles over the nature of the problem as well as recursive processes between public and private norm making and practice at different levels of social organization.

Take for example the area of trade law and the promotion of the “free flow” of data by the United States.² There are clashes of interest and ideological struggles among nation-states and private actors. Many trade lawyers, especially in the United States, focus on the liberalization of the digital economy and thus of data flows. They are concerned about the rise of data nationalism and the raising of border walls against data flows. These legal struggles affect the ability of companies to innovate, to develop an “Internet of Things,” and to improve performance. In opposition to this framing of the problem are those concerned with surveillance capitalism and the surveillance state that accumulate and use data to control us.

Very different templates for legal ordering are developed in competition with each other. Those pressing for a world of free data flows aim to develop a transnational legal order that ensures it. The European Union, in contrast, has developed a transnational legal order protecting data privacy, first within it, and then through exporting its legal norms transnationally as a condition for companies to access, transfer, and use personal data gathered from within the European Union. Other large developing countries, such as India, Indonesia, and Brazil, rather are interested in China’s model of data nationalism, which has given rise to huge Chinese companies that have exclusive access to data within China’s borders. These countries want to generate their own national “champions” in the digital economy. In parallel, national security and foreign policy concerns rise in prominence, as reflected in U.S. concerns over TikTok and WeChat and concerns regarding foreign interference in national elections. These concerns provide a new frame for assessing how to regulate the digital economy. In each case, issues are viewed within different lenses, shaping a legal response, which, in turn, implicates other social concerns.

2. Gregory Shaffer, *Trade Law in a Data-Driven Economy: The Need for Modesty and Resilience*, WORLD TRADE REV. (forthcoming 2021).

Huge corporations, having assets greater than the gross domestic product of many states, create their own standards and interact with governments. Given the challenges for reaching global agreement, civil society organizations engage directly with companies, often placing countervailing pressure on them in response to pressure they receive from governments, which corporations must navigate. Many political communities see problems as beyond the reach of public processes.

The concept of transnational law was made famous in a series of “Storrs lectures” given by Philip Jessup in 1956 at Yale Law School.³ Jessup coined the term transnational law to address the need for problem-solving at a time of cynicism during the Cold War regarding the prospects of international law and international organizations. Interestingly, Jessup himself was a victim of the Cold War as the U.S. government wished to have him appointed to the International Court of Justice, but McCarthyites within Congress accused him of being a Communist and blocked his designation. Jessup derived the concept of transnational law with the aim of supporting new governance arrangements at a time when international institutions were largely dysfunctional.

This symposium begins with *Regulating Disinformation in Europe: Implications for Speech and Privacy* by **Joris van Hoboken and Ronan Ó Fathaigh**. Their article addresses the interaction of privacy and speech implicated by the regulation of “disinformation” in the European Union.⁴ The authors categorize European disinformation regulation into four areas: (1) access to platform data, reflected in regulation requiring platforms to share data with academics for research purposes;⁵ (2) content-based restrictions on disinformation, reflected in laws prohibiting the manipulation of election-related information;⁶ (3) law enforcement cooperation, reflected in laws regarding the reporting of misleading internet content to authorities;⁷ and (4) the “pseudo-militarization” of disinformation regulation, implicating foreign policy.⁸

The authors examine the implication of these regulations for freedom of speech. Given the vagueness and subjectivity of the definition of “disinformation” under the law, the authors find that “public officials have great latitude in the type of content that may be labelled disinformation,”⁹ leading to potential censorship of

3. Gregory Shaffer & Carlos Coye, *From International Law to Jessup's Transnational Law, from Transnational Law to Transnational Legal Orders*, in *THE MANY LIVES OF TRANSNATIONAL LAW: CRITICAL ENGAGEMENTS WITH JESSUP'S BOLD PROPOSAL* 126, 126 (Peer Zumbansen, ed., 2020).

4. Joris van Hoboken & Ronan Ó Fathaigh, *Regulating Disinformation in Europe: Implications for Speech and Privacy*, 6 U.C. IRVINE J. INT'L, TRANSNAT'L & COMP. L. 9, 11 (2021).

