Yale Journal of Law and Technology

Volume 16
Issue 1 *Yale Journal of Law and Technology*

Article 1

2014

CONFIDENTIALITY AND THE PROBLEM OF THIRD PARTIES: Protecting Reader Privacy in the Age of Intermediaries

BJ Ard
Yale Law School

CONFIDENTIALITY AND THE PROBLEM OF THIRD PARTIES: PROTECTING READER PRIVACY IN THE AGE OF INTERMEDIARIES

BJ Ard*

16 YALE J.L. & TECH. 1 (2013)

ABSTRACT

We often regulate actors as a proxy for protecting categories of information. Rather than directly protect reading records, for example, we target actors like libraries who are likely to possess them. This approach has proven increasingly untenable in the digital age, where the relevant actors are difficult to identify and constantly shifting. Unanticipated third parties now insert themselves as intermediaries or eavesdroppers in all manner of transactions, even in protected spaces like libraries. Where this happens, actor-defined regimes fail to vindicate their privacy commitments even within the institutions for which they were designed.

Libraries provide a clear example of this problem. Private reading historically has been protected through a regime that restricts libraries' ability to exploit reading records. Yet this regime now fails to protect reading records even in libraries because it does not bind third parties who provide library services digitally. Illustrating the point, Amazon facilitates e-book lending for a number of public and academic libraries. Although Amazon collects detailed reading records from patrons utilizing these services, the library confidentiality regime does not restrict what it can do with the records. These patrons accordingly confront the risks to intellectual privacy the library regime was meant to counter.

This Article proposes a content-defined approach whereby confidentiality obligations would attach to particular types of information regardless of which actors possessed it. Such an approach would not only save extant confidentiality regimes from obsolescence, but also provide a vehicle for extending privacy commitments to future data practices that implicated the same types of sensitive records.

---

* Postdoctoral Associate in Law and Thomson Reuters Fellow at the Yale Law School Information Society Project. Yale Law School, J.D. 2010. I would like to thank Ian Ayres and Madhavi Sunder for their advice and encouragement during the early stages of this project, and Colin Agur, Valérie Bélair-Gagnon, Kiel Brennan-Marquez, Brookes Brown, Alan Hurst, Margot Kaminski, David Nimmer, Neil Richards, Christina Parajon Skinner, Andrew Tutt, and Bruce Wessel for sharing valuable insights as the project has evolved. I am also grateful to Mike DiRaimo, Max Mishkin, and their colleagues on the *Yale Journal of Law and Technology* for their assistance throughout the editing process. Finally, I would like to specially thank Lucas Franklin for sharing his in-depth knowledge of library ethics, privacy policies, and e-book lending. All errors are of course my own.

CONFIDENTIALITY AND THE PROBLEM OF THIRD PARTIES

16 YALE J.L. & TECH. 1 (2013) 2013-2014

INTRODUCTION

Private, anonymous reading may soon be a thing of the past. This is due in part to a shift towards research and reading facilitated by private entities with an interest in exploiting readers' data, rather than by trusted institutions, like libraries, with normative and legal commitments to privacy. But the coup de grâce comes from emerging information practices that threaten reader privacy even within ostensibly protected institutions like libraries. Library confidentiality is maintained through an actor-defined approach that restricts what libraries themselves can do with patron information.[1] In an age where library services are increasingly provided and intermediated in a digital format by third parties, however, non-library actors have broad latitude to collect and exploit records of patrons' library activity. As a case-in-point, Amazon facilitates e-book borrowing for the Kindle e-reader as a service to library patrons, but it collects detailed reading records from these patrons and uses the records for marketing purposes.[2] Because third parties like Amazon are not libraries, libraries' actor-defined confidentiality rules do not restrict them despite their involvement in library transactions and their collection of the very sorts of data the library confidentiality regime is meant to protect.

While this Article is grounded in the library context, the problem of third parties for actor-defined confidentiality is not unique to libraries. The involvement of third parties, whether as Internet service providers, advertising partners, or content providers, has become ubiquitous in contemporary e-commerce. But policymakers continue to devise confidentiality regimes that, like the library regime, limit their mandates to particular pre-defined classes of actors and thereby fail to protect information in the hands of third parties who were unanticipated when the regimes were designed.[3] While such regimes could be updated to cover new

[1] Following common usage within the library profession, the term "patron" refers to an individual person who uses the library.

[2] This Article uses the term "Amazon" to refer to the company Amazon.com. "E-books," or electronic books, are book-length digital texts. Most e-books are simply electronic versions of conventional, hardcopy books, but some texts are published exclusively in digital format. "E-readers," or electronic book readers, are mobile electronic devices that allow users to read e-books. The Kindle is a popular e-reader developed and marketed by Amazon.

[3] Historically, confidentiality obligations have arisen in contexts where they were necessarily actor-defined, such as within the context of a societally recognized confidential relationship (such as the physician-patient relationship), a fiduciary relationship, or an express or implied confidentiality agreement. Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 157-58 (2007).

actors as they emerged, piecemeal updates are unsatisfying in this context: e-commerce evolves rapidly, and confidentiality schemes would be perpetually rendered obsolete with each generation of unanticipated actors.

Overcoming these difficulties requires an approach to confidentiality where obligations are defined with reference to the content we wish to protect rather than the actors we suppose will possess it. The advantages of this approach go beyond merely protecting confidentiality within existing institutions. Content-defined confidentiality also facilitates the extension of confidentiality to whichever entities play a role in facilitating access to such content in the future.

Imagine, for example, that the protections afforded by the library confidentiality regime were redefined so they applied not specifically to librarians, but rather to any entities who came to possess an individual's reading records. Such a regime would of course cover third parties who facilitated library services, establishing more complete protection within the library as an institution. But it would also cover a range of other information providers who facilitate reading entirely outside the library context. If society is serious in its commitment to private reading, then such an extension seems necessary as non-library intermediaries become the primary actors who facilitate individuals' research and reading.

The move from an actor-defined approach to a content-defined approach would not, however, excuse policymakers from attending to the business practices and norms of the specific entities being regulated. Actor-defined approaches, for all their limits, have the advantage of being situated

---

When legislators create new confidentiality obligations by fiat, they often follow the same model. *See, e.g.*, Gramm-Leach-Bliley Act of 1999, 15 U.S.C. §§ 6801-6809 (2012) (imposing obligations on "financial institutions"); Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (2006), *amended by* Video Privacy Protection Act Amendments Act of 2012, Pub. L. No. 112-258, 126 Stat. 2414 (2013) (imposing non-disclosure obligations on "video tape service providers"); Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721 (2006) (imposing non-disclosure obligations on a "State department of motor vehicles" and its contractors); Cable Communications Policy Act of 1984, 47 U.S.C. § 551 (2006) (imposing obligations on "cable operators"). As prior scholarship has recognized, privacy statutes that target specific industries sometimes create significant loopholes; they protect information in the hands of the covered entities but fail to protect the same information once it passes to non-covered entities, and they fail to protect comparable information if it is collected in the first instance by non-covered entities. *See* Clark D. Asay, *Consumer Information Privacy and the Problem(s) of Third-Party Disclosures*, 11 NW. J. TECH. & INTELL. PROP. 321, 326 (2013) (criticizing this "sectoral approach" to privacy law); *see also* Joshua L. Simmons, Note, *Buying You: The Government's Use of Fourth-Parties To Launder Data About "The People,"* 2009 COLUM. BUS. L. REV. 950 (2009) (explaining that third parties who are prohibited from disclosing certain information to the government are often free to give the same information to non-government "fourth parties," who can then turn around and sell the information to the government).

within the known practices of a particular industry. Content-defined approaches, on the other hand, must speak to multiple industries with divergent commitments and business motives. The library confidentiality regime, for example, derives much of its force from librarians' normative commitments and lack of a business motive to track user data; extending its formal obligations to other information providers would not necessarily provide strong protections for reader data. The regime would require adjustment to be effective in new contexts. Even though the content-defined approach would resemble an actor-defined approach insofar as it required continued attention to the particular entities utilizing certain types of data, it would nonetheless advance the discussion by moving beyond the question of *who* to regulate to the question of *how* to do so effectively.

This argument develops in five parts. While the limits of actor-defined confidentiality regimes are apparent throughout e-commerce, my argument is grounded in the threats that third parties pose for private reading in libraries because these developments make the problem concrete. Part I examines the importance of private reading and the threats that digitally intermediated reading poses for such privacy—particularly the threats arising from the involvement of third parties with commercial interests in exploiting reader data. It also delineates two classes of third parties: "extra-institutional" third parties, who provide reading materials outside protected institutions like libraries, and "intra-institutional" third parties, who participate in transactions within these institutions. Exposing intra-institutional third parties to scrutiny is a key goal of this Article, but both types of third parties must be accounted for to preserve private reading. Part II examines the library confidentiality regime, an actor-defined regime restricting libraries' use of patron data. In a time where library transactions were two-party affairs between the librarian and patron, this regime had many successes. Part III explores libraries' arrangement with Amazon to show how the library regime now fails to protect private reading in a world where library transactions have become multi-party affairs involving intra-institutional third parties. Part IV proposes a content-defined approach to confidentiality as a means to protect existing regimes from obsolescence and to extend existing commitments to confidentiality to new contexts where the same types of sensitive information are implicated. Finally, Part V addresses the continuing need to tailor confidentiality obligations to the norms and incentives of the industries being regulated, even under a content-defined regime.

I. PRIVATE INQUIRY AND THE CHALLENGES OF THE DIGITAL ERA

A. Private Reading Advances First Amendment Values

Private, anonymous reading is of fundamental importance to free thought and free expression because it provides individuals with the opportunity to engage with controversial ideas, develop intellectually, and formulate speech they intend to share with others.[4] Private inquiry also serves democratic values beyond the receipt or cultivation of speech per se, for example advancing autonomy by allowing individuals to engage with unpopular materials in pursuit of their personal development.[5]

When people find their reading monitored by either the government or private actors, they are often deterred from reading controversial materials for fear of the consequences, which may include official sanctions or social stigma.[6] To be clear, these harms do not necessarily hinge on

---

[4] 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, 818 (2006) (arguing that "information-seeking by itself, even when unconnected to any specific willing speaker or any specific instance of speech, deserves to be valued and constitutionally-protected because of its crucial role in promoting core First Amendment values"); Julie E. Cohen, *A Right To Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981, 1007 (1996) (arguing that a lack of protection for anonymous reading "would chill inquiry, and as a result, public discourse concerning politically and socially controversial issues—precisely those areas where vigorous public debate is most needed, and most sacrosanct"); Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 419 (2008) [hereinafter Richards, *Intellectual Privacy*] ("Intellectual exploration must be private insofar as the act of reading must be free from interference by outsiders, and also unwatched, lest the surveillance of others chill the development of new thoughts in the direction of the bland and the mainstream."); Neil M. Richards, *The Perils of Social Reading*, 101 GEO. L.J. 689, 705 (2013) [hereinafter Richards, *Perils of Social Reading*] ("[S]urveillance chills and deters free thinking and reading.").

[5] *See* Blitz, *supra* note 4, at 802 (casting the right to read privately as "an alternative way for individuals to exercise liberty of conscience and self-development").

[6] *See* Lamont v. Postmaster Gen. of the United States, 381 U.S. 301, 307 (1965) (explaining the "deterrent effect" that follows government monitoring of citizens' reading); Blitz, *supra* note 4, at 827 ("[P]rivacy may be valuable for an individual not only because she wants to avoid the opprobrium of friends and family, but also because she wants to avoid unnecessarily hurting or disappointing them."); Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1951 (2013) [hereinafter Richards, *Dangers of Surveillance*] ("Federal prosecutions based on purely intellectual surveillance are thankfully rare, but the coercive effects of monitoring by our friends and acquaintances are much more common."); Richards, *Intellectual Privacy*, *supra* note 4, at 404 ("Thoroughgoing surveillance, whether by public or private actors, has a normalizing and stifling effect.").

whether the monitoring entity intends to disclose the data. Rather, free inquiry may be chilled whenever citizens find themselves watched and their activities linked to a permanent and traceable record.[7]

As to government action, one might argue the feds are not interested in citizens' intellectual pursuits or beliefs. Yet recent events—such as the I.R.S.'s aggressive auditing of nonprofit groups with the terms "Tea Party" or "patriots" in their titles[8]—make the risk of government sanctions based on unpopular intellectual or political affiliations all too tangible. Moreover, recent disclosures regarding surveillance by the National Security Agency ("NSA") have demonstrated the federal government's capacity and apparent willingness to collect and analyze the content of Americans' electronic communications.[9]

Monitoring and disclosure by commercial entities may also cause harms beyond stifling free inquiry. For example, Neil Richards argues that companies may use consumer data to unduly manipulate consumer preferences, or to sort people into different categories and treat them differently in ways that might unfairly privilege or discriminate against people on the basis of wealth, geography, gender, race, or ethnicity. Richards, *Dangers of Surveillance*, *supra*, at 1957; *see also* Simmons, *supra* note 3, at 952 n.1, 991 (explaining that data aggregation companies already sell lists that sort people into such categories, including an "Affluent Hispanics" list and the "Gay America Megafile").

