Idaho Law Review

Volume 51 | Number 3 Article 1

March 2019

The Limits of Industry-Specific Privacy Law

BJ Ard

THE LIMITS OF INDUSTRY-SPECIFIC PRIVACY LAW

BJ ARD*

TABLE OF CONTENTS

I. INTRODUCTION

The Internet raises several challenges for privacy law. In particular it often disrupts laws that regulate specific industries. As prior scholarship has shown, industry-specific laws are prone to circumvention and obsolescence whenever firms outside the covered industry begin collecting and using the same sorts of data.[1] And the rapid birth (and death) of online business models makes these sorts of disruptions increasingly common.[2] The resulting scheme is one that has sustained substantial criticism for drawing arbitrary distinctions between entities collecting the same sorts of personal information.[3]

This essay argues that the distinct features of online commerce not only challenge discrete industry-specific laws, but also expose more fundamental difficulties for the industry-specific approach. The piecemeal enactment of laws regulating

* Ph.D. Candidate in Law, Yale University, and Resident Fellow at the Yale Information Society Project. J.D. 2010, Yale Law School. I would like to thank Kiel Brennan-Marquez, Lauren Henry, Christine Jolls, Margot Kaminski, David Medine, Bilyana Petkova, Sofia Ranchordás, Yana Welinder, and my colleagues at the Yale Information Society Project for invaluable feedback on this project, as well as the participants at the 2015 Idaho Law Review Symposium on Privacy in the Age of Pervasive Surveillance. Responsibility for any loopholes or obsolescence rests with the author.

1. *See, e.g.*, Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 923–25 (2009) (describing the challenges that telecommunications convergence poses for laws premised on stable divisions between types of broadcasters or platforms). Technology-specific laws face comparable challenges when firms use non-covered technologies to collect the sorts of data the laws are meant to protect. *See, e.g.*, Michael Birnhack, *Reverse Engineering Informational Privacy Law*, 15 YALE J.L. & TECH. 24, 38–42 (2012) (arguing that flexibility is one of the main advantages that legislators seek through technology-neutral privacy laws).

2. *See* Part II.A, *infra*.

3. Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 257 (2011) (articulating this position as the prevailing critique of U.S. privacy statutes).

specific industries may have been effective in a time when lawmakers could identify all the industries involved in a particular data-collection practice and trust that new industries would not soon enter the same niche. Indeed, when the business landscape is stable, this approach may offer advantages insofar as it allows lawmakers to tailor their interventions to the specific incentives and norms of the regulated industries. But the information age creates at least three complications for industry-specific lawmaking.[4] First, the accelerated rate of entry that characterizes online commerce makes it hard for legislators to keep pace on an industry-by-industry basis. Second, the intermediation of online transactions by third parties—parties ranging from Internet service providers to search engines, advertising networks, and financial institutions—exposes gaps in any intervention that targets only the industry itself without accounting for these intermediaries.[5] And third, the relative obscurity of online surveillance makes it difficult for lawmakers to identify and target the right class of entities through the industry-specific paradigm. Neither legislators nor their constituents are well equipped to deal with surveillance practices that are invisible to them.

The argument proceeds in three parts. Part I demonstrates the limits of industry-specific privacy laws and lawmaking by reference to the regulation of "book services" under the California Reader Privacy Act of 2011 ("CRPA")[6] and "financial institutions" under the Financial Privacy Rule of the Gramm-Leach-Bliley Act ("GLBA").[7] Part II explains in greater detail why rapid turnover, dense intermediation, and lack of transparency render the industry-specific approach untenable for regulating commerce online. Part III explores three possibilities for responding to these challenges: (1) moving from industry-specific privacy laws to more transaction-centered approaches; (2) making contemporary data-collection practices more transparent, and thereby more amenable to regulation; and (3) looking beyond Congress to consider the role that more agile bodies like administrative agencies or state lawmakers play in responding to changes in technology and business methods.

II. INDUSTRY-SPECIFIC PRIVACY LAWS

The following examples illustrate the coverage problems that undermine industry-specific laws as business models change. The CRPA fails to protect the very digital reading records it was meant to cover because its definition of "book services" is too narrow. Besides overlooking common intermediaries like Internet service providers, the Act seems to exclude Google Books and other services that are

4. *See* Part II, *infra*.

5. This understanding of the shortcomings in industry-specific privacy laws—that they fail to regulate intermediaries and interlopers despite their entanglement with the covered entity—treads common ground with Anita Krug's critique of entity-centric financial regulations. *See generally* Anita K. Krug, *Escaping Entity-Centrism in Financial Services Regulation*, 113 COLUM. L. REV. 2039 (2013). Krug argues that entity-centric regulations, which regulate financial firms as though they were standalone entities, cannot achieve their purposes without also speaking to the complex web of affiliates, parent companies, or subsidiaries instrumental to a firm's operations. *See id.* at 2043–44.

6. CAL. CIV. CODE §§ 1798.90–1798.90.05 (West 2012).

7. 15 U.S.C. §§ 6801–6809 (2012).

funded by advertising. The GLBA's Financial Privacy Rule encountered similar functional obsolescence almost as soon as it passed. While Congress attempted to protect consumers' financial information by regulating "financial institutions," advances in computing power delivered retailers the tools to assemble detailed consumer dossiers without the banks' assistance.

