Notre Dame Law Review Reflection

Volume 96 | Issue 4 Article 1

5-19-2021

Introduction

Mark P. McKenna
John P. Murphy Foundation Professor of Law, Notre Dame Law School; Director, Notre Dame Technology Ethics Center

SYMPOSIUM

INTRODUCTION

*Mark P. McKenna**

Julie Cohen's *Between Truth and Power* is, as Orly Lobel writes, a "dazzling tour de force" that "asks us to consider the new ways powerful actors extract valuable resources for gain and dominance."[1] As she has done so frequently, Cohen takes an incredibly complex story and weaves together a comprehensive narrative that changes the entire framing of legal questions. Agree or disagree with her diagnoses, no one who seriously engages this book will ever think about regulation in the information economy the same way.

In January 2020 (seemingly a lifetime ago, given what 2020 would bring), we gathered leading thinkers about the governance of new technologies at Notre Dame Law School and spent a day reflecting on the book and considering its implications across a range of areas. This symposium edition includes three essays that derive from those conversations, each focusing on just one of the many threads from that day.

Ari Waldman takes up Cohen's managerialism theme, focusing particularly on its impact on privacy.[2] Waldman persuasively describes managerialized privacy as driving structures and mechanisms that "focus[] on minimizing . . . impact on . . . innovation" instead of prioritizing privacy's substantive goals.[3] Waldman characterizes the resulting privacy regime as "compliance in name only" and "merely symbolic."[4] One might instead call the regime compliance only.

* John P. Murphy Foundation Professor of Law, Notre Dame Law School; Director, Notre Dame Technology Ethics Center.

1 Orly Lobel, *Biopolitical Opportunities: Between Datafication and Governance*, 96 NOTRE DAME L. REV. REFLECTION 181, 181 (2021) (citing JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF THE INFORMATIONAL CAPITALISM (2019)).

2 *See* Ari Ezra Waldman, *Outsourcing Privacy*, 96 NOTRE DAME L. REV. REFLECTION 194 (2021).

3 *Id.* at 195.

4 *Id.*

Managerialism has two dimensions in Waldman's telling—one at the level of regulatory apparatus, and one at the level of the entities being regulated.[5] But these are deeply related: the managerialized regulatory apparatus is much more likely to defer to managerialized privacy compliance structures.[6]

Here Waldman argues that the role of technology vendors is underappreciated in the privacy space.[7] Outsourcing, Waldman suggests, is usually reserved to functions that lie outside the "core competencies" of a firm.[8] "What does it say about companies" that they outsource important aspects of their privacy compliance while claiming that privacy matters to them so much?[9]

Those companies' reliance on outsourcing "chang[es] the medium through which . . . interpretation and implementation of legal rules . . . are performed—namely, from humans to technology."[10] "[O]utsourcing assessment management requires outsourcing legal interpretations" to "technologies . . . [that] embed[] . . . particular assumptions and interpretations of legal rules."[11] Similarly, incident response tools are marketed as guiding clients through (legally) "*correct*" responses and meeting mandatory timelines and notification requirements.[12] De-identification software is said to meet anonymization requirements, "translating a legal requirement into coding language."[13]

Waldman fears that courts and regulators will defer to these tools, treating them as industry standards and therefore regarding them as sufficient to meet legal obligations.[14] If that were to happen, the legal interpretations these technologies embed would, in a meaningful sense, create the new legal reality.

Waldman also argues that increased reliance on outsourced privacy will exacerbate inequalities between large corporate interests and everyone else.[15] Large companies have the advantage of size and scale to shape vendor relationships and products and, as a result, they can frame the legal

5 *See id.*

6 *Id.*

7 *Id.* at 195–96.

8 *Id.* at 197 (first citing James Brian Quinn, *Strategic Outsourcing: Leveraging Knowledge Capabilities*, SLOAN MGMT. REV., Summer 1999, at 9, 12; and then citing Peter Gottschalk & Hans Solli-Saether, *Critical Success Factors from IT Outsourcing Theories: An Empirical Study*, 105 INDUS. MGMT. & DATA SYS. 685, 686 (2005)).

9 *Id.* at 196.

10 *Id.* at 197.

11 *Id.* at 200–01.

12 *Id.* at 202 (quoting RESILIENT, BREACH NOTIFICATION UNDER THE GENERAL DATA PROTECTION REGULATION: NEW CAPABILITIES IN THE IBM RESILIENT INCIDENT RESPONSE PLATFORM (2018), https://www.ibm.com/downloads/cas/9WYZP24P).

13 *Id.* at 203.

14 *See id.* at 194–95.

15 *Id.* at 204–05.

interpretations embedded in technology in ways that benefit them and not competitors or consumers.[16]

Waldman also focuses on the big picture, describing several systemic dangers of managerialization of privacy, namely: (1) "reduc[ing] privacy to its codable pieces[;]" and (2) reducing privacy to the risk of being investigated (making it a compliance issue focused on corporate risk).[17] Those shifts inherently focus employees on the interests of their corporate employers rather than on the interests of users, making privacy primarily about avoidance of a corporate problem rather than advancement of an affirmative goal.[18]

In combination, outsourcing privacy compliance to technological tools risks erosion of legal expertise and loss of the qualitative dimensions that come with human judgment.[19] It also erodes accountability.[20] "Shifting . . . [to] the language of technology . . . empowers technologists" and "disempowers consumers, who [do not have] access to a technology-driven privacy discourse."[21] It is, after all, largely technologists that privacy law aims to constrain.