5. *Id.* at 16–17.

6. *Id.* at 17–20.

7. *Id.* at 21–22.

8. *Id.* at 20–23.

9. *Id.* at 24.

lawful information. Disinformation regulation typically involves increased online monitoring and surveillance,¹⁰ providing governments with access to user data.¹¹

The article notes the potential of EU data protection law to confront disinformation by requiring transparency and consent to the processing of personal data.¹² This potential is important because “disinformation campaigns may involve the use of profiling of audiences with regard to their susceptibility to being misled by certain communications.”¹³ The data-driven profiling of audiences for purposes of disinformation can be addressed, in part, the authors contend, through data protection laws.

The authors develop an alternative for the future of European regulation, pointing to the European Democracy Action Plan. The Plan aims to combat disinformation through measures more in line with international human rights standards. It would, for example, fund projects to support “deliberative democratic infrastructures,” strengthen “media freedom and media pluralism,” and empower citizens “by strengthening media literacy.”¹⁴

evelyn douek’s article *The Limits of International Law in Content Moderation* responds to the call for social media platforms to implement international human rights principles as standards for speech-related decision-making, such as content moderation. Observing that social media companies have been eager to “jump on the bandwagon”¹⁵ of international human rights compliance, douek maintains that platforms are willing to do so at least in part because international human rights principles do not provide a real constraint on their activities.¹⁶ While douek is sympathetic to the proposition that international human rights law (IHRL) offers a useful framework for social media platforms in regulating content while respecting freedom of speech, she critiques this position.¹⁷ She finds that failing to acknowledge the limits of IHRL in constraining the activity of social media platforms serves to legitimize corporate practices, without benefiting social media users.¹⁸

douek’s article examines how social media platforms benefit from coopting the language of international human rights. Human rights discourse, she contends, provides social media platforms with legitimacy—similar to what Daniel Berliner

10. *Id.* at 25–26.

11. *Id.* at 26–29.

12. *Id.* at 32.

13. *Id.* at 34.

14. *Id.* at 34.

15. evelyn douek, *The Limits of International Law in Content Moderation*, 6 U.C. IRVINE J. INT’L, TRANSNAT’L & COMP. L. 37, 39 (2021).

16. *Id.* at 40.

17. Compare DAVID KAYE, *SPEECH POLICE: THE GLOBAL STRUGGLE TO GOVERN THE INTERNET* (2019).

18. *Id.* at 41.

and Aseem Prakash term “bluewashing.”¹⁹ douek summarizes the arguments of proponents of the use of international human rights law in social media content moderation as follows: IHRL provides an agreed-upon set of global rules, which is what is needed in a “borderless internet”;²⁰ it provides a common language for discussing issues of content moderation and censorship;²¹ it offers a strong normative ground from which social media platforms can resist authoritarian demands;²² it provides both procedural and substantive standards;²³ and, finally, it is the “least-worst option.”²⁴ douek nonetheless critiques this approach because of the indeterminacies, gaps, inconsistencies, and contestation over the meaning of IHRL norms. She contends that the constraints IHRL imposes on social media companies are quite limited in practice, providing them with great discretion in maintaining that they are complying with it. In addition, she argues, social media platforms lack the competence to properly adhere to the procedural requirements and engage in the substantive balancing of interests required under IHRL.²⁵ In her view, the problems raised by content moderation require shifting from individualistic rights to a systemic frame, for which IHRL does not yet provide a method because it so far has focused on individual cases.²⁶

Although she acknowledges the benefit of IHRL’s use as a common language to deliberate over the rules governing content moderation, she argues that there is need for an institutional structure that facilitates the conversation. Otherwise, there is too much reliance on platforms applying IHRL behind closed doors.²⁷ An external, public mechanism could check and contest platforms’ application of IHRL in order for IHRL to be applied to platform decision-making on content moderation in a more meaningful way.²⁸