A. California Reader Privacy Act

Industry-specific limitations can render laws obsolete even in the regulation of the very activities for which they are designed. Consider library confidentiality laws. Following the conventional critique of our piecemeal approach to privacy law, one might argue that these laws are defective in protecting reader privacy to the extent they draw arbitrary lines in the treatment of libraries, bookstores, and online databases.[8] But the laws now face a more fundamental problem. They fail to protect records that arise from library activity itself unless they cover the various cloud-computing platforms, e-book providers, and other intermediaries that have become integral to the delivery of library services.[9]

The CRPA repeats the same mistakes. California enacted the law to cover booksellers with privacy protections like those that already cover libraries and video stores.[10] The Act's sponsors were specifically concerned with protecting privacy in the face of changing reading habits, particularly the adoption of e-books.[11] Notwithstanding the drafters' intent to address the challenges of the digital medium, the CRPA's industry-specific limits undermine its ability to cover emergent practices in the distribution of digital books.

The Act only regulates disclosures by a "book service," defined as "a service that, as its primary purpose, provides the rental, purchase, borrowing, browsing, or viewing of books."[12] The definition further excludes stores where book service sales "do not exceed 2 percent of the store's total annual gross sales of consumer products sold in the United States."[13] One gap in coverage therefore arises when a book provider funds itself by means other than the sale of books. No one sells more

---

8. *Cf.* Anne Klinefelter, *Library Standards for Privacy: A Model for the Digital World?*, 11 N.C. J.L. & TECH. 553, 561 (2010) (arguing for the extension of library privacy laws to these contexts). For background reading on the importance of reader privacy, see generally Marc Jonathan Blitz, *Constitutional Safeguards for Silent Experiments in Living: Libraries, the Right To Read, and a First Amendment Theory for an Unaccompanied Right To Receive Information*, 74 UMKC L. REV. 799 (2006); Julie E. Cohen, *A Right To Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981 (1996); and Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387 (2008).

9. *See generally* BJ Ard, *Confidentiality and the Problem of Third Parties: Protecting Reader Privacy in the Age of Intermediaries*, 16 YALE J.L. & TECH. 1 (2013) (exploring the library confidentiality regime's difficulties regulating non-librarian third parties like Amazon when they deliver library services); Michael Zimmer, *Patron Privacy in the "2.0" Era: Avoiding the Faustian Bargain of Library 2.0*, 22 J. INFO. ETHICS 44 (2013) (examining the challenges that Web 2.0 technologies pose for librarians' privacy commitments).

10. *See* CAL. S. REP. S.B. 602, 2011 WL 1364760, at 8 (2011) (Comm. Rep.).

11. *See id.* at 1–3.

12. CAL. CIV. CODE § 1798.90(b)(2) (West 2012).

13. *Id.* Relatedly, the law restricts its scope to "commercial entities" that provide book services. *Id.* § 1798.90(b)(6).

books online—electronically or in hardcopy—than Amazon.[14] Yet book sales represent only a fraction of its total business: books accounted for 7 percent of Amazon's revenues last year.[15] One can imagine a future where Amazon so diversified its business that it moved beyond the reach of the statute. Google—which provides millions of users with limited unpaid access to books via its Google Books service and sells books on Google Play alongside apps and other media—already appears to fall short of the 2 percent threshold.[16]

It would not be surprising, moreover, if a future book service went further than Google Books in giving books away for "free." Many online services—take Spotify[17]—now provide access to digital media without charging the user and make money through some combination of advertisement and monetization of user data.[18] A book service that made its money off advertisements rather than by charging for books could colorably argue that the statute did not apply to its activities. Unfortunately for California readers, this could mean that the businesses most interested in the trafficking of user data were not subject to the CRPA.

Even if California were to iron out the wrinkles in its definition of book service, the CRPA would still provide little protection against digital intermediaries and eavesdroppers. The Act operates by limiting the book service's ability to disclose reading records to third parties. It does not address the possibility that third parties might collect users' reading records directly without need for such disclosure. Some of these third parties might learn our reading preferences in the course of facilitating our online transactions. Internet Service Providers ("ISPs"), for example, would know which books we browsed at Amazon or Project Gutenberg unless those pages were encrypted.[19] And while we might purchase a book at the corner store using cash, few people pay anonymously online. This means that our credit card providers—or online alternatives like PayPal or Google Wallet—are also privy to our book purchases.

---

14. *See* Polly Mosendz, *Amazon Has Basically No Competition Among Online Booksellers*, THE WIRE (May 30, 2014, 2:44 PM), http://www.thewire.com/business/2014/05/amazon-has-basically-no-competition-among-online-booksellers/371917/.

15. Jeff Bercovici, *Amazon vs. Book Publishers, By the Numbers*, FORBES (Feb. 10, 2014, 2:49 PM), http://www.forbes.com/sites/jeffbercovici/2014/02/10/amazon-vs-book-publishers-by-the-numbers/.