[7] *See* Richards, *Dangers of Surveillance*, *supra* note 6, at 1948 (defending the empirical claim that being watched deters engagement with materials others might find deviant). This response may arise because the stockpiling of information even by commercial entities makes it a target for government requests for information and creates a risk of inadvertent disclosures. *See infra* Section II.C (explaining how libraries have recognized and accounted for this risk); *infra* Section III.B (describing these risks in the context of Amazon's collection and retention of records).

Additionally, the chill may arise due to concerns that the collecting entity itself will abuse the information. *See* Richards, *Dangers of Surveillance*, *supra* note 6, at 1957; *see also* Randal C. Picker, *Competition and Privacy in Web 2.0 and the Cloud*, 103 NW. U. L. REV. COLLOQUY 1, 10-11 (2008) (arguing that "disclosure may not be the act of relevance," and that firms may simply expand vertically so they can make greater use of consumer data without having to disclose it to an outside firm).

[8] Jonathan Weisman, *I.R.S. Apologizes to Tea Party Groups Over Audits of Applications for Tax Exemption*, N.Y. TIMES, May 11, 2013, at A11.

[9] Nicole Perlroth, Jeff Larson & Scott Shane, *N.S.A. Able To Foil Basic Safeguards of Privacy on Web*, N.Y. TIMES, Sept. 5, 2013, at A1 (describing the N.S.A.'s circumvention of encryption over "e-mails, Web searches, Internet chats, and phone calls of Americans and others"); Charlie Savage, *N.S.A. Often Broke Rules on Privacy, Audit Shows*, N.Y. TIMES, Aug. 16, 2013, at A12 ("The National Security Agency violated privacy rules protecting the communications of Americans and others on domestic soil 2,776 times over a one-year period, according to an internal audit . . . ."); Charlie Savage & Scott Shane, *Top-Secret Court Castigated N.S.A. on Surveillance*, N.Y. TIMES, Aug. 21, 2013, at A1 (discussing "an N.S.A. program that systematically searches the contents of Americans' international Internet communications, without a warrant," including "tens of thousands of domestic e-mails and other Internet communications of Americans").

CONFIDENTIALITY AND THE PROBLEM OF THIRD PARTIES

The chilling effect on individuals' reading is the most direct consequence of monitored reading, but this chill extends to other important expressive rights. The freedom of speech itself rings hollow when speakers are deprived of private opportunities to formulate thoughts worth sharing.[10] Likewise, freedom of association is hampered when disclosure of a citizen's reading habits threatens to expose his otherwise anonymous affiliation with certain groups or beliefs.[11] The Supreme Court prohibited the government from probing this connection between citizens' reading habits and their protected associations when it held that the postal service could not require citizens to "opt in" as a prerequisite to receiving materials the government deemed "communist political propaganda,"[12] and that Congress could not compel a publisher of books and pamphlets to reveal a list of its purchasers.[13]

This chilling of speech caused when reading is monitored is recognizable as a First Amendment harm regardless of one's theory for why free speech is valuable.[14] One prevalent articulation is that free speech is meant to "facilitate the pursuit of truth" through the "marketplace of

[10] Cohen, *supra* note 4, at 1007 (arguing that a failure to protect "the entire series of intellectual transactions" through which an opinion is formed "would chill inquiry, and as a result, public discourse, concerning politically and socially controversial issues—precisely those areas where vigorous public debate is most needed, and most sacrosanct"); Richards, *Intellectual Privacy*, *supra* note 4, at 403 ("In a world of widespread public and private scrutiny, novel but unpopular ideas would have little room to breathe. Much could be said, but it would rarely be new, because original ideas would have no refuge in which to develop, save perhaps in the minds of hermits.").

[11] *See* Cohen, *supra* note 4, at 1014. As the Supreme Court recognized in *NAACP v. Alabama*, 357 U.S. 449, 460-62 (1958), the First Amendment protects associational anonymity in order to guard the freedom of assembly against the chilling effect of community pressures.

[12] *See* Lamont v. Postmaster Gen. of the United States, 381 U.S. 301 (1965).

[13] *See* United States v. Rumely, 345 U.S. 41 (1953). As Justice Douglas warned: "Once the government can demand of a publisher the names of the purchasers of his publications, the free press as we know it disappears." *Id.* at 57 (Douglas, J., concurring). See also *Lubin v. Agora, Inc.*, 389 Md. 1, 21-22 (2005) ("Compelled disclosure of an individual's decision to read, purchase, or subscribe to certain publications may invade that individual's privacy of belief and association . . . .").

[14] *See* Richards, *Danger of Surveillance*, *supra* note 4, at 1946, 1950; Richards, *Intellectual Privacy*, *supra* note 4, at 404-07; *see also* Blitz, *supra* note 4, at 801 ("Reading and listening, as much as speaking, are essential and concomitant parts of the process by which citizens interact in debates over democratic values and also in a wider marketplace of ideas, and are valuable for largely the same reason: to bring us closer to the truth, foster individual self-development, or improve the quality of collective deliberation and self-government.").

ideas."[15] Yet, as Neil Richards has articulated, there is no logical reason to protect only outward speech under this approach, when "private contemplation, in acts of reading, thinking, and confidential conversation," are important means by which individuals seek the truth and share their findings when (if ever) they are ready.[16]

Another prominent approach holds that free speech is meant to promote democratic-self governance, so it should be protected to the extent necessary for citizens to participate "in the communicative processes relevant to the formation of democratic public opinion."[17] Here, too, private inquiry is essential to the development of the faculties required for citizens to participate in their own governance and the cultivation of ideas important to political debate.[18] Even under a narrower conception of democratic self-governance—such as Alexander Meiklejohn's idea that free speech is meant to protect only the communicative processes necessary for informed voting[19]—private inquiry is valuable because it provides a means for citizens to inform themselves about candidates and issues free from outside pressure. In this sense, anonymous reading protects democracy while citizens form their views much like the anonymous ballot protects democracy when citizens act on these views.

Surveillance of one's reading history could also threaten political participation more directly. As Neil Richards warns, the state could silence dissenters by blackmailing them with book titles or search queries that could be characterized as controversial or deviant.[20]

Private inquiry is also fundamentally important for approaches to free speech based on cultural and personal autonomy. Jack Balkin argues "the free speech principle is about, and always has been about, the

---

[15] *See* Robert Post, *Reconciling Theory and Doctrine in First Amendment Jurisprudence*, 88 CAL. L. REV. 2353, 2362-63 (2000).

[16] Richards, *Intellectual Privacy*, *supra* note 4, at 404-05.

[17] *See* Post, *supra* note 15, at 2366-69.

[18] Richards, *Intellectual Privacy*, *supra* note 4, at 405; *see* Blitz, *supra* note 4, at 816 ("Libraries . . . provide a part of individuals' education in citizenship.").

[19] Post, *supra* note 15, at 2367.

[20] Richards, *Intellectual Privacy*, *supra* note 4, at 406. Sadly, this sort of blackmail is one of the FBI's old tricks: the bureau historically engaged in surveillance of Vietnam war protestors and civil rights leaders, including the Reverend Dr. Martin Luther King, Jr., for the purpose of gathering information with which to discredit them. Colin Moynihan, *Trove of F.B.I. Files on Lawyers Guild Shows Scope of Secret Surveillance*, N.Y. TIMES, June 25, 2007, at B1. Recent news suggests that the NSA is now taking the same tack in its surveillance of Muslim targets who are alleged "radicalizers," gathering records of their pornography viewing habits to damage their reputations. James Temple, *Spying on Online Sex Lives Raises Red Flags*, S.F. CHRON., Nov. 28, 2013, at C2.

promotion and development of a democratic culture."[21] This vision of democracy includes participation in governance, but it radiates outward to participation in culture more broadly: it is concerned with the ultimate impact of culture on the individual, and the individual on culture.[22] Private inquiry cuts to the heart of these concerns because such privacy is central to individuals' opportunities to engage with culture, find their own meanings, and cultivate their own "intellectual diversity and eccentric individuality" unfettered by community pressures.[23]

B. Institutional Limits to Private Reading

Despite the importance of private reading, society does not protect it universally. Instead, we protect it primarily within certain privileged institutions, such as libraries.[24] It bears noting that even this limited recognition of reader privacy helps preserve important democratic values.

So long as libraries remain safe for private reading, they provide citizens a space to wrestle with unpopular ideas without fear of government surveillance or social coercion. Marc Blitz praises libraries for creating a space where people can "conduct valuable thought experiments in living where actual experiments aren't practical."[25] People can explore many more ideas through private reading than they could through action—or through

[21] Jack M. Balkin, *Digital Speech and Democratic Culture*, 79 N.Y.U. L. REV. 1, 34 (2004).
[22] *Id.* at 33 ("A democratic culture is valuable because it gives ordinary people a fair opportunity to participate in the creation and evolution of the processes of meaning-making that shape them and become part of them . . . .").
[23] Richards, *Dangers of Surveillance*, *supra* note 4, at 1948; *see* Blitz, *supra* note 4, at 817 ("[T]he First Amendment sanctuary offered by libraries provides a platform not for political deliberation, but rather individual self-fulfillment and autonomy.").
[24] Despite our legal culture's emphasis on the sanctity of the home, reading at the library may sometimes be more secure than reading at home. Marc Blitz describes circumstances where a teenager might read in the library to avoid his family's judgment regarding his reading habits. Blitz, *supra* note 4, at 870-71.

Moreover, books a citizen physically brings home may become evidence in a criminal investigation. In *Tattered Cover, Inc. v. City of Thornton*, 44 P.3d 1044 (Colo. 2002), for example, the government seized two books on illicit drug-making from a home methamphetamine lab then (unsuccessfully) subpoenaed a local bookstore to ask who had purchased the books. Books that an individual reads at the library, especially those that are never checked out, are less likely to become involved in an investigation. *But see* HERBERT N. FOERSTEL, SURVEILLANCE IN THE STACKS: THE FBI'S LIBRARY AWARENESS PROGRAM (1991) (describing literal witch-hunts whereby local law enforcement sought to find out who had borrowed books about Satanism from the library as recently as the late 1980s).
[25] Blitz, *supra* note 4, at 820.

monitored reading—because privacy reduces the social costs associated with these explorations.[26]

Stated another way, spaces like libraries are important because they offer readers the opportunity to "play" with new and sometimes controversial ideas outside the constraints imposed by government, commercial, or interpersonal monitoring. Julie Cohen offers the provocative argument that unconstrained play is important for individual development, and therefore that gaps in existing regulatory or surveillance regimes where such play can occur—gaps she calls "semantic discontinuities"—are important for individual flourishing.[27] Privacy rules, like those in effect in libraries, create semantic discontinuities by sheltering users from certain forms of data collection or usage.[28] This framework explains how libraries play an important role even if they are one of few settings where one's reading records are private.

---

[26] *Id.*

[27] *See* JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE ch. 9 at 14 (2012), *available at* http://www.juliecohen.com/page5.php ("Creativity, critical subjectivity, and everyday practice flourish in conditions of (partial) unpredictability, and humans require creativity, critical subjectivity, and everyday practice to flourish.").