Orly Lobel picks up Cohen's call to "consider the new ways powerful actors extract valuable resources for gain and dominance."[22] But Lobel sees it as "a call to action," and she seeks to identify "ways in which governments can engage in new forms of governance to leverage the very same biopolitical data extracted by private actors for profit purposes, in service of public goals of fairness, equality, and distributive justice."[23] Specifically, Lobel explores "how datafication can, and indeed should, be employed to aid regulatory research, enforcement, and accountability."[24]

Rather than accepting that new technologies must be used extractively, Lobel articulates "a more positive vision, one [that] can . . . be constructed through engagement with new capabilities and recognition of the opportunities that data can offer."[25] Specifically, Lobel highlights three examples of "opportunities within disruptive technological changes," arguing that "policymakers have no choice but to . . . mirror, rather than attempt to block, these innovations."[26]

First, Lobel describes "[n]ew reforms . . . targeting . . . information asymmetries" regarding wage information, "imagin[ing] a role for digital platforms [to] create[] more systematic transparency" than "[s]elf-reported"

16 *Id.*
17 *Id.* at 205–06.
18 *Id.*
19 *Id.* at 207–08.
20 *Id.* at 208–09.
21 *Id.* at 209.
22 Lobel, *supra* note 1, at 181 (citing COHEN, *supra* note 1).
23 *Id.*
24 *Id.*
25 *Id.* at 193.
26 *Id.* at 182.

information.[27] New technologies can help "detect[] salary inequities, . . . uncover, and tame, persisting biases and narratives that contribute to inequality in the workplace" (e.g., "certain phrases used in [job ads]" that "decrease [the number of] women applicants").[28]

Lobel then focuses on ways that governments and private actors might turn data harvesting and extraction toward "public ends."[29] Here, she responds to Cohen's powerful description of the way "law enables . . . data harvesting and data enclosure . . . via platforms extracting massive amounts of [data] from users, turning the data into profitable resources" and "claiming ownership over th[e] extracted information."[30]

But, Lobel notes, there's nothing inevitable here—these tools can be used for public good. New companies, for example, sometimes offer services that depend on scraping technologies "to cities to monitor short term rentals" to help ensure "compliance with local laws."[31] Importantly, however, Lobel notes that scraping has uncertain legal status, and for that sort of public-oriented vision to come to fruition, the law would need to continue to evolve.[32]

Lastly, Lobel suggests that new technologies can be harnessed for public health purposes.[33] She notes, for example, the ways technologies have complemented responses to the COVID-19 pandemic, at least in some countries.[34] One challenge here is a potential clash with privacy values.[35] Another is rejection of what some would regard as a form of tech solutionism. But Lobel remains optimistic that technology can serve a valuable role here too.

Felicia Caponigri "proposes cultural heritage as a subject matter worthy of . . . analysis" in light of Cohen's characterization of "labor, land, and money" as "tangible[s]" that have been "dematerialized . . . and then reified . . . as information."[36]

---

27 *Id.* at 183.

28 *Id.* at 184.

29 *Id.* at 185.

30 *Id.* (citing COHEN, *supra* note 1, at 44–45).

31 *Id.* (citing Tom Banse, *Pacific Northwest Cities Hire Outside Vendors to Police Airbnb-Type Rentals*, NW NEWS NETWORK (Aug. 22, 2018), https://www.nwnewsnetwork.org/post/pacific-northwest-cities-hire-outside-vendors-police-airbnb-type-rentals).

32 *Id.* at 190 ("[I]n an age where data extraction is the key to tech's future, web scraping law should be designed to enable more transparency, research, accountability, and competition.").

33 *See id.*

34 *Id.* at 190–92.

35 *Id.*

36 Felicia Caponigri, *Cultural Heritage Law Between Truth and Power: Law's Evolution and Our Collective Cultural Interest in an Informational Economy*, 96 NOTRE DAME L. REV. REFLECTION 163, 165–66 (2021) ("If cultural heritage is increasingly seen as information, as data to be consumed all over the world, how should cultural heritage law regulate this cultural information, if at all?").

The most significant tension here is between cultural property's traditional focus on the material object, which manifests in part in restrictions on reproductions and imposition of a duty to preserve the material object, and the institution of digitization efforts (which are themselves preservation tools).[37] But when "[c]ultural property is reproduced and then becomes reified anew through images shared on Instagram[,] it exists as information or data with which we interact in networked infrastructures."[38]

Here's a fundamental conflict: "[T]he reproductions of cultural properties on social media and digital platforms . . . now, at the very least, help produce the very public cultural interests in cultural property which Italian cultural property law is meant to preserve and protect."[39] How, then, can cultural property law evolve to recognize the value of digitization, and the reality that it creates new cultural meaning, when the concept itself is rooted in preservation?

Caponigri also worries about power structures, as Cohen implores us to do. More specifically, Caponigri wonders about the changes that will inevitably result from digitization if it shifts responsibility for determining what counts as cultural property away from public institutions and to private companies.[40] The "who decides" question looms large in cultural property, since it purports to reflect common cultural value. But we should be more worried about putting those decisions in private hands, for many of the reasons Cohen articulates.

These essays come from very different perspectives and have different goals. But collectively they reflect the range of conversations Cohen's book provokes, and we were grateful to have the opportunity to engage with such a distinguished group of participants.

37 *See id.* at 172–73.
38 *Id.* at 172.
39 *Id.* at 173.
40 *Id.* at 176–77.