16. Financial coverage from last year suggests that Google Play makes up 10 percent or less of Google's total revenue. Steve Symington, *How Google Play Is Serving Up Stunning Growth*, MOTLEY FOOL (June 26, 2014), http://www.fool.com/investing/general/2014/06/26/googles-latest-growth-driver-is-just-getting-start.aspx. The same analysis suggests that as much as 98 percent of Google Play's own revenue comes from in-app purchases within free-to-download apps, particularly games. *Id.* Book sales would therefore need to account for nearly 20 percent of in-app purchases—if they fall into the category of in-app purchases at all—for Google to meet the 2 percent statutory threshold.

17. Spotify is a popular music-streaming service that allows users to listen to the music of their choice for no charge. *See* SPOTIFY, https://www.spotify.com/us/ (last visited Mar. 31, 2015). Like many free services online, Spotify makes money by advertising to these listeners.

18. *See generally* Chris Jay Hoofnagle & Jan Whittington, *Free: Accounting for the Costs of the Internet's Most Popular Price*, 61 UCLA L. REV. 606 (2014) (describing this business model and its consequences for consumer welfare).

19. *See* Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417, 1422 (2009) ("The ISP operates the network chokepoint—its computers stand between the user and the rest of the Internet—and from this privileged vantage point it has access to all of its users' private communications.").

Other third parties simply eavesdrop on our book-browsing activities, collecting user data without playing an intermediary role. A user might ignorantly download a third-party cookie that collected detailed records of her browsing activities, providing that party with an activity log comparable to that held by an ISP.[20] Or a company might release an e-reader that wirelessly reported all its contents to the manufacturer. Assuming that the manufacturer stayed out of the business of selling books, it could ostensibly collect detailed records on its customers' reading habits without qualifying as a book service.[21] Without coverage as to parties like these—parties whose very business model involves collecting and exploiting user data—the Act would offer extraordinarily thin protection for the digital reading practices it aimed to cover.

B. Gramm-Leach-Bliley's Financial Privacy Rule

The GLBA's Financial Privacy Rule imposes nondisclosure obligations on financial institutions like banks and credit card issuers.[22] Congress enacted this measure in 1999 in response to concerns that banks were abusing consumers' personal information by selling it to telemarketers and other third parties.[23] The Rule is a partial success insofar as it imposes new barriers against marketers who would like to subsume centralized records of our transaction histories, like our checking ledgers and our credit-card statements, into detailed consumer dossiers.[24]

But industry-specific regulations targeted at financial institutions work well only so long as we can assume that only one's bank or credit card issuer—or a consumer reporting agency, which is subject to a separate industry-specific law in the Fair Credit Reporting Act[25]—could maintain a detailed consumer profile. This

---

20. *See* Hoofnagle & Whittington, *supra* note 18, at 627 (quoting a report from 2010 finding that "the nation's 50 top websites on average installed 64 pieces of tracking technology onto the computers of visitors, usually with no warning"); Woodrow Hartzog, *Chain-Link Confidentiality*, 46 GA. L. REV. 657, 680 (2012) ("Websites that use cookies, Web bugs, and other data collection technologies have access to a host of information, including comprehensive browsing and search histories, payment information, and contact information such as addresses, phone numbers, and e-mail addresses.") (footnotes omitted).

21. *See* Ard, *supra* note 9, at 49 (contemplating the difficulties such a device might present).

22. *See* 15 U.S.C. §§ 6801-6809 (2012). Many commentators question the efficacy of the law in practice given that few consumers read the notices required under the law or exercise the opt-out rights the law provides. *See* Edward J. Janger & Paul M. Schwartz, *The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. 1219, 1220 (2002). One need not be paranoid to wonder, for example, how a credit card issuer like Capital One exercises the option it has reserved to share personal information for "nonaffiliates to market to you," where "nonaffiliates" expressly include "insurance companies, service providers, co-branded partners, retailers, data processors, and advertisers." *See* Capital One, *What Does Capital One® Do With Your Personal Information?* (Feb. 2013 revision), *available at* www.capitalone.com/identity-protection/privacy/?nojs. But assessment of how the law works in practice is beyond the scope of this essay, which focuses on shortcomings that become apparent even if we limit our examination to the law's formal coverage.

23. *See* H.R. REP. NO. 106-434, at 171 (1999) (Conf. Rep.).

24. For an introduction to the privacy issues that dossiers like these pose, see Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1095 (2002) ("[D]igital dossiers are increasingly becoming digital biographies, a horde of aggregated bits of information combined to reveal a portrait of who we are based upon what we buy, the organizations we belong to, how we navigate the Internet, and which shows and videos we watch.").

25. *See* 15 U.S.C. § 1681(a).

might have been a fair assumption in an earlier decade, when the expense required to maintain the transaction history for a given credit card, link the card to a specific person, and track down her mailing address was too much to bear without the assistance of the credit card company. In some instances state law even operated to keep these costs high. California's Song-Beverly Credit Card Act of 1971, for example, attempts to thwart unwanted marketing by barring retailers from collecting personal identifiers such as zip codes as a condition of accepting a credit-card payment.[26]

The roadblocks imposed by the GLBA are all but irrelevant in the twenty-first century, however, given that the declining costs of computing have enabled retailers to construct elaborate consumer profiles by directly monitoring their customers' shopping habits.[27] Target, for example, employs algorithms that identify shoppers whose purchases indicate pregnancy and then mails them baby-related coupons.[28] This practice has become (in)famous for outing an expectant teen to her own father before she made the decision to share the news.[29]