While Cohen's valorization of semantic discontinuity might be challenged in some settings due to the potential harms of under-enforcement, or concerns that large business interests would leverage these regulatory dead zones to the detriment of consumers, *see* Jack M. Balkin, *Room for Maneuver: Julie Cohen's Theory of Freedom in the Information State*, 6 JERUSALEM REV. LEGAL STUD. 79, 92 (2012) (reviewing COHEN, *supra*), these concerns are largely inapposite here. The typical concern with under-enforcement is that individuals will utilize the semantic discontinuity to commit acts that are harmful to society, but this concern does not make sense here: the idea that readers should be monitored to discourage them from reading "harmful" books is incompatible with the First Amendment. *See* Stanley v. Georgia, 394 U.S. 557, 565 (1969) ("If the First Amendment means anything, it means that a State has no business telling a man, sitting alone in his own house, what books he may read or what films he may watch. Our whole constitutional heritage rebels at the thought of giving government the power to control men's minds."); *see also* Hustler Magazine, Inc. v. Falwell, 485 U.S. 46, 51 (1988) ("The First Amendment recognizes no such thing as a 'false' idea."); Cohen, *supra* note 4, at 1013 ("[T]he mere act of reading cannot injure.").

The concern of corporate exploitation is likewise inapposite because it is difficult to imagine how corporations would arrogate the gains of private reading to their own benefit. Indeed, the limited prospects for commercial exploitation may explain the relative lack of corporate effort to protect private inquiry, particularly vis-à-vis monitoring by commercial entities. *See* Balkin, *supra*, at 95 ("[G]overnments and businesses will want to maintain their own form of semantic discontinuity. They will want to preserve for *themselves* plenty of room for maneuver and avoid surveillance of their own operations, while reducing or eliminating semantic discontinuity that benefits ordinary individuals.").

[28] COHEN, *supra* note 27, ch. 9 at 23.

The value of library privacy is diminished, however, as more individuals turn to non-library sources as their primary information providers, and as library reading itself becomes less confidential. The next Section describes these shifts.

C. Digital Intermediaries Threaten Private Reading

Reader privacy faces new challenges because it is possible—and commercially valuable—to monitor digitally intermediated reading. This Section describes the business incentives that give rise to this threat, then discusses two scenarios where individuals risk losing privacy by dealing with non-library information providers. The first occurs when information seekers turn to commercial providers who offer services entirely outside protected institutions like libraries; these are "extra-institutional" third parties. The second occurs when commercial third parties participate in sensitive information transactions within protected institutions like libraries; these are "intra-institutional" third parties.

1. The Incentive To Monitor

Digital technologies offer tremendous opportunities for the pursuit of knowledge. These technologies facilitate wider access to traditional types of media such as books and newspapers, as well as to a range of new types of content on the Internet. They also enable users to simultaneously consume and create knowledge through new modes of user-generated production, reflected in large collaborations like Wikipedia and smaller projects like individual blogs and YouTube channels.[29]

But the same basic technologies also provide tools for monitoring what people read.[30] On the Internet, nearly every click a user makes, and every web page a user visits, generates a record.[31] When the user's activities

[29] Beyond providing greater access to knowledge, these technologically facilitated collaborative projects may be valuable because they democratize culture, allowing more people to participate in the production of knowledge and meaning. *See* MADHAVI SUNDER, FROM GOODS TO A GOOD LIFE: INTELLECTUAL PROPERTY AND GLOBAL JUSTICE 8-9 (2012); Balkin, *supra* note 21, at 1-2.

[30] Presciently, Julie Cohen observed in 1996: "The same technologies that enable readers to access digitally stored works . . . also will also enable copyright owners to generate precise and detailed records of such access." Cohen, *supra* note 4, at 983.

[31] *See* JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET—AND HOW TO STOP IT 186 (2008), *available at* http://futureoftheinternet.org/download/ ("[N]early all formerly transient communication ends up permanently and accessibly stored in the hands of third parties, and subject to comparatively weak statutory and constitutional protections against

are directed towards research or reading, the resulting records are quite sensitive because they portray the user's questions and interests in vivid detail.[32]

In the information economy, the probative thoroughness of the data is what makes it commercially valuable.[33] Companies generate systems to collect and store this data so they can put it to several types of commercial use. One use is the improvement and personalization of a company's services. An Internet search engine, for example, might study users' queries as a whole to improve its search algorithms; at a more personal level, it might analyze a specific user's search habits to provide customized results for that user.[34] Another use is advertisement. A company might gather information on consumers to better advertise its own products to the customers most likely to be interested, or it might share that information with other parties for their advertisement purposes.[35] Still other companies aggregate data and sell it to interested parties, including advertisers and the government.[36] User information is the lifeblood of companies pursuing any of these strategies.[37] These opportunities and incentives drive companies to collect and monetize data from those who use their services.

---

surveillance."); Picker, *supra* note 7, at 5 ("Intermediaries have the ability to see what is happening with every click . . . .").

[32] Richards, *Intellectual Privacy*, *supra* note 4, at 439 (arguing "search-engine records come very close to being a transcript of the operation of a human mind"); *see* Cohen, *supra* note 4, at 981 ("In truth . . . the new information age is turning out to be as much of an age of information *about* readers as an age of information *for* readers."); James Grimmelmann, *The Structure of Search Engine Law*, 93 IOWA L. REV. 1, 18 (2007) ("Given the sensitivity of [search query] information and the ease of linking it back to particular individuals, users have an evident privacy interest that their queries not be misused.").

[33] Cohen, *supra* note 4, at 1013 ("Reader profiles are valuable to marketers precisely because they disclose information about the reader's tastes, preferences, interests, and beliefs.").

[34] *See* Grimmelmann, *supra* note 32, at 52 ("Search engines use query and clickthrough data to target advertisements, to refine search quality, and to personalize search. Prohibiting these uses outright could have significant negative effects on users . . . .").

[35] *See* Richards, *Dangers of Surveillance*, *supra* note 6, at 1939 ("[W]e are building an Internet that is on its face free to use, but is in reality funded by billions of transactions where advertisements are individually targeted at Internet users based upon detailed profiles of their reading and consumer habits."); *see also* Grimmelmann, *supra* note 32, at 52.

[36] *See* Simmons, *supra* note 3, at 991 ("Today, data aggregators are able to cross-index various sources of information to produce incredibly extensive—and invasive—lists for practically any purpose."); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 SO. CAL. L. REV. 1083, 1095 (2002) ("Database firms are willing to supply the information and the government is willing to pay for it.").

[37] Picker, *supra* note 7, at 3. Moreover, a given entity may utilize user data for several of these purposes. A company like Amazon, for example, stands to benefit by not only

2. Extra-Institutional Third Parties

Reader privacy is at risk when readers turn to extra-library information providers such as e-book retailers, Internet search engines, or research databases. Even though the information these entities obtain about individuals' reading habits implicates serious First Amendment concerns, these entities owe few confidentiality obligations under existing law. Accordingly, these entities have wide latitude to exploit reader data for commercial uses.

Many scholars recognize that extra-library information providers threaten reader privacy, and they recommend extending confidentiality obligations like those in effect in libraries to these new information providers.[38] Neil Richards, for example, expressly proposes that entities like bookstores, search engines, ISPs, and video providers should be governed by confidentiality rules similar to those governing libraries.[39] He also argues these entities should be encouraged to recognize that they play a role similar to libraries in our "cognitive and expressive infrastructure" so they will adopt similar privacy norms.[40]

As Richards explains, confidentiality is fundamentally important in the context of information seeking.[41] On the one hand, people need intellectual privacy to make up their minds. If they fear that they are being monitored and scrutinized, then they may not engage with controversial ideas, they may be impeded from making fully informed decisions, and in either case society will be the worse for it.[42] On the other hand, the information we can access on our own is constrained by the limits of our personal resources and knowledge, and "we often need the assistance and recommendations of others . . . be they friends, librarians, or search

---

employing user data to improve or customize the search results a customer sees when seeking a particular product (a search-improvement function), but also using the data to target advertisements for Amazon or third-party products the customer is not seeking (an advertisement function).

[38] *See* Anne Klinefelter, *Library Standards for Privacy: A Model for the Digital World?*, 11 N.C. J.L. & TECH. 553, 561 (2010) (arguing we need legal protection equivalent to libraries' protections for the "extra-library digital environment of Google Books, e-readers, and Internet reading"); Richards, *Intellectual Privacy*, *supra* note 4, at 419-21; Richards, *Perils of Social Reading*, *supra* note 4, at 712; Bradley Schaufenbuel, *Revisiting Reader Privacy in the Age of the E-Book*, 45 J. MARSHALL L. REV. 175, 186 (2011).

[39] Richards, *Perils of Social Reading*, *supra* note 4, at 723-24.

[40] Richards, *Intellectual Privacy*, *supra* note 4, at 441; *see also id.* at 437 (describing how law and norms could be fashioned to shape the incentives of such entities).

[41] Richards, *Perils of Social Reading*, *supra* note 4, at 712.

[42] *Id.*

engines."[43] Disclosing interests to these others nonetheless invites potentially toxic monitoring and scrutiny. Identifying this problem as a paradox, Richards recognizes librarians' confidentiality scheme as a "successful and proven solution" that allows patrons to disclose their interests without fear that their private interests will be exposed.[44]

Anne Klinefelter takes a similar tack. She finds it problematic that commercial information intermediaries who fill the same niche as libraries have broad discretion to share or even sell their readers' data.[45] She recommends that services like Google Books, e-book retailers, and Internet sites be regulated by legal protections that achieve the same cumulative effect as libraries' practices and procedures, norms, and protective statutes.[46] Other scholars have noted the same set of problems and issued similar proposals.[47] Moreover, some states have recently passed or considered legislation seeking to regulate these extra-library parties under a library-style confidentiality regime.[48]

---

[43] *Id.*

[44] *Id.* This point dovetails with Richards and Solove's broader critique of privacy regimes—as opposed to confidentiality regimes—for refusing to recognize protection of information if it is shared with another party rather than guarded closely as a secret. *See* Richards & Solove, *supra* note 3, at 126 ("American law has never fully embraced privacy within relationships; it typically views information exposed to others as no longer private."); Solove, *supra* note 36, at 1086 ("Privacy is about protecting the skeletons that are meticulously hidden in the closet."). Such an approach is unworkable for a right such as free inquiry, where private reading is paramount but certain disclosures are necessary for the effective exercise of the right. *See* Richards, *Perils of Social Reading*, *supra* note 4, at 712.

[45] Klinefelter, *supra* note 38, at 561.

[46] *Id.* Note that the large-scale digitization of books contemplated by the Google Books project has moved closer to realization in light of Judge Denny Chin's recent opinion recognizing the project as fair use. *See* Authors Guild, Inc. v. Google, Inc., No. 05 Civ. 8136, 2013 WL 6017130 (S.D.N.Y. Nov. 14, 2013).

[47] *See, e.g.*, Schaufenbuel, *supra* note 38, at 186 ("[S]ince e-book providers are taking on the functions once performed by public libraries, they should be required to provide similar privacy protections to readers."); *id.* at 196; *see also* Margot Kaminski, *Reading Over Your Shoulder: Social Readers and Privacy*, 2 WAKE FOREST L. REV. ONLINE 13, 18 (2012) (praising the California Reader Privacy Act because it "extends the type of protections traditionally afforded to library patrons to all books and e-books").

[48] *See, e.g.*, California Reader Privacy Act of 2011, CAL. CIV. CODE §§ 1798.90-1798.90.05 (West Supp. 2013) (establishing a reader privacy act that covers non-library "book services"); Assemb. B. 3802, 215th Legis., Reg. Sess. (N.J. 2013) (proposing a similar reader privacy act in New Jersey). The California Act's author, Senator Leland Yee (D), specifically noted that booksellers were not subject to the same protections as libraries and sought to bridge that gap. *See* CAL. S. REP. S.B. 602, 2011-2012 Sess., 2011 WL 1364760 at *8 (Apr. 11, 2011).