Kyung Sin Park, in his article *Data as Public Goods or Private Properties?: A Way Out of Conflict Between Data Protection and Free Speech*, starts with a comparison of U.S. and EU privacy laws and follows the trans-Atlantic genealogy of modern data protection laws to Alan Westin’s concept of a property right in which “you own data about you.”²⁹ The ownership model is designed to compensate for a market

19. *Id.* at 40 (citing Daniel Berliner & Aseem Prakash, “Bluewashing” the Firm? Voluntary Regulations, Program Design, and Member Compliance with the United Nations Global Compact, 43 POL’Y STUD. J. 115, 132 (2015)).

20. *Id.* at 45–46.

21. *Id.* at 46–47.

22. *Id.* at 47.

23. *Id.* at 47–49.

24. *Id.* at 49.

25. *Id.* at 59–62.

26. *Id.* at 63–65.

27. *Id.* at 72.

28. *Id.* at 73.

29. Kyung Sin Park, *Data as Public Goods or Private Properties?: A Way Out of Conflict Between Data Protection and Free Speech*, 6 U.C. IRVINE J. INT’L, TRANSNAT’L & COMP. L. 77, 80 (2021).

failure in which the data subject is powerless to control and negotiate the terms of use of data. It thus creates “a default rule that one cannot collect or control data about another without explicit consent to such collection or use” since the data *belongs* to the latter.³⁰ Park contends that this ownership model is not workable or desirable in all circumstances. For example, some data, he contends, does not justify the ownership model because there is no market failure to be corrected for the information that data subjects already deliberately shared with the public without any restriction.³¹ Hence the exemptions in several countries’ data protection laws, such as in Europe. In parallel, he notes that U.S. privacy jurisprudence has reduced the scope of its “draconian third-party doctrine” that disregarded privacy whenever voluntary disclosure was made, opening the possibility for some transnational ordering on this issue.³²

Park theorizes the rationale for limiting the ownership model. He argues that presuming ownership as a default rule and then allowing for derogations on a case-by-case basis for publicly available data is too “parsimonious”³³ for the following reasons. First, data inherently “resist ownership in favor of [either] data subjects or in favor of data controllers.”³⁴ Because data is created by a shared interaction between the sensed being (the subject of the data) and the sensing being (the observer, or the data processor), ownership of that co-created data should be “an open question, not a deontological absolute.”³⁵ Second, data is often created for the purpose of diffusing knowledge, in which case data ownership should be interpreted so as not to favor repose, but sometimes diffusion and repurposing.³⁶ Third, it is often unclear who ought to own (or whether any one ought to own) data in the case of *relationally-created* or *transactionally-created* data.³⁷ Finally, Park emphasizes an element of property ownership favoring transfer, namely that “ownership exists not just to prevent use and transfer but to promote use and transfer[.]”³⁸

Park is concerned that a libertarian, ownership-based conception of data protection law will incentivize people to render data unavailable about themselves “to the point of rendering research of common benefit to all impossible.”³⁹ In order to avoid this “tragedy of data commons,” Park proposes data socialism: “the idea that data is one of such essential commodities or infrastructures that need to be left to public control, namely public properties.”⁴⁰

30. *Id.* at 92.

31. *Id.* at 85.

32. *Id.* at 88.

33. *Id.* at 93.

34. *Id.*

35. *Id.* at 94.

36. *Id.* at 94–95.

37. He provides the example of domestic violence offenders where the data of the offender was “created relationally” where the victim makes a public accusation. *Id.* at 95.

38. *Id.* at 97.

39. *Id.* at 98.

40. *Id.* at 99.

This symposium addresses the regulation of data, privacy, and speech in a world of highly contested norms involving competing priorities over the definition of the underlying problems to be addressed. The arenas in which these struggles occur are national, regional, and global, involving state and private rulemaking and practice, which can engage both international and transnational law. Developments in one arena implicate others, generating dynamic processes of transnational legal ordering that affect us as individuals and as members of different transnationally connected societies.