Retailers and advertisers also leverage modern networking technologies to pool their information and scour public records to draw inferences that might not be apparent from a customer's purchases at any one store. The sharing arrangements have borne disquieting fruit. Grieving father Mike Seay once received a marketing letter from OfficeMax addressed to "Mike Seay, Daughter Killed in Car Crash."[30] OfficeMax subsequently explained that this mailer was the result of "information they unintentionally bought from a third party data broker."[31] A closer look at the sorts of lists available for purchase reveals that people have been grouped into categories touching on the most intimate details of personal life, ranging from lists of people who take Prozac to survivors of rape and AIDS patients.[32] Others group people by their religion (lists of persons who believe in the Bible), ethnicity ("Affluent Hispanics"), or sexuality ("the Gay America Megafile").[33]

This is not to single retailers out for derision. The roles that different industries play in the creation of dossiers like these is obscure, and deliberately so. Firms

---

26. CAL. CIV. CODE § 1747.08 (West 2012); Pineda v. Williams-Sonoma Stores, Inc., 246 P.3d 612 (Cal. 2011). *But see* Apple, Inc. v. Superior Court, 292 P.3d 883 (Cal. 2013) (rejecting the application of the law to online transactions).

27. *See* Harry Surden, *Structural Rights in Privacy*, 60 SMU L. REV. 1605, 1617 (2007) ("Since structural constraints employ costs and barriers to regulate, anything that tends to reduce these costs or undermine these barriers significantly reduces their regulatory effectiveness.").

28. FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 28–29 (2015); Omer Tene & Jules Polonetsky, *A Theory of Creepy: Technology, Privacy, and Shifting Social Norms*, 16 YALE J. L. & TECH. 59, 66–68 (2013) ("Target assigns customers a pregnancy prediction score, which is based on their purchase habits, in order to beat its competitors in identifying a precious moment when shopping habits are most amenable to change—the birth of a baby.").

29. *See* PASQUALE, *supra* note 28, at 29.

30. *See* Kashmir Hill, *OfficeMax Blames Data Broker for 'Daughter Killed in Car Crash' Letter*, FORBES (Jan. 22, 2014, 12:09 PM), http://www.forbes.com/sites/kashmirhill/2014/01/22/officemax-blames-data-broker-for-daughter-killed-in-car-crash-letter/.

31. *Id.*

32. *See* Daniel Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 22 (2014); Joshua L. Simmons, *Buying You: The Government's Use of Fourth-Parties to Launder Data About "The People,"* 2009 COLUM. BUS. L. REV. 950, 991 (2009).

33. *See* DANIEL SOLOVE, THE DIGITAL PERSON 22 (2004); Simmons, *supra* note 32, at 991.

share the intuition that customers would not approve of these practices and (ironically) bind the recipients of customer information to keep their sources secret.[34] The point here is that regulation of privacy in consumer transactions defies any approach that regulates a single industry, whether it be banking or retail. This atmosphere of obscurity, moreover, makes it difficult for consumers and regulators to track the data flows or hold the relevant actors accountable.

III. CHALLENGES OF E-COMMERCE

A. Rapid Change

The Internet raises three challenges for the industry-specific approach. The first arises from the rapid turnover of firms online.[35] For better or worse, the Internet has heralded a disruptive cycle that ushers new industries into the market while displacing the incumbents.[36] New entrants might take on the portfolios of older players, as Google and other search engines have supplanted libraries in answering reference questions. Or they might engage in collection and disclosure practices with no direct precedent, like advertising networks' use of cookies to monitor a user's browsing patterns across the Internet. Without some mechanism to expand privacy commitments to new industries on a regular basis, industry-specific laws have become particularly prone to obsolescence in the digital age.

B. Pervasive Intermediation

The second challenge arises from the intermediation of online activity. Suppose that Maxwell and Pete want to purchase hammers. In the pre-digital world Maxwell might go to Sears and purchase his hammer directly. Only Maxwell and Sears would be privy to this one-to-one transaction. Even if Maxwell placed his order by phone, moreover, the telephone and delivery service would not typically know the content of the transaction. Putting their heads together, they would only know that Maxwell called Sears and subsequently received a package weighing about 16 ounces.

If Pete bought his hammer online, he would expose the details of his transaction to a much larger cast of characters. Even if Pete went directly to sears.com, he

---

34. PASQUALE, *supra* note 28, at 145.

35. This challenge is a version of the "pacing problem" that scholars like Gary Marchant have identified, whereby the "growing gap between the pace of technology and law" results in "increasingly outdated and ineffective legal structures, institutions and processes to regulate emerging technologies." Gary E. Marchant, *The Growing Gap Between Emerging Technologies and the Law*, *in* THE GROWING GAP BETWEEN EMERGING TECHNOLOGIES AND LEGAL-ETHICAL OVERSIGHT: THE PACING PROBLEM 19, 19 (Gary E. Marchant, Braden R. Allenby & Joseph R. Herkert eds. 2011); *see also* Lyria Bennett Moses, *Recurring Dilemmas: The Law's Race To Keep Up with Technological Change*, 2007 U. ILL. J.L. TECH. & POL'Y 239, 264–69 (2007) (explaining how technological change can render laws obsolete).