3. Intra-Institutional Third Parties

The diminishment of privacy caused by intra-institutional third parties, by contrast, has received little attention. Reader privacy is now at risk within ostensibly protected spaces like libraries because third parties participate in digital transactions within these spaces. These third parties collect sensitive user information even though they are neither integrated into our trusted institutions nor bound by the same confidentiality obligations as the institutions themselves. Helen Nissenbaum's articulation of privacy as contextual integrity provides a clear framework for understanding why these developments are problematic: they directly transgress the information gathering and dissemination norms we expect in the library context.[49]

These intra-institutional third parties play a range of different roles. The third party can provide content; in the example described in detail below, for example, Amazon is a third party who supplies e-books to library patrons while simultaneously gathering detailed information regarding their reading habits.[50] Or, rather than provide content, a third-party service like PayPal or Google Wallet might collect information on users' transactions in the process of facilitating payments.[51]

Third parties' activities during consumer web browsing illustrate additional roles. A third party might provide advertisements or other background services: some website operators willingly opt into programs like Google's AdSense, which nets revenues for the website in exchange for giving Google the opportunity to advertise on the site.[52] Or a third party

---

[49] *See* Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 151 (2004) ("To establish whether contextual integrity is breached requires an examination of governing norms of appropriateness and flow to see whether and in what ways the proposed new practices measure up."). I thank Katherine Strandburg for directing me to Nissenbaum's work on contextual integrity.

[50] *See infra* notes 130-148 and accompanying text.

[51] *See* Google, *Google Wallet Privacy Notice*, WALLET.GOOGLE.COM, https://wallet.google.com/files/privacy.html (last modified Aug. 1, 2012) ("When you use Google Wallet to conduct a transaction, we may collect information about the transaction, including: Date, time and amount of the transaction, a description provided by the seller of the goods or services purchased, any photo you choose to associate with the transaction, the names and email addresses of the seller and buyer (or sender and recipient), the type of payment method used, your description of the reason for the transaction, and the offer associated with the transaction, if any."); PayPal, *Payment History and Tracking*, PAYPAL.COM, https://www.paypal.com/webapps/helpcenter/article/?articleID=94020 (last visited Dec. 22, 2013) (describing records kept by PayPal).

[52] *See* Google, *Advertising*, GOOGLE POLICIES & PRINCIPLES, http://www.google.com/policies/technologies/ads/ (last visited Dec. 22, 2013). Google's

might simply be in a position to eavesdrop. Internet service providers become privy to detailed records on a subscriber's online activities in the process of providing Internet service.[53] Other parties may achieve similarly pervasive monitoring by installing cookies or other devices that enable them to track the user's browsing habits on other sites.[54] The ubiquitous Facebook "Like" buttons that appear on non-Facebook websites are one such monitoring device: "even if you don't hit the button, Facebook knows you were there."[55] Suffice it to say that a wide range of third parties can be involved in any given transaction. And this discussion is directed at third parties *directly* involved in facilitating or watching the users' activities. The universe of privacy risks expands dramatically when one considers that these third parties may disclose consumer data to additional third parties who were not involved in the transaction.

Much of this third-party activity is opaque to the end user. In the course of normal Internet browsing, for example, the user may be under the impression that he is visiting and transacting with just one information provider or website at a time.[56] In truth, a user may be sharing information with dozens of third parties while visiting just a single website. To the extent this perception arises from users' difficulty in visualizing the presence of these invisible third parties, technological interventions may offer a better understanding. Mozilla, the developer of the Firefox web browser, recently released a tool called Lightbeam directed at this issue.[57]

AdWords, Google Analytics, and DoubleClick-branded services present similar issues. *See id.*

[53] 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.").

[54] *See* Woodrow Hartzog, *Chain-Link Confidentiality*, 46 GA. L. REV. 657, 680 (2012) ("Websites that use cookies, Web bugs, and other data collection techniques have access to a host of information including comprehensive browsing and search histories, payment information, and contact information such as addresses, phone numbers, and email addresses.") (footnotes omitted).

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

[56] *Cf.* Solove, *supra* note 36, at 1092 (explaining the false sense of privacy many people hold on the Internet: "[t]he secrecy and anonymity of the Internet is often a mirage").

[57] As the developers explain:

> Lightbeam is a Firefox add-on that uses interactive visualizations to show you the first and third party sites you interact with on the Web. As you browse, Lightbeam reveals the full depth of the Web today, including parts that are not transparent to the average user.

The tool distinguishes between the first-party websites the user intentionally visits, and the third parties at other Internet addresses who send data to or receive data from the user.[58] When Alex Fowler of Mozilla demonstrated the tool, he interacted with over 120 different companies in the course of visiting just four websites.[59]

The case for extending confidentiality protections to these intra-institutional third parties is especially strong, because to ignore them would be to permit the erosion of privacy within institutions where society expressly recognizes a need for privacy. The following Parts illustrate this problem in the context of the library confidentiality regime. Part II details the library confidentiality regime. Part III then describes an arrangement whereby Amazon has become involved in library transactions without being constrained by this regime.

II. THE LIBRARY CONFIDENTIALITY REGIME

Librarians take responsibility for promoting private reading because they recognize the democratic values it protects. The American Library Association ("ALA") defines "privacy" as "the right to open inquiry without having the subject of one's interest examined or scrutinized by others,"[60] and they protect it directly by creating an environment where patrons can engage in unmonitored reading, for example when they browse books on the shelf and read them in the library. Libraries also protect privacy through a regime of "confidentiality," which the ALA defines as "exist[ing] when a library is in possession of personally identifiable information about users and keeps that information private on their behalf."[61] The library profession recognizes that patrons may hesitate to seek assistance if they fear their interests will be disclosed, so to promote free inquiry they protect reference requests, circulation records, and similar materials created through interactions with patrons.[62]

Mozilla, *Lightbeam for Firefox*, MOZILLA.ORG, http://www.mozilla.org/en-US/lightbeam/ (last visited Dec. 22, 2013); *see also* Brian Fung, *Who Tracks the Trackers that Track You Online? You Can, with Lightbeam*. WASHINGTON 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/ (explaining and demonstrating the tool).

[58] *See Lightbeam for Firefox*, *supra* note 57.

[59] Dell Cameron, *Discover Which Companies Are Tracking You Online with Lightbeam*, DAILY DOT (Oct. 28, 2013), http://www.dailydot.com/politics/mozilla-lightbeam-firefox-privacy/.

[60] OFFICE OF INTELLECTUAL FREEDOM, AM. LIBRARY ASS'N, INTELLECTUAL FREEDOM MANUAL 191 (7th ed. 2006).

[61] *Id.*

[62] *See* Richards, *Perils of Social Reading*, *supra* note 4, at 712.

Librarians' protection for private inquiry consists of three interrelated frameworks: professional norms and ethics, library privacy statutes, and administrative policies and procedures. These frameworks, explored in the following Sections, establish a confidential relationship between librarians and their patrons, and restrict the uses and disclosures a librarian may make of patrons' records. Moreover, the confidentiality regime derives much of its force from librarians' normative commitments rather than formal legal obligations. As this Part shows, these commitments evolved primarily in response to controversial government attempts to monitor citizens' reading.

A. Library Norms and Ethics in Historical Context

Librarians view their protection of private inquiry as fundamental to promoting democracy and individual liberty.[63] They have articulated and re-articulated this commitment to intellectual privacy through codes of ethics and public statements many times over the past seven decades in response to perceived threats. Significantly, librarians resisted the disclosure of patron records even when they had no legal obligation to do so. This Section describes the threats to privacy that libraries have faced and the normative commitments the profession has adopted in response.[64]

The profession's stance on intellectual freedom first coalesced when the ALA adopted its 1939 Library Bill of Rights, drafted in response to nationwide pressures to ban John Steinbeck's *The Grapes of Wrath*.[65] Mindful that "indications in many parts of the world point[ed] to growing intolerance, suppression of free speech, and censorship affecting the rights of minorities and individuals," the ALA rejected discrimination on the basis of an author's viewpoint and declared "[t]he library as an institution to educate for democratic living."[66] With this move, the profession cast off the

[63] Am. Library Ass'n, *Why Libraries?*, CHOOSE PRIVACY WEEK, http://chooseprivacyweek.org/our-story/why-libraries/ (last visited Dec. 22, 2013) ("[T]he freedom to read and receive ideas anonymously is at the heart of individual liberty in a democracy.").

[64] This history is also relevant to the development of library protection laws and the profession's policies and practices, discussed below in Sections II.B and II.C, and alluded to throughout the present Section. For parsimony, however, the historical discussion is confined mainly to this Section.

[65] Judith F. Krug, *ALA and Intellectual Freedom: A Historical Overview*, *in* INTELLECTUAL FREEDOM MANUAL, *supra* note 60, at 14, 18.

[66] INTELLECTUAL FREEDOM MANUAL, *supra* note 60, at 58-59.

ambivalence that previously characterized it,[67] and adopted a new role as protector of democracy and intellectual freedom.

The same year, the ALA formalized the profession's commitment to privacy with its 1939 Code of Ethics: "It is the librarian's obligation to treat as confidential any private information obtained through contact with library patrons."[68]

Librarians battled censorship over the next several decades, particularly during the McCarthy era.[69] Their commitment to privacy did not face its first major tests until the 1970s. IRS agents approached public libraries in 1970 to request access to circulation records so they could determine who had been reading about explosives or guerilla warfare.[70] The IRS attempted to do so without "any process, order, or subpoena."[71] The profession's response was swift: the ALA issued an advisory statement condemning the attempted surveillance as "an unconscionable and unconstitutional invasion of the right of privacy of library patrons," and urging libraries to adopt confidentiality policies requiring a court order prior to the release of any records.[72] The U.S. Department of Treasury relented and publicly stated it would discontinue this search program.[73] Subsequently, the ALA's advisory statement grew into its 1971 Policy on Confidential Records,[74] which continues to "strongly recommend[]" that each library adopt a policy specifically recognizing the confidentiality of circulation records, and release these records only subject to "process, order, or subpoena" which is in "proper form" and issued with "a showing of good cause."[75]

Meanwhile, the FBI targeted academic libraries. In 1971, it came to light the FBI had been monitoring the activities of Father Philip Berrigan at a college library.[76] Berrigan had been arrested along with six other Vietnam

---

[67] Prior to 1939, the role of librarians in society was a source of contention. In the late 1800s, when ALA was formed, many librarians acted as moral censors whose goal was to uplift the masses, while a vocal minority advocated exposing people to a variety of opinions and viewpoints. Blitz, *supra* note 4, at 837-39. The 1939 Library Bill of Rights marked a sea change. *Id.* at 837-38.

[68] INTELLECTUAL FREEDOM MANUAL, *supra* note 60, at 257.

[69] *Id.* at 60-61.

[70] FOERSTEL, *supra* note 24, at 4-5 ("Their investigations took them to urban centers across the country, cutting a swath so wide as to reveal the names of teenagers working on term papers."); Krug, *supra* note 65, at 21-22.

[71] FOERSTEL, *supra* note 24, at 5.

[72] *Id.* at 5-6.

[73] *Id.* at 5.

[74] INTELLECTUAL FREEDOM MANUAL, *supra* note 60, at 297.

[75] *Id.* at 293, 294-95 & n.*.

[76] FOERSTEL, *supra* note 24, at 7-8.

War protestors, collectively known as the "Harrisburg Seven," who were charged with an alleged conspiracy to kidnap Henry Kissinger and destroy certain Pentagon computers.[77] He was working at the library pursuant to a prison work-release program while he awaited trial.[78]

The FBI subsequently sent agents to question library staff in an attempt to enlist them as informants.[79] Zoia Horn, head reference librarian at the college, rebuffed the agents and spearheaded an ALA resolution condemning the presence of government spies in the library, asserting the importance of library confidentiality and resolving that librarians should not volunteer patrons' reading habits to the government.[80] When it came time for trial, Horn refused to testify and was jailed twenty days for contempt of court.[81]

In the face of these government intrusions into patrons' activities, the profession continued to affirm its commitment to confidentiality. The ALA's 1975 Statement on Professional Ethics, for example, states expressly that a librarian "[m]ust protect the essential confidential relationship which exists between a library user and the library."[82]

From the late 1970s through the late 1980s, libraries faced additional pressures not just from law enforcement, but also from private actors seeking to pry into their neighbors' and family members' business under the auspices of state open records laws.[83] In some of the more colorful non-law enforcement requests, a Florida religious group asked who checked out certain books so it could invite these people to join the group; a married man in Virginia requested his wife's circulation records in an attempt to prove she had been plotting a divorce; and the Christian-right political organization Moral Majority asked the Washington State Library to release the names of school teachers who borrowed a particular sex-education film.[84] Incidents like these incensed the library community, whose confidentiality norms were well established by this point. The profession

---

[77] *Id.*; *see* Ramsey Clark, *"How Can You Represent that Man?": Ethics, the Rule of Law, and Defending the Indefensible*, 44 GA. L. REV. 921, 927 (2010). As one juror commented after trial: "I thought the whole thing was kind of funny, the idea of a bunch of priests and nuns zipping off with Henry Kissinger." FOERSTEL, *supra* note 24, at 8.

[78] FOERSTEL, *supra* note 24, at 7.

[79] Bruce M. Kennedy, *Confidentiality of Library Records: A Survey of Problems, Policies, and Laws*, 81 LAW LIBR. J. 733, 741-42 (1989).

[80] FOERSTEL, *supra* note 24, at 9; Kennedy, *supra* note 79, at 742.

[81] FOERSTEL, *supra* note 24, at 9.

[82] Am. Library Ass'n, *Statement on Professional Ethics, 1975*, ALA.ORG, http://www.ala.org/advocacy/proethics/history/index3 (last visited Dec. 22, 2013).

[83] *See* FOERSTEL, *supra* note 24, at 123-25; Kennedy, *supra* note 79, at 755.

[84] FOERSTEL, *supra* note 24, at 123.

was remarkably successful in lobbying for state laws protecting library circulation records against open-records requests, and sometimes even against law enforcement investigations.[85]

At the same time librarians were winning victories with state lawmakers, federal agents had begun administering yet another covert library surveillance program. For a brief period from 1973-1976, and again beginning in 1985, the FBI engaged in the "Library Awareness Program."[86] In late 1987, it came to light that FBI agents were approaching library clerks to ask what "suspicious-looking foreigners" had been reading, in some cases requesting circulation records.[87] In effect the FBI was asking librarians to profile library use by "people with accents or 'with foreign-sounding names.'"[88] The profession publicly expressed its outrage that government spies had once again infiltrated libraries, and it won the support of members of Congress, who called the FBI to testify on the program.[89] Rep. Don Edwards (D-CA), a former FBI agent himself, chastised the FBI: "You have not measured what you are doing to freedom of speech and privacy and so forth against the panic that you are causing in this country. And it is real."[90] While the FBI never publicly abandoned the program, at the very least it was forced to change its tactics.[91] In the wake of this incident, many states passed additional library privacy statutes or updated existing laws to better protect against government intrusion.[92]

The profession recently re-articulated its stance on privacy in response to federal surveillance under the Patriot Act, which was signed into law on October 26, 2001.[93] Section 215 of the Patriot Act permits the

---

[85] *See* Kennedy, *supra* note 79, at 745, 758. The statutes are described in greater detail below. *See infra* Section II.B.
[86] FOERSTEL, *supra* note 24, at 14.
[87] Krug, *supra* note 65, at 22-23.
[88] Nat Hentoff, *The FBI in the Library*, WASH. POST, July 23, 1988, at A3.
[89] FOERSTEL, *supra* note 24, at 27-32; Linda Greenhouse, *F.B.I. Search for Spies in Library Is Assailed*, N.Y. TIMES June 21, 1988, at A16. The hearing is transcribed on public record as *FBI Counterintelligence Visits to Libraries: Hearing Before the Subcomm. on Civil and Constitutional Rights of the H. Comm. on the Judiciary*, 100th Cong. (1988).
[90] *FBI Counterintelligence Visits to Libraries*, 100th Cong. 121 (statement of Rep. Don Edwards); *see* FOERSTEL, *supra* note 24, at 44-45.
[91] *See* Krug, *supra* note 65, at 23.
[92] *See* FOERSTEL, *supra* note 24, at 134; Anne Klinefelter, *Privacy and Library Public Services: Or, I Know What You Read Last Summer*, 26 LEGAL REFERENCES SERV. Q. 253, 259 (2007) (explaining most library privacy laws "were passed in reaction to the Library Awareness Program of the 1970s and later"). Only thirty-eight states had library privacy laws at the time the Library Awareness Program came to light in 1987, compared to forty-two by the end of 1989 or today's forty-eight. FOERSTEL, *supra* note 24, at 133; Krug, *supra* note 65, at 22.
[93] USA PATRIOT ACT of 2001, Pub. L. No. 107-56, 115 Stat. 272.

government to request "any tangible things (including books, records, papers, documents, and other items)."[94] Such a request is typically accompanied by a nondisclosure order, or "gag order," which prohibits the recipient from speaking publicly about receiving or complying with the request.[95] When Congress re-authorized the Patriot Act in 2006,[96] it made clear that "library circulation records, library patron lists, book sales records, [and] book customer lists . . . containing information that would identify a person" are subject to a Section 215 request.[97] Section 505, which governs the issuance of National Security Letters ("NSLs"), permits the government to obtain an order requesting "subscriber information and toll billing records information, or electronic communication transactional records."[98] NSLs are also typically accompanied by a gag order.[99]

Gravely concerned that the Patriot Act increased the federal government's ability to monitor library use, the ALA passed a resolution declaring that "sections of the USA PATRIOT ACT are a present danger to the constitutional rights and privacy rights of library users" and urging Congress to take action.[100] The ALA also called on the profession to re-double its efforts to avoid collecting and retaining unnecessary information,

[94] 50 U.S.C. § 1861(a)(1) (2006).

[95] *Id.* § 1861(d); *cf.* In re Nat'l Sec. Letter, 930 F. Supp. 2d 1064, 1074 (N.D. Cal. 2013) (noting that the government issues a nondisclosure order with 97% of the requests it makes via National Security Letter ("NSL")).

[96] USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006, Pub. L. No. 109-178, 120 Stat. 278.

[97] 50 U.S.C. § 1861(a)(3).

[98] 18 U.S.C. § 2709(a) (2006).

[99] *Id.* § 2709(c); In re Nat'l Sec. Letter, 930 F. Supp. 2d at 1074. Note, however, that the Northern District of California in *In re National Security Letter* recently held that the NSL statute is unconstitutional because, *inter alia*, the nondisclosure provision violates the First Amendment (albeit not on intellectual privacy grounds). *See generally id.* The ruling is stayed pending appeal.

[100] Am. Library Ass'n, *Resolution on the USA Patriot Act and Related Measures that Infringe on the Rights of Library Users*, ALA.ORG (Jan. 29, 2003), http://www.ala.org/offices/oif/statementspols/ifresolutions/resolutionusa [hereinafter ALA Resolution (Jan. 29, 2003)]; *see also* Am. Library Ass'n, *Resolution on the USA PATRIOT Act and Libraries*, ALA.ORG (June 29, 2005), http://www.ala.org/advocacy/intfreedom/statementspols/ifresolutions/usapatriotactlibraries [hereinafter ALA Resolution (June 29, 2005)] (expressing particular concern regarding Section 215, arguing that it allows "the government to secretly request and obtain library records for large numbers of individuals without any reason to believe they are involved in illegal activity," and Section 505, arguing that it permits "the FBI to obtain electronic records from libraries with a National Security Letter without prior judicial oversight").

tacitly advising its constituents that the government cannot obtain records that do not exist.[101]

One of the first legal challenges to the Patriot Act's NSL provisions came from the "Connecticut Four," a group of three librarians and a computer systems engineer working for a Connecticut library consortium called Library Connection.[102] In 2005, the FBI issued an NSL under Section 505 of the Patriot Act, along with an accompanying gag order, to Library Connection.[103] The FBI was interested not in what books patrons had been reading, but their Internet activity: the order demanded "any or all subscriber information, billing information and access logs of any person or entity" that had used computers during a specific 45 minute timeframe at any of the 26 libraries who were members of the consortium.[104]

The U.S. District Court for Connecticut held the gag order was invalid, but it entered a stay preserving the gag order pending the government's appeal.[105] In the meantime, Congress debated the extension of the Patriot Act.[106] The Connecticut Four wanted "to speak about their own experience and to impress upon Congress their view that the FBI should not be allowed to demand information like this without judicial review," but the gag order constrained them.[107] The FBI subsequently withdrew the gag order and its NSL requests, but only after the Patriot Act's 2006 extension.[108] The Connecticut Four's stance, despite the considerable

---

[101] ALA Resolution (Jan. 29, 2003), *supra* note 100; *see also* INTELLECTUAL FREEDOM MANUAL, *supra* note 60, at 193 (encouraging these kinds of policies); *infra* Section II.C (explaining the significance of libraries' practices and procedures for protecting patrons' confidentiality).

[102] *See* SUSAN N. HERMAN, TAKING LIBERTIES: THE WAR ON TERROR AND THE EROSION OF AMERICAN DEMOCRACY 139-40 (2011); *see also* Doe v. Gonzalez, 386 F. Supp. 2d 66, 74 n.6 (D. Conn. 2005) (explaining that this case was at the time one of only three known challenges to any NSL issued under 18 U.S.C. § 2709).

[103] HERMAN, *supra* note 102, at 136-37.

[104] *Id.* at 136-38; Amy Goodman & David Goodman, *America's Most Dangerous Librarians*, MOTHER JONES, Sept./Oct. 2008, at 42.

[105] 386 F. Supp. 2d at 82-83; *stay aff'd* Doe v. Gonzalez, 546 U.S. 1301 (2005).

[106] HERMAN, *supra* note 102, at 140.

[107] *Id.* Ironically, *The New York Times* had discovered and published the identities of the Connecticut Four well in advance of the Patriot Act's renewal, Alison Leigh Cowan, *Librarians Must Stay Silent in Patriot Act Suit, Court Says*, N.Y. TIMES, Sept. 21, 2005, at B2, yet the FBI insisted the gag order remain in place. *See* HERMAN, *supra* note 102, at 143-45.

[108] HERMAN, *supra* note 102, at 145. After the gag order was lifted—which was after the Patriot Act had been extended—Library Connection Executive Director George Christian wrote: "The fact that I can speak now is a little like being permitted to call the Fire Department only after a building has burned to the ground." George Christian, Doe v. Gonzales*: Fighting the FBI's Demand for Library Records*, ACLU.ORG (May 30, 2006),

difficulty of challenging the Patriot Act, is a telling illustration of the profession's continuing normative commitment to protecting patrons' privacy.

B. Library Privacy Statutes

Forty-eight states and the District of Columbia have enacted laws protecting library records from disclosure.[109] Considerable variation pervades this patchwork of state law, vesting private reading with greater formal protection in some states than others.

The difference in the laws is partly accounted for in the fact that the statutes respond to two different sets of problems: protecting against disclosure under state open-records laws versus protecting against overreaching by law enforcement. A statute protecting only against open-records requests may be limited in scope and merely exempt library records from such requests.[110] Laws like these may prevent citizens and private groups from spying on their neighbors or pushing their agendas on those who read controversial books, yet "afford no protection against government requests."[111]

Other statutes are broad enough to cover not only private open-records requests, but also certain government requests. These statutes typically allow disclosure of library records only subject to a warrant or similar process.[112] Some states go further, imposing heightened substantive requirements as a prerequisite to issuance of a warrant for library records. Iowa, for example, requires "a judicial determination that a rational connection exists between the requested release of information and a

---

http://www.aclu.org/national-security/doe-v-gonzales-fighting-fbis-demand-library-records-statement-george-christian.

[109] For a complete listing of these laws, see Klinefelter, *supra* note 38, app.; and Am. Library Ass'n, *State Privacy Laws Regarding Library Records*, ALA.ORG., http://www.ala.org/offices/oif/ifgroups/stateifcchairs/stateifcinaction/stateprivacy (last visited Dec. 22, 2013). Bruce Kennedy has created a helpful five-part framework for comparing these laws. Kennedy, *supra* note 79, at 754-66 (comparing statutory design, scope of the privacy rights, exceptions to the privacy rights, disclosure procedures, and sanctions).