36. *See, e.g.*, CLAYTON M. CHRISTENSEN, THE INNOVATOR'S DILEMMA: WHEN NEW TECHNOLOGIES CAUSE GREAT FIRMS TO FAIL (rev. ed. 1997) (developing the idea of "disruptive innovation"); *id.* at xxvi ("Not surprisingly, the Internet looms as an infrastructural technology that is enabling the disruption of many industries."); *see also* Neal Katyal, *Disruptive Technologies and the Law*, 102 GEO. L.J. 1685, 1685 (2014).

would encounter the ubiquitous "share" buttons for Facebook, Twitter, and Google+.[37] Buttons like these often embed code that allows sites like Facebook to monitor their users' activities regardless of whether they actually click the button.[38] These forms of surveillance are joined by more invasive cookies that monitor browsing activity without the need for a button embedded on the page, to say nothing of the constant flow of data to one's ISP.[39] The web would grow even more tangled if Pete began with a Google search ("If I had a hammer…") rather than going directly to Sears. Google would then be able to add this query to Pete's search history. More surprisingly for Pete, if Pete followed Google's link to Sears then Google would tell Sears exactly what search query Pete had entered.[40]

Setting aside for the moment our concerns with targeted advertisements, we might not lose sleep over a world where dozens of third parties knew we wanted to purchase a hammer. Where these forms of intermediation characterize the majority of our online experience, however, we have reason to be concerned that industry-specific laws may fail to vindicate privacy commitments that we hold quite dear. We might be troubled, for example, by our loss of intellectual privacy when library- or bookseller-centric laws did nothing to prevent legions of intermediaries from learning and disclosing what we have read.[41] We might likewise be concerned about the loss of health privacy that would follow if search engines and advertisement networks could freely eavesdrop as we searched for information on an embarrassing rash or for the number to a suicide prevention hotline. The intermediation and surveillance characteristic of electronic commerce beggars any regulatory approach premised on the regulation of specific entities engaged in neat one-on-one transactions.[42]

C. Obscurity of Surveillance

The third challenge lies in the relative obscurity of these third parties. A reasonably savvy user might intuit that Google tracked one's search history and scanned one's Gmail messages or that the Washington Post kept a log of which stories the user had read.[43] The user might even understand—albeit dimly—that Google or the Washington Post retained the option under its privacy policy to dis-

---

37. SEARS, http://www.sears.com/ (last visited Mar. 31, 2015) (search for "hammer" and browse the resulting links).

38. Riva Richmond, *As 'Like' Buttons Spread, So Do Facebook's Tentacles*, N.Y. TIMES: BITS BLOG (Sept. 27, 2011, 3:51 PM), http://bits.blogs.nytimes.com/2011/09/27/as-like-buttonsspread-so-do-facebooks-tentacles/.

39. *See supra* notes 19–20 and accompanying text.

40. *See* Hoofnagle & Whittington, *supra* note 18, at 643 ("[R]eferrer headers indicate information about users' intentions, and in the case of Google, they often reveal the specific search string entered by the user.").

41. *See* sources cited *supra* note 8 (articulating the importance of intellectual privacy for personal development and the advancement of public discourse).

42. *Cf.* Krug, *supra* note 5, at 2044 (developing a similar critique of entity-centric regulations in consumer finance).

43. The *Washington Post* comes to mind because of its early deployment of a "social reader" app, which automatically posted the user's reading history to her Facebook News Feed, often without the user's knowledge. *See* Neil M. Richards, *The Perils of Social Reading*, 101 GEO. L.J. 689, 713–714 (2013).

close the records to third parties.[44] That user might be quite surprised to learn that the site had invited several third-party sites to directly observe the user's activities.[45] Add to these the invisible third parties the user might bring in the form of tracking cookies installed from elsewhere.[46] Users are hard pressed to regulate their own disclosures when they do not know who is surveilling them. Lawmakers, for their part, can hardly respond to activities that are invisible to them and to their constituencies.

* * *

Collectively these features of electronic commerce increase not only the public burden of firms' data collection practices but also the complexity of lawmaking. The increased burden is relatively easy to see. Where changed business practices render laws obsolete, the public does not receive the intended benefit of the laws. Where the surveillance itself is opaque—as surveillance by intermediaries often is—members of the public may also lose privacy by disclosing facts they would have withheld had they known who was really watching.

Lawmaking is made more difficult because the public faces challenges in organizing around rapidly changing, technically dense, and largely invisible issues of surveillance. Public choice theory predicts that a minority bloc with concentrated interests (like firms who benefit from lax privacy regulation) will often wield more political influence than a majority with more diffuse interests (like the general public that would favor expanded privacy protection).[47] As Neil Komesar argues, one factor that works in favor of more concentrated interest groups is their greater access to information concerning what's at stake.[48] The more complex or obscure the disputed practice, the less likely it is that those with more diffuse interests will be able to understand the impact of the practice on their own lives, much less to mobi-

---

44. Any such understanding would be attenuated, however, by the privacy policies' lack of detail regarding the identities or number of third parties implicated. *See* Clark D. Asay, *Consumer Information Privacy and the Problem(s) of Third-Party Disclosures*, 11 NW. J. TECH. & INTELL. PROP. 321, 324 (2013) (arguing that "consumers receive little to no information about who specifically will receive their information and how they will use it").