In the two states without statutory protection—Hawaii and Kentucky—the state attorneys general have issued opinions recognizing certain protections for library records. *See* Haw. Op. Att'y Gen. 90-30 (Oct. 23, 1990), 1990 WL 482378; Ky. Op. Att'y Gen. 82-149 (Mar. 12, 1982), 1982 WL 176791; Ky. Op. Att'y Gen. 81-159 (Apr. 21, 1981), 1981 WL 142193.

[110] *See, e.g.*, DEL. CODE ANN. tit. 29, § 10002(l)(12) (Supp. 2012).

[111] Kennedy, *supra* note 79, at 758.

[112] *See, e.g.*, ARK. CODE ANN. § 13-2-704(3) (Supp. 2013) (permitting disclosure to law enforcement only pursuant to a search warrant).

legitimate end and that the need for the information is cogent and compelling."[113]

Protection is sometimes discretionary under these laws. Rather than prohibit disclosure, some statutes permit a librarian to choose whether to withhold a record.[114] These statutes legitimate the decisions librarians would make pursuant to their normative commitments, but they impose no independent obligation.

The penalties for violating these laws also vary. Most laws are silent regarding civil liability, although a handful provide statutory damages and fee-shifting for prevailing plaintiffs.[115] Where the laws are silent, patrons might be able to pursue a tort action for invasion of privacy or breach of confidentiality.[116]

Finally, practically all states permit disclosure of library records with the patron's consent. Many state laws say so explicitly,[117] and, as Bruce Kennedy recognizes, disclosure subject to consent is implied under the remaining laws: because the laws are designed to protect patrons' privacy, patrons should be capable of waiving this protection.[118]

C. Library Policies and Procedures

In order to fulfill their professional and legal obligations, libraries have designed their administrative and technical infrastructures to safeguard patrons' records. In particular, library systems are built to avoid collecting or retaining a patron's reading history and to facilitate patrons' anonymous browsing of third-party resources.

---

[113] IOWA CODE ANN. § 22.7(13) (West 2010). As Kennedy explains, this heightened requirement is the result of the Iowa legislature's dissatisfaction that the courts construed a prior version of the law to apply only against citizen public-records requests, not law enforcement requests. Kennedy, *supra* note 79, at 758.

[114] *See, e.g.*, IND. CODE ANN. § 5-14-3-4(b)(16) (LexisNexis Supp. 2013) (including "library records" in a class of records that can be exempted from the public records law "at the discretion of a public agency"); *see also* Kennedy, *supra* note 79, at 762 & n.139 (collecting similar statutes).

[115] *See, e.g.*, MICH. COMP. LAWS § 397.604 (West 1997) (providing $250 in statutory damages plus attorney fees and the costs of the action); *see also* Kennedy, *supra* note 79, at 765.

[116] *See* Kennedy, *supra* note 79, at 765; *see also* Richards & Solove, *supra* note 3, at 157 ("A plaintiff can establish a breach of confidence action by proving the existence and breach of a duty of confidentiality.").

[117] *See, e.g.*, ARIZ. REV. STAT. ANN. § 41-151.22(B)(2) (2013); ARK. CODE ANN. § 13-2-704(2) (Supp. 2013).

[118] Kennedy, *supra* note 79, at 763. For discussion of how the notice and comment model might be abused, *see infra* Section V.B.

A library's records policies are its patrons' first line of defense against disclosure of their reading history. The profession's norms and statements of ethics are not legally binding and, as noted above, many privacy statutes permit liberal disclosures. A library's local policies fill the gaps by establishing protective day-to-day practices.[119]

These day-to-day practices often include technical measures to reduce the amount of data collected or subsequently retained. One of the most commonplace and effective measures is deleting circulation records as soon as a book is returned.[120] Under these systems, the record that someone has borrowed a book lingers only long enough to ensure its return. These practices keep with the ALA's recommendation that libraries adopt policies that avoid the creation or retention of unnecessary records.[121] This practice makes it difficult for any government or private entity to query a person's prior reading habits, regardless of the laws or policies that otherwise govern those requests, because the records do not accumulate.[122]

Beyond protecting book circulation records, libraries also facilitate anonymous access to third-party databases and the Internet. Rather than requiring patrons to create an account with a research database, for example, libraries often create an institutional account and then authenticate patrons on its network as valid users.[123] This strategy is thwarted, of course,

---

[119] Klinefelter, *supra* note 38, at 557-58; *see generally* INTELLECTUAL FREEDOM MANUAL, *supra* note 60, at 304-13 (offering detailed guidelines regarding confidentiality policies and law enforcement inquiries).

[120] *See* Mary Minow, *Library Patron Records and Freedom of Information Laws*, LIBRARYLAW (1998), http://www.librarylaw.com/publicrecords.html ("In part to protect confidentiality, most circulation systems delete circulation records after they are no longer needed to track a book."); Dean E. Murphy, *Some Librarians Use Shredder To Show Opposition to New F.B.I. Powers*, N.Y. TIMES, Apr. 7, 2003, at A12 (explaining, in the wake of the Patriot Act, "the shredder here is not new, but the rush to use it is").

[121] INTELLECTUAL FREEDOM MANUAL, *supra* note 60, at 307; *see also* Kennedy, *supra* note 79, at 766 ("Libraries should become information storage centers *for* their patrons, and not *about* their patrons."). Interestingly, at least one state mandates these practices. *See* ARK. CODE ANN. § 13-2-703(b) (2003) ("Public libraries shall use an automated or Gaylord-type circulation system that does not identify a patron with circulated materials after materials are returned.").

[122] Viktor Mayer-Schönberger recognizes a similar point in his book *Delete*, where he explains the importance of users' ability to delete records of their online activities, or at least to have their records expire. *See generally* VIKTOR MAYER-SCHÖNBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE (2009).

[123] *See* Klinefelter, *supra* note 38, at 559. Legal researchers accessing HeinOnline through a university or law-firm network often benefit from such institutional subscriptions.

by services (like the lending of Kindle e-books[124]) that require individualized logins.[125]

Libraries support anonymous Internet browsing more generally by allowing patrons to access websites using library computers, which carry the library's IP address rather than one linked to the user's home or workplace,[126] and by eliminating records that identify which patrons utilized library computers at a particular time.[127] Recall that the NSL that the Connecticut Four resisted was one in which the privacy of library patrons' Internet usage was at issue.[128]

* * *

To fulfill their normative and legal commitments, librarians have built an administrative and technical architecture that is highly protective of patrons' privacy and therefore protective of free-speech values.[129] While this regime has proven capable of dealing with many threats to privacy in the pre-networked world, the next Part demonstrates its inadequacies with respect to the third-party information providers ubiquitous in digital transactions and communications.

III. E-BOOK LENDING ILLUSTRATES THE LIBRARY REGIME'S LIMITS

Despite their longstanding commitment to intellectual privacy, libraries currently broker transactions whereby patrons, using services facilitated and paid for by the library (often with taxpayer dollars), tender detailed records of their reading habits to a third party. The third party does not share libraries' normative commitments or legal obligations to protect

[124] *See infra* Section III.A.

[125] Klinefelter, *supra* note 38, at 559. Legal researchers likely recognize the ongoing need to provide an individualized LexisNexis or Westlaw password as an example of this approach.

[126] *See id.* at 561.

[127] *See* HERMAN, *supra* note 102, at 147 (describing a library's daily shredding of computer sign-up sheets); INTELLECTUAL FREEDOM MANUAL, *supra* note 60, at 350 (advising that librarians "protect the confidentiality of records, electronic or otherwise, that identify individual users and link them to search strategies, sites accessed, or other specific data about the information they retrieved or sought to retrieve" and "destroy all unnecessary Internet use records"). *But see* David E. Rosenbaum, *A Nation Challenged: Questions of Confidentiality*, N.Y. TIMES, Nov. 23, 2001, at B7 (explaining that librarians voluntarily turned over computers they believed had been used by the hijackers behind the September 11, 2001 attacks on the World Trade Center and the Pentagon).

[128] *See supra* notes 102-108 and accompanying text.

[129] *See* Balkin, *supra* note 21, at 47-49, 50-52 (describing the importance of encoding free-speech values into technological and regulatory infrastructures); Richards, *Intellectual Privacy*, *supra* note 4, at 430 (arguing for the recognition of intellectual privacy as a free-speech value within Balkin's framework).

patrons' data, and does not implement protective practices like deleting information once borrowed materials are returned.

The example under scrutiny in this Article is the arrangement libraries have entered with Amazon via a service called Overdrive.[130] Overdrive, an entity separate from Amazon, provides e-book lending services for libraries.[131] For years, Overdrive had offered e-books for the Barnes & Noble nook e-reader, the Sony Reader, and various other devices, notably excluding Amazon's Kindle.[132] In this process, the patron typically did not turn over personally identifiable information such as name, email address, or even library card number to Overdrive or any other non-library entity. Instead, the patron logged into the library system, and the library certified to Overdrive that the patron was entitled to borrow e-books.[133]

On September 21, 2011, Overdrive began offering e-books for the Kindle.[134] This borrowing process differs from Overdrive's prior practices. After a patron selects a title using Overdrive's service, he is routed to Amazon's website to complete the transaction and asked to give up his anonymity by logging in using the Amazon account associated with his

[130] To be clear, this Article is about the challenges facing confidentiality in today's information economy. It is not an indictment of Amazon's practices. Although Amazon's arrangement with libraries serves as my case study, and I argue that reading records are inadequately protected under this arrangement, I disclaim the argument that Amazon is a bad actor. Its Privacy Notice, while not perfect, protects user information in several important ways, including against unfettered disclosure. *See Privacy Notice*, AMAZON.COM, http://www.amazon.com/privacy (last updated Apr. 6, 2012); *see also infra* notes 149-150 and accompanying text. Moreover, Amazon has asserted its customers' privacy rights and successfully challenged government attempts to obtain records of its customers' retail purchases in at least two cases. *See* Amazon.com LLC v. Lay, 758 F. Supp. 2d 1154 (W.D. Wash. 2010); In re Grand Jury Subpoena to Amazon.com, 246 F.R.D. 570 (W.D. Wis. 2007). Scrutiny of Amazon's current practices is nonetheless informative because these practices expose significant gaps in the protection of reading records in contemporary e-commerce. Moreover, notwithstanding the protections Amazon provides, Amazon reserves the right to change its position, *see* Privacy Notice, *supra*, and other companies with access to similar records might make less protective choices.

[131] *See* Julie Bosman, *Kindle Connects to Library E-Books*, N.Y. TIMES, Sept. 22, 2011, at C1. To date, Overdrive is the only such service that provides e-books for the Kindle. Michael Kelley, *OverDrive & Big (Private) Data*, LIBRARYJOURNAL (Mar. 11, 2013), http://lj.libraryjournal.com/2013/03/opinion/editorial/overdrive-big-private-data/.

[132] Bosman, *supra* note 131.

[133] *See OverDrive*, OCLC, http://www.oclc.org/support/services/ezproxy/documentation/db/overdrive.en.html (last visited Dec. 22, 2013) (describing authentication procedures that withhold personally identifiable information from Overdrive). This sort of authentication scheme is consistent with libraries' historical practice of providing institutional subscriptions or in-house authentication schemes to protect patrons from having to identify themselves to third-party databases. *See supra* Section II.C.

[134] Bosman, *supra* note 131.

Kindle.[135] From that point onward, Amazon treats the information the same as it treats information from retail sales: it matches the book selection with the individual's account, it tracks granular data on the patron's reading habits, and it uses the data for marketing purposes.[136]

A. Amazon Uses E-Book Lending Records for Marketing

Many librarians were surprised to learn Amazon was collecting patrons' data. Indeed, many learned about Amazon's practices only after patrons complained about the promotional emails Amazon had begun sending them.[137] Around the time a borrowed Kindle e-book came due for return, Amazon emailed patrons to inform them of their books' pending expirations and invite them to purchase the books.[138] These invitations indicated not only that Amazon knew the patron had checked out a particular book (the type of fact a library would traditionally know), but also that Amazon knew the patron had not finished reading it (something Amazon knew only because of the monitoring built into the Kindle).