45. As one correspondent at the Washington Post explained:

> When your browser landed on this article, it didn't just talk to the friendly servers at washingtonpost.com. It also made contact with Chartbeat, a company that helps us understand where else you've been on the Web, and how you're interacting with the site. Your browser also connected to a personalized news applet called Trove, various marketing plug-ins and a social bookmarking service run by a company known as AddThis.

Brian Fung, *Who Tracks the Trackers that Track You Online? You Can, with Lightbeam*, WASH. POST: THE SWITCH (Oct. 30, 2013), http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/30/who-tracks-the-trackers-that-track-you-online-you-can-with-lightbeam/.

46. *See supra* note 20 and accompanying text.

47. *See, e.g.*, William N. Eskridge, Jr., *Dynamic Statutory Interpretation*, 135 U. PA. L. REV. 1479, 1530 (1987) (articulating public choice theory's prediction that legislatures will pass few laws that benefit the general public "because they rarely stimulate the formation of supportive interest groups").

48. NEIL K. KOMESAR, IMPERFECT ALTERNATIVES: CHOOSING INSTITUTIONS IN LAW, ECONOMICS, AND PUBLIC POLICY 71–73 (1994).

lize a campaign to advance their interests.[49] Rapid shifts in business practices, the unprecedented complexity hidden below the surface of simple transactions, and the general invisibility of data collection and disclosure online therefore raise the costs of political action and threaten to sap popular will for new privacy laws. These added difficulties for political action are troubling given how rapidly an industry-specific regime can fall into obsolescence without new and revised laws.

IV. BEYOND INDUSTRY-SPECIFIC LAW

The preceding discussion has outlined the challenges that the Internet poses for industry-specific privacy laws and industry-specific approaches to privacy law. While it is beyond the scope of this essay to offer a comprehensive alternative paradigm, the following sections outline three avenues for further consideration: the translation of industry-specific laws to transaction-centered regimes; enhanced transparency; and increased reliance on agencies and other institutions equipped to respond to rapid change.

A. Transaction-Centered Interventions

Many industry-specific privacy laws could be translated into terms that were industry-neutral but transaction-specific. In other words, lawmakers could define a law's scope by reference to the kinds of activity they wished to regulate rather than by reference to the industry currently conducting that activity.

Some laws have already achieved this result. Take the Fair Credit Reporting Act ("FCRA"). On its face it looks like an industry-specific law: it covers only "consumer reporting agencies."[50] But tracing the definitions provided by the Act reveals that a "credit reporting agency" includes anyone in the practice of furnishing reports for the purpose of establishing a consumer's eligibility for credit, insurance, or employment.[51] This open-ended definition provided the basis for an FTC action against Spokeo, a "people search" website, for collecting consumers' information from social media sites and selling it to prospective employers without adhering to the Act.[52] Any party who engages in the targeted transaction—providing reports used to evaluate someone's credit or employability—must accordingly be mindful of the FCRA.

---

49. *See id.* at 71 ("[O]ne important form of information is the basic recognition of the existence of an interest. . . . The more complex the social issue the more difficult or expensive it is to recognize one's position.").

50. *See* 15 U.S.C. § 1681b (2012) ("[A]ny consumer reporting agency may furnish a consumer report under the following circumstances and no other . . . .").

51. *See id.* § 1681a(f) (defining "consumer reporting agency" as one engaged in the practice of "furnishing consumer reports to third parties"); *id.* § 1681a(c) (defining "consumer report" as any communication that is used or expected to be used in establishing eligibility for credit, insurance, or employment).

52. *See* Press Release, Fed. Trade Comm'n, Spokeo To Pay $800,000 To Settle FTC Charges Company Allegedly Marketed Information to Employers and Recruiters in Violation of FCRA (June 12, 2012), *available at* https://www.ftc.gov/news-events/press-releases/2012/06/spokeo-pay-800000-settle-ftc-charges-company-allegedly-marketed.

Laws can also be drafted to curtail surveillance by digital intermediaries. The GLBA Security Rule effectively excludes third parties from eavesdropping on bank transactions: it imposes on each financial institution a "continuing obligation . . . to protect the security and confidentiality of [its] customers' nonpublic personal information" and authorizes agencies to establish security standards,[53] including encryption requirements that reduce the likelihood that financial records will leak to unauthorized intermediaries or eavesdroppers.[54] The result is to make it quite difficult for intermediaries to intercept communications between the consumer and a financial institution. To make the point a bit more concrete: try to recall the last time you received a bank statement by e-mail as opposed to an invitation to view the statement on a secure website hosted by the bank.

Short of excluding intermediaries from our transactions via security rules and encrypted communications, we could imagine transaction-centered privacy regimes that simply attached the same obligations to all parties to an online transaction, whether the party was the direct service provider, a facilitating intermediary, or an eavesdropping advertiser. Legislators might amend the CRPA, for example, to cover all parties to a book sale or book-lending transaction rather than cover the book service alone.[55]

Transaction-centered laws are well suited to preserve privacy commitments we have already adopted. Rapid turnover among businesses that provide the same basic service does not threaten a transaction-centered law with obsolescence. Nor does intermediation and eavesdropping. But transaction-centered approaches would not cover emergent data collection practices that lacked a clear connection to today's protected transactions. Other approaches, such as enhanced transparency, are needed to pave the way for future regulation.

B. Enhanced Transparency

Heightened visibility for commercial firms' collection and disclosure practices is an important first step towards the development of effective privacy laws. As it stands, the firms who have the greatest interest in perpetuating digital surveillance also benefit from a practical monopoly on information about the scope and nature of these practices.[56] The stage is therefore set for increasing private surveillance while these practices escape public scrutiny.

---

53. 15 U.S.C. § 6801.

54. *See, e.g.*, Interagency Guidelines Establishing Info. Sec. Standards, 12 C.F.R. Pt. 30, app. B, Sec. III.C.1.c. (2014).

55. One might question the feasibility of requiring third parties like Internet service providers and search engines to treat traffic to or from book services differently than other traffic. But as a technical matter it would be relatively easy for the book service to signal to third parties that the information required special treatment. In one implementation, the book service could simply run a snippet of code during protected transactions—much like the industry-standard robot.txt file that sites already use to communicate their indexing preferences to search engines, *see* Field v. Google, 412 F. Supp. 2d 1106, 1113 (D. Nev. 2006) ("The Internet industry has widely recognized the robots.txt file as a standard for controlling automated access to Web pages since 1994.")—indicating that CRPA protections apply.

56. *See supra* notes 47–49 and accompanying text (explaining how informational advantages can translate into political advantages).

Right now the primary window into firms' data practices lies in their privacy policies, though practically no one reads them.[57] Even in a counterfactual world where everyone read these terms, however, the public would remain poorly informed about how their data was actually being handled. Firms often reserve the right to disclose information to some set of third parties but they seldom identify who these parties are or how many are involved.[58] Even the diligent user, therefore, has little visibility into whether the firm intends to share information with one or two close partners, to disclose it indiscriminately to a dozen loose associates, or to sell personal data wholesale to a data aggregator who intends to repackage and resell the data to anyone willing to pay.[59]

One set of transparency-enhancing interventions would accordingly focus on making the chain of disclosures more visible. At present many firms bind the downstream recipients of user data to strict confidentiality.[60] We could imagine a regime where these firms were required instead to carefully log the chain of custody for any data they transmitted. These obligations could be made viral, so that each firm in the chain of transmission had to make a record of who else received the data.[61] Like the privacy policies themselves, the resulting logs might be impenetrable to the average user. But they would lower the costs of investigation and action by Congress, the Federal Trade Commission, and public advocacy groups.[62]

Another set of interventions might focus on making the initial collection of data both visible and salient.[63] Where written disclosures fail to communicate what's going on, Ryan Calo argues for the deployment of "visceral notice."[64] Just as cameras (and camera apps) can be designed to announce their presence by making an audible shutter sound, Calo argues that web interfaces can be designed in ways that would alert the user to ongoing surveillance.[65] For example, "each advertising network on the Internet [could have] an avatar that ran onto the bottom of the

---

57. It's doubtful that we could find the time even if we tried: Aleecia McDonald and Lorrie Cranor estimate that it would have taken the average Internet user 244 hours to read all the privacy policies she encountered in the year 2008 alone. Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & POL'Y FOR INFO. SOC'Y 543, 560 (2008).

58. *See* Asay, *supra* note 44, at 324.

59. Because this lack of visibility insulates the firm from consumer scrutiny, it may also increase the likelihood that the firm will choose the most profitable option regardless of its impacts on consumer privacy. *See* Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2080–82 (2004) (explaining how the market for privacy policies can devolve into one for lemons when consumers lack the ability to compare the quality of terms).

60. *See supra* note 34 and accompanying text.

61. *Cf.* Hartzog, *supra* note 20, at 695–96 (proposing the use of contracts to bind downstream recipients of user information to a set of confidentiality obligations as well as an obligation to perpetuate the contractual chain in any future disclosures).

62. *See* KOMESAR, *supra* note 48, at 71 (emphasizing the role that information costs play in the success of political organizing).

63. These interventions would be particularly helpful in cases where third parties obtained information not via downstream disclosures, but by insinuating themselves into the initial transaction as intermediaries or eavesdroppers.

64. *See generally* M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027 (2013).

65. *See id.* at 1034–41.

screen to denote the fact that the network was following the user."[66] Better yet, Calo suggests the interface could be designed so that users could click on these avatars to exercise their opt-out rights.[67] The psychological response to feeling "watched" by these avatars—a common response to anthropomorphic designs[68]—could trigger the sort of visceral notice that would help people to understand the actual scope of surveillance in their daily lives.[69] Like other transparency-enhancing interventions, visceral notice could reduce the burdens of organizing—whether in the market or in politics—by making information easier to acquire.

C. Responsive Lawmaking

Conventional privacy legislation—industry-specific or not—may struggle to keep pace with the rapid change and technical complexity of digital surveillance.[70] Commentators have long criticized Congress in matters of privacy for being "both reactive and slow to react."[71] And some argue, in light of contemporary deadlock, that Congress has devolved into a "vetocracy" where special interests can co-opt the system to block legislation even in the face of majority support.[72] These issues counsel in favor of looking beyond Congress for privacy law's continued development.