It has subsequently come to light that—just as Amazon collects detailed profiles of its paying customers' reading habits[139]—Amazon collects detailed profiles on its library patrons including pages read, passages highlighted, and annotations made.[140] Because a patron logs into the book-borrowing service using the same account he uses for book purchases, the reader's paid-book and borrowed-book histories are compiled into a single profile linked with the reader's identity.[141]

---

[135] *See Borrow Books from a Public Library*, AMAZON.COM, http://www.amazon.com/help/kindle/publiclibraries (last visited Dec. 22, 2013) ("At checkout, sign in to your Amazon account, and select the device or reading app to send the book to.").

[136] *See infra* Section III.A.

[137] Marc Parry, *As Libraries Go Digital, Sharing of Data Is at Odds with Tradition of Privacy*, CHRON. HIGHER EDUC. (Nov. 5, 2012), http://chronicle.com/article/As-Libraries-Go-Digital/135514/.

[138] *Id.*

[139] *See, e.g.*, NICOLE A. OZER, ACLU OF NORTHERN CALIFORNIA, DIGITAL BOOKS: A NEW CHAPTER FOR READER PRIVACY 5 (2010), *available at* https://www.aclunc.org/issues/technology/asset_upload_file295_9047.pdf; Jennifer Elmore, Note, *Effective Reader Privacy for Electronic Books: A Proposal*, 34 HASTINGS COMM. & ENT. L.J. 127, 135 n.63 and accompanying text; Richards, *Perils of Social Reading*, *supra* note 4, at 698 n.56 and accompanying text.

[140] *See* Deborah Caldwell-Stone, *A Digital Dilemma: Ebooks and Users' Rights*, AM. LIBRARIES, May/June 2012, at 20, 22.

[141] To avoid this linkage, Overdrive recommends that users concerned about privacy create a separate Amazon account for library borrowing. *See* Lindsey Levinsohn, *A Note on Library Patron and Student Privacy*, DIGITAL LIBRARY BLOG (Oct. 4, 2011), http://overdriveblogs.com/library/2011/10/04/a-note-on-library-patron-and-student-

Amazon utilizes this data for targeted marketing, subject to its Conditions of Use, Privacy Notice, and related terms of service.[142] One of the most direct uses, described above, is the attempt to convert the borrower into a purchaser. Amazon also recommends other books for purchase by extrapolation from books the user has previously read.[143] Advertisements for these materials appear not only on Amazon.com itself, but also as "interest-based advertising" on other websites.[144] Even though customers might prefer not to create a permanent record of their shopping and reading, Amazon makes no promises to delete information it has collected, and it does not provide patrons with the option to clear their records.[145]

---

privacy/. This advice ignores both the hassle created by maintaining and switching between two accounts and the reality that, so long as the separate account is linked to a Kindle, Amazon will have the means to link that account with the purchaser of the Kindle. *Librarians Weigh Kindle Ebook Lending Against Reader Privacy*, AMERICAN LIBRARIES BLOG (Oct. 19, 2011), http://www.americanlibrariesmagazine.org/blog/librarians-weigh-kindle-ebook-lending-against-reader-privacy.

[142] *See Conditions of Use*, AMAZON.COM, http://www.amazon.com/conditionsofuse (last updated Dec. 5, 2012); *Privacy Notice*, *supra* note 130.

[143] Amazon founder and CEO Jeff Bezos himself has been embarrassed by Amazon's recommendation system: years ago, when he was demonstrating the personalized recommendations feature to an audience of financial analysts, the system recommended he purchase a DVD copy of the B-movie *Slave Girls from Beyond Infinity* (Titan Productions 1987). Monty Phan, *Online Retailers Are Trying To Pair Consumers with What They Like, but the System Has Proven a Double-Edged Sword*, NEWSDAY, May 15, 2005, at A36. To be sure, *Slave Girls from Beyond Infinity* is the type of film one might be embarrassed for others to see among one's recommended purchases. Senator Jesse Helms (R-North Carolina) specifically criticized it on the Senate floor as an example of indecent programming cable providers should be forced to block. 138 CONG. REC. S587-01 (daily ed. Jan. 29, 1992) (statement of Sen. Jesse Helms).

Users today have the option to curate their recommendations by excluding parts of their purchase history on an ad-hoc basis from being considered when Amazon makes recommendations. *See Improve Your Recommendations*, AMAZON.COM, http://www.amazon.com/gp/help/customer/display.html/?nodeId=13316081 (last visited Dec. 22, 2013).

[144] *Interest-Based Ads*, AMAZON.COM, http://www.amazon.com/interestbasedads (last visited Dec. 22, 2013) ("On both Amazon-owned and operated sites *and unaffiliated sites*, Amazon displays interest-based advertising using information you make available to us . . . .") (emphasis added). Accordingly, one's tastes in books—be they cookbooks or erotica—might be exposed through personally targeted advertising that appeared on non-Amazon websites. Note that Amazon does offer users the option to turn off interest-based ads, giving informed users the ability to mitigate this exposure. *Id.*

[145] *E-Reader Privacy Chart, 2012 Edition*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/pages/reader-privacy-chart-2012 (last visited Dec. 22, 2013). As noted above, however, Amazon offers its users certain options to mitigate embarrassing uses of the data by curating the recommendations that are displayed or turning off interest-based ads. *See supra* notes 143-144.

Amazon's terms of service also reserve the right to use readers' data in other, less transparent ways. For example, it partners with "affiliated businesses" and "share[s] customer information related to those transactions" with these businesses.[146] It also shares "personal information" with third-party service providers for functions such as "analyzing data" and "providing marketing assistance."[147] Little public information is available on these relationships or the extent of data disclosed. Moreover, these are just the business uses that Amazon makes of the data. Amazon's collection and retention of the information may also facilitate government access or other unintended uses of the data.[148]

Notwithstanding the liberties that Amazon claims, its Privacy Notice contains a number of consumer-friendly protections: outright sales or disclosures of personally identifiable information are prohibited, subsidiaries are required to adopt privacy practices at least as protective as Amazon's own, and Amazon commits itself not to retroactively reduce the protections in place for data it has already collected.[149] While consumers today enjoy these protections, Amazon reserves the right to change its policies prospectively,[150] and other parties who moved into the same niche may not adopt similar terms.

B. Collecting Reading Records Creates Risks for Intellectual Privacy

Privacy scholars and activists often focus on government intrusions, warning of a growing surveillance state in the style of George Orwell's *Nineteen Eighty-Four*. Notably, commentators have invoked Orwell even when addressing e-book vendors' collection of readers' data, even though these vendors are private corporations, not state actors.[151] Recent scholarship, however, suggests this allusion may be justified insofar as corporate monitoring poses threats to intellectual development and free expression similar to those posed by government monitoring, and insofar as private monitoring facilitates government access.[152] Yet the Orwellian

[146] *Privacy Notice*, *supra* note 130.
[147] *Id.*
[148] *See infra* Section III.B.
[149] *Privacy Notice*, *supra* note 130.
[150] *See id.* ("Our business changes constantly, and our Privacy Notice and Conditions of Use will change also.").
[151] *See, e.g.*, Alison Flood, *Big E-Reader Is Watching You*, GUARDIAN (U.K.), July 5, 2012.
[152] *See supra* note 6. *But see* Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393 (2001) (arguing that the Big Brother metaphor focuses too narrowly on the problems of surveillance, and that other

metaphor may fail to capture the full scope of the risk, which encompasses potentially harmful data practices on the part of private parties.

Private data collection facilitates government access to citizens' intellectual records because it is relatively easy for the government to obtain such information once it is in the hands of commercial entities. Private-sector entities can collect all sorts of information that the government—by virtue of the First Amendment, Fourth Amendment, and various statutory restrictions that apply only to state action—cannot.[153] Indeed, commercial data collection often results from consumers' voluntary disclosures in exchange for access to goods or services.

Yet individuals' Fourth Amendment protections evaporate when they give information to these third parties, meaning protections that would customarily apply to searches or seizures—such as a warrant requirement—do not apply to records in a third party's possession unless a statute imposes comparable protections.[154] The fact that the commercial entity may retain information indefinitely, rather than deleting it like a library customarily would, also makes it an attractive target for investigation.[155]

---

literary examples offer better illustrations of the other threats faced by information privacy).

[153] *See* Simmons, *supra* note 3, at 954.

[154] Under the Fourth Amendment's third-party doctrine, "[t]he rule is simple: By disclosing to a third party, the subject gives up all of his Fourth Amendment rights in the information revealed." Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 (2009). The doctrine is a lightning rod for criticism, as Justice Sotomayor's recent concurrence in *United States v. Jones* illustrates:

> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. . . . I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.

123 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

[155] *Compare* Section II.C, *supra* (describing libraries' deletion policies), *with* Section III.A, *supra* (describing Amazon's retention of customer records for marketing purposes).

CONFIDENTIALITY AND THE PROBLEM OF THIRD PARTIES

Protection is particularly thin where third parties are willing to volunteer user data to the government. There appears to be no legal barrier preventing parties like bookstores from voluntarily disclosing their records to the government or other third parties, except perhaps their privacy policies.[156] Moreover, many companies voluntarily sell customer information in exchange for substantial monetary remuneration.[157] Such companies often structure themselves so as to avoid statutory protections that might otherwise restrict the flow of data from private business to the federal government.[158] One example is the SRDC Direct Marketing List Source, which offers lists ranging form the "Gay America Megafile" to lists of Prozac users, online gamblers, and sex toy purchasers.[159] These lists contain "information about people's reading and buying habits, *including the books they buy*, *[and] the magazines they read*."[160] The secrecy of voluntary transactions between the private sector and the government also makes it difficult for citizens to assert any constitutional or statutory rights they might have,[161] and the mere suspicion that information providers are acting as government informants may itself impose a chilling effect.[162]

Further complicating matters, the Patriot Act offers two routes for federal investigators to request records of individuals' intellectual activities, both of which present transparency issues. As noted above, Section 215 allows the government to request tangible records including records of books circulated or sold, and Section 505 allows the government to request transaction records for electronic communications.[163] Both types of requests are typically accompanied by gag orders,[164] and this added level of secrecy makes it difficult to know what sort of requests have been made, and whether the recipients of the requests have asserted their users' rights to privacy.

---

[156] Richards, *Perils of Social Reading*, *supra* note 4, at 698.
[157] *See* Simmons, *supra* note 3, at 990-99 (describing data acquisition and analysis firms whose business model involves collecting personal data and then selling it to interested parties, including the U.S. government).
[158] *Id.* at 954-55 (explaining a data-laundering process whereby third parties, who are bound by statutory restrictions, transmit data to "fourth parties," who are free from these statutes and can pass information to the government).
[159] *Id.* at 991 n.151.
[160] *Id.* (emphasis added).
[161] *See* Solove, *supra* note 36, at 1098 (explaining that a customer may lack knowledge of a subpoena issued to a third party, let alone the opportunity to challenge it).
[162] *Cf.* FOERSTEL, *supra* note 24, at 44 (describing the potential chilling effect caused by "even the perception of library complicity in federal surveillance such as the Library Awareness Program").
[163] *Supra* notes 93-99 and accompanying text.
[164] *Id.*

To be clear, I would argue that the First Amendment *should* restrain the government's ability to pry into bookseller records, notwithstanding the apparent lack of protection under the Fourth Amendment's third-party doctrine.[165] This argument has carried the day in a handful of cases—including two involving Amazon—where bookstores resisted government requests for records.[166] In these cases, the courts held that a "heightened standard" applies to government subpoenas and warrants requesting book records.[167] Under this test, the government must establish both a "compelling interest" which could not be advanced by less restrictive means, and a "substantial relation" between the compelling interest and the information sought.[168] But the scope of First Amendment protections for intellectual records held by third parties remains ill-defined because it has not been tested in a federal appellate court,[169] or on non-book intellectual records such as search queries.[170]

Collection of reading habits also threatens to chill intellectual exploration through the possibility of inadvertent disclosure to private actors, which could lead to ridicule or other social sanctions.[171] A patron can browse hardcopy books in a library, or even read a book in the library without checking it out, without creating any record whatsoever. Even if the patron requires a librarian's assistance to find books on a particular topic, or

---

[165] My argument echoes Daniel Solove's proposal that the First Amendment be treated as a source of criminal procedure. *See* Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112 (2007).