The search for more responsive institutions offers new perspectives on two trends in privacy law: agency delegation and state legislation. As Daniel Solove and Woodrow Hartzog have recognized, the FTC has become the de facto regulator in all matters of privacy.[73] Its transaction-focused regulatory mandate—to police against "unfair or deceptive acts"[74]—has given it the flexibility to fill the gaps between our industry-specific privacy statutes.[75] Its growing substantive expertise with Internet privacy, moreover, equip it to cut through the complexity and obfuscation of cyberspace in ways that generalist legislators cannot. The FTC's agility

---

66. *Id.* at 1040.

67. *Id.*

68. *See id.* at 1038–39.

69. Mozilla's Lightbeam add-on offers a model on which to build such an intervention. Lightbeam provides interactive visualizations showing the various sites—including hidden third parties—that one has encountered while browsing the web. *See* Fung, *supra* note 45; *see also Lightbeam for Firefox*, MOZILLA.ORG, http://www.mozilla.org/en-US/lightbeam/ (last visited Mar. 31, 2015).

70. *Cf.* Marchant, *supra* note 35.

71. Lior Jacob Strahilevitz, *Toward a Positive Theory of Privacy Law*, 126 HARV. L. REV. 2010, 2012 (2013).

72. *See* Sanford Levinson, *How I Lost My Constitutional Faith*, 71 MD. L. REV. 956, 957–58 (2012) (criticizing the "vetocratic" features of our government).

73. *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 588 (2014) (arguing that "FTC regulation is . . . the largest and arguably the most important component of the U.S. privacy regulatory system."); Lauren Henry, Note, *Institutionally Appropriate Approaches to Privacy: Striking a Balance Between Judicial and Administrative Enforcement of Privacy Law*, 51 HARV. J. ON LEGIS. 193, 210 (2014) ("The FTC is well suited to handle data privacy conflicts that involve balancing the interests of many stakeholders because of its expertise in data privacy, ability to do independent research and adapt quickly to changing customs and technology, and custom of providing tailored solutions through consent orders.").

74. 15 U.S.C. § 45(a)(2) (2012).

75. Solove & Hartzog, *supra* note 73, at 588.

relative to Congress provides an additional yardstick to measure its apparent success in addressing the distinct challenges posed by the Internet and other new technologies.

Congress might also find new ways to leverage the FTC's speed and expertise in this space. While Congress may lack the capacity to update legislation to keep pace with the latest developments in e-commerce, it could pass transaction-centric laws and delegate authority to the FTC to more carefully tailor the regime to particular industries as needed. A system like this could combine the coverage of transaction-centered law with the grounded specificity of industry-specific law. To avoid overtaxing its own resources, the FTC could require regulated industries to bear the burden of persuasion in seeking any special accommodations. This approach would have the advantage of requiring the regulating party—as the one with better information about its own business practices—to disclose the distinctive features of its business model to regulators. By opening any such proceedings to public scrutiny, moreover, the FTC could enlist the industry's competitors in monitoring against abuse of the system. Given that any industry that gained an exemption would wield a competitive advantage, competitors who could not benefit from the exemption would be motivated to voice their objections.[76]

State legislatures deserve attention as another set of institutions that are more responsive than Congress. Paul Schwartz has famously argued that we ought to leave room for the states to regulate privacy so that we can capture the benefits of state-level experimentation between alternative privacy regimes.[77] We might also look to state actors because the states have proven themselves to be more active than Congress in updating their privacy regimes to account for changed circumstances. In recent years states have enacted new privacy legislation in matters as disparate as e-readers, drones, and cellphone tracking.[78] As California's CRPA demonstrates, state laws offer no panacea—industry-specific lawmaking is just one of the pitfalls that might limit their effectiveness. The recent flurry of activity nonetheless sets the stage for serious scholarly investigation of the states' competence, relative to federal actors, in keeping pace with emerging surveillance practices.

V. CONCLUSION

The industry-specific approach to privacy lawmaking is a poor fit for Internet surveillance. We can bolster many existing laws by translating them into industry-neutral, transaction-centered terms. But the greater challenge lies in identifying

---

76. *Cf.* Schwartz, *supra* note 1, at 924 ("A sectoral law might create competitive disadvantages for companies that fall under it and a corresponding subsidy to those outside of its reach.").

77. *See id.* at 932; *see also* Margot E. Kaminski, *Drone Federalism: Civilian Drones and the Things They Carry*, 4 CALIF. L. REV. CIRCUIT 57, 65–66 (2013) (endorsing state development of drone privacy laws).

78. *See, e.g.*, Kaminski, *supra* note 77, at 59 & n.11 (documenting state efforts to regulate drone privacy); Hanni Fakhoury, *Why Wait for Congress? States Passing Electronic Privacy Legislation*, ELEC. FRONTIER FOUND. (June 3, 2013), https://www.eff.org/deeplinks/2013/05/why-wait-congress-states-passing-electronic-privacy-legislation (documenting recent state bills to extend privacy protections over emails and cellphone location tracking); *see also* Part I.A, *supra* (describing California's new reader privacy law).

approaches to lawmaking that can generate effective new laws in the face of the rapid change, technical complexity, and sheer uncertainty that surround technologies and business practices online. As a start, this essay proposes that we find new ways to equip the public to play an informed role in privacy lawmaking and that we continue to explore opportunities for regulation by highly responsive institutions like the FTC.