[166] *See* Amazon.com LLC v. Lay, 758 F. Supp. 2d 1154 (W.D. Wash. 2010); In re Grand Jury Subpoena to Amazon.com, 246 F.R.D. 570 (W.D. Wis. 2007); In re Grand Jury Subpoena to Kramerbooks & Afterwords, Inc., 26 Med. L. Rptr. 1599 (D.D.C. 1998); Tattered Cover, Inc. v. City of Thornton, 44 P.3d 1044 (Colo. 2002).

[167] *See* sources cited *supra* note 166.

[168] *See* Amazon.com, 758 F. Supp. 2d at 1169.

[169] As Margot Kaminski notes, this is particularly true for digital reading records: "[T]here has not yet been a case where a litigant has successfully made this argument to protect digital reader records under the First Amendment." Kaminski, *supra* note 47, at 18.

[170] Google did successfully resist a subpoena from the Department of Justice for its search queries in 2006. *See* Gonzalez v. Google, 234 F.R.D. 674 (N.D. Cal. 2006). However, the matter was not decided on privacy or First Amendment grounds—the government had not asked for personally identifiable information—but rather because the government's request was unduly burdensome. *See id.*; Grimmelmann, *supra* note 32, at 43 n.193; Nicole Wong, *Judge Tells DoJ "No" on Search Queries*, GOOGLE OFFICIAL BLOG (Mar. 17, 2006), http://googleblog.blogspot.com/2006/03/judge-tells-doj-no-on-search-queries.html.

[171] Ironically, desire for interpersonal privacy fueled the adoption of e-readers. Many readers interested in romance novels, for example, turned to e-books because the format spares readers from having to publicly display the telltale cover of a "sexy romance novel" or facing a cashier at checkout. Katherine Rosman, *Books Women Read When No One Can See the Cover*, WALL ST. J., Mar. 14, 2012, at D1.

decides to borrow the book, the librarian is bound by professional obligations and sometimes law not to disclose this fact. Under this regime, a patron can learn about an embarrassing medical condition with minimal risk of alarming loved ones or insurance providers, seek advice on sensitive topics such as sexuality or body image, or explore controversial texts ranging from the political (like *The Anarchist Cookbook*[172]) to the gratuitous (like the erotic bestseller *Fifty Shades of Grey*[173]).

Amazon's practices of maintaining a detailed reading history and engaging in targeted marketing, by contrast, create a risk of inadvertent disclosure. The patron may now receive a series of emails telling him that his copy of *God Is Not Great: How Religion Poisons Everything* is about to expire, and inviting him to purchase it. Or his Amazon's home page may inform him, based on items from his recent viewing history (say, *Changing Bodies, Changing Lives*) that he should also consider reading *Sex: A Book for Teens*. As noted above, the patron may even see banner ads on third party websites, unexpectedly calling his interests to the screen during wholly unrelated web browsing.[174] These types of recurring notifications present risks of disclosure for anyone who checks email or browses the Internet in public using a mobile device, in an office environment, or on a shared computer.[175] The creation of email records also gives the government an additional opportunity to learn what someone is reading by way of monitoring the patron's email service.[176]

---

[172] This controversial book might be dismissed today as "The Disgruntled Idiot's Guide to Rebellion," but, however misguided it may have been in execution, it was originally written in protest of the Vietnam War and the draft. Katharine Mieszkowski, *Blowing up "*The Anarchist Cookbook,*"* SALON.COM (Sept. 18, 2000), http://www.salon.com/2000/09/18/anarchy/.

[173] Notwithstanding its scandalous subject matter—or quite possibly because of it—librarians reported in early 2012 that *Fifty Shades of Grey* was "the most popular book in circulation, with more holds than anyone [could] remember on a single title." Julie Bosman, *Libraries Debate Stocking 'Shades,'* N.Y. TIMES, May 22, 2012, at C1.

[174] *See supra* note 144 and accompanying text.

[175] Lest these concerns be dismissed lightly, it is worth remembering the history of unhappy spouses attempting to access their significant others' library records to determine whether they were cheating or contemplating divorce. *See supra* note 84 and accompanying text. Readers may genuinely be at risk of physical or emotional harm if spouses, family members, or other community members learn what they are reading. *See* Blitz, *supra* note 4, at 871.

[176] *See* Solove, *supra* note 36, at 1141-42 (explaining that the government can obtain emails stored with a service provider without having to meet the probable cause standard required for obtaining a warrant).

Recent disclosures regarding the National Security Agency's intelligence operations suggest that the federal government may also be collecting and retaining the contents of

The risks are worst for young people, who may be in a situation where family members monitor Internet use, where the family shares a Kindle and Amazon account, or where Amazon browsing simply takes place on a family computer. Setting aside the diverse opinions on whether parents should have the right to monitor or restrict their children's reading habits—itself a controversial topic[177]—library experts recognize that teenagers who lack confidence in the privacy of their library use shy away from controversial or potentially embarrassing materials.[178] A reticence to engage with controversial materials threatens not only to stunt a teenager at an intellectually formative stage, but also to cause immediate harm for teens who would otherwise consult library materials for advice on topics like safe sex, coming out as an LGBT person, or extricating themselves from an abusive situation—particularly if the abuse comes from the family itself.[179]

C. Library Confidentiality Obligations Do Not Cover Amazon

The act of checking out a library book is one of very few instances where private inquiry is protected by law, a protection bolstered by the library profession's norms and practices. The protections arise through an

---

emails sent between U.S. citizens at the time of transmission, rather than obtaining them after the fact. *See, e.g.*, Savage & Shane, *supra* note 9.

[177] Contrast the position articulated by ALA in interpreting the Library Bill of Rights, which "affirm[s] the responsibility and the right of all parents and guardians to guide their own children's use of the library and its resources and services," INTELLECTUAL FREEDOM MANUAL, *supra* note 60, at 153, with the position some school librarians have taken in refusing to disclose students' reading records to parents, *see* Helen R. Adams, *Privacy & Confidentiality: Now More Than Ever, Youngsters Need To Keep Their Library Use Under Wraps*, 33 AM. LIBRARIES, no. 10, 2002, at 44. Some states appear to have split the difference by permitting disclosures to parents only until a minor reaches age sixteen. *See, e.g.*, WIS. STAT. ANN. § 43.30(4) (West Supp. 2012).

[178] Adams, *supra* note 177.

[179] *See* Blitz, *supra* note 4, at 871 ("[W]aiting for information may have unbearably high costs for a teenager in other circumstances—where a minor is desperately depressed at being confined into his family or community's way of life. Or where he is unable to rely on the family itself to educate himself (and cope with) abuse or dysfunctional behavior that originates from the family itself.").

Prominent jurist Richard Posner has also articulated the importance of minors' access to information:

> Now that eighteen-year-olds have the right to vote, it is obvious that they must be allowed the freedom to form their political views on the basis of uncensored speech *before* they turn eighteen, so that their minds are not a blank when they first exercise the franchise. . . . People are unlikely to become well-functioning, independent-minded adults and responsible citizens if they are raised in an intellectual bubble.

Am. Amusement Mach. Ass'n v. Kendrick, 244 F.3d 572, 577 (7th Cir. 2001) (Posner, J.).

actor-defined regime, however, and the analogous act of borrowing a library *e-book* carries none of the same protections when a non-librarian actor delivers the service, leaving patrons' reading habits distinctly vulnerable.[180] Unfortunately, many library patrons likely harbor a false sense of privacy with respect to e-book activities by virtue of the simple fact that they expect privacy in library transactions.[181]

1. Library Privacy Laws Do Not Cover Non-Library Actors

Library privacy statutes are actor-defined: they regulate the conduct of libraries. By their text, the laws typically apply to "libraries" or "library circulation records" without defining the terms.[182] Booksellers like Amazon would likely fall outside this undefined term. States that define libraries more specifically typically limit their scope to libraries that are "established," "operated," or "funded" by the state.[183] Amazon was not established by any state, nor is it operated or funded by any state, and it would not fall under these statutes either.

To be clear, if libraries directly transmitted their patrons' information to a third party like Amazon, they would likely violate their confidentiality obligations. Perhaps in such a situation libraries' obligations would travel downstream with the disclosure to Amazon.[184] But the library is not making the disclosures. Rather, the patron himself is the one who tenders his login credentials to Amazon to complete the borrowing process, thereby linking the borrowed book to his existing customer profile.[185]

---

[180] *See* Charles Hamaker, *Ebooks on Fire: Controversies Surrounding Ebooks in Libraries*, SEARCHER, Dec. 2011, at 20, 23 ("That most basic of responsibilities of libraries, to protect patron-specific information on usage of library materials, might not survive in the ebook era.").

[181] *Cf.* Andrew A. Proia, Note, *A New Approach to Digital Reader Privacy: State Regulations and Their Protection of Digital Book Data*, 88 IND. L.J. 1593, 1605 (2013) ("What makes the possibility of exploiting a person's digital reading habits so concerning is in part related to the historical significance, and long history of legal protection, that physical books have enjoyed throughout our nation's history.").

[182] Kennedy, *supra* note 79, at 759-60.

[183] *Id.* at 759.

[184] *Cf.* Dirkes v. Borough of Runnemede, 936 F. Supp. 235, 240 (D.N.J. 1996) (holding, even though the Video Privacy Protection Act ("VPPA") on its face imposes confidentiality obligations only on "video tape service providers," that its protections nonetheless apply to individuals who have unlawfully obtained information from said service providers). For a proposal to use contract law to ensure such downstream obligations, *see* Hartzog, *supra* note 54.

[185] *See supra* notes 134-136 and accompanying text.

2. Non-Library Actors Do Not Share Libraries' Ethics and Norms

Librarians' ethical and normative commitments likewise apply only to librarians themselves. Unfortunately for reader privacy, many of the library confidentiality regime's strongest protections, such as its stance against retaining unnecessary circulation records, are rooted in these norms rather than any formal legal obligations.

The gulf between librarians' commitments and those of parties like Amazon is further widened because these non-library parties do not share the same rich history of protecting intellectual privacy. Examination of the video rental industry demonstrates this point. Citizens arguably have stronger statutory protections when renting a movie than when checking out a book: movie rental records are protected by a federal statute that restricts disclosures to the government and private parties alike,[186] whereas library records are protected by state laws that sometimes fail to impose any substantive requirements.[187] But citizens cannot rely on any normative commitment by the rental industry.[188] Instead, as targeted advertisement has become commercially significant, the rental industry has begun to stockpile and even disclose customer data notwithstanding its legal obligations. Blockbuster was sued in 2008 under the Video Privacy Protection Act of 1988 ("VPPA") after disclosing customers' recent rentals to Facebook as part of Facebook's controversial Beacon program.[189] The following year, Netflix publicly released over 100 million subscriber movie ratings, collected from approximately 480,000 different subscribers, as part of a contest designed to improve its movie recommendation system.[190] Even

---

[186] The Video Privacy Protection Act ("VPPA") permits disclosure of personally identifiable records to law enforcement only subject to a warrant, a grand jury subpoena, or a court order, 18 U.S.C. § 2710(b)(2)(C) (2006), and it provides consumers with a cause of action against a video tape service provider who wrongfully discloses rental records to any other party, government or not, *id.* § 2710(b)-(c).

[187] *See supra* Section II.B (describing gaps in state library statutes, including some states' legislative decisions to leave privacy to librarians' discretion).

[188] Richards, *Intellectual Privacy*, *supra* note 4 at 430 (arguing norms explain "why we trust the discretion of our librarians more than our video store clerks, even though statutes impose strong duties of confidentiality on both of them").

[189] Harris v. Blockbuster, ELECTRONIC PRIVACY INFORMATION CENTER, http://epic.org/amicus/blockbuster/ (last visited Dec. 22, 2013).

[190] Natalie Newman, *Netflix Sued for "Largest Voluntary Privacy Breach to Date,"* PROSKAUER PRIVACY L. BLOG (Dec. 28, 2009), http://privacylaw.proskauer.com/2009/12/articles/invasion-of-privacy/netflix-sued-for-largest-voluntary-privacy-breach-to-date/.

though Netflix attempted to anonymize the data, researchers proved quite capable of re-linking the records to specific individuals.[191]

Moreover, it is not just that the rental industry lacks a normative commitment to its customers' confidentiality—the industry has financial interests that are adverse to it.[192] Like other information-age industries, it stands to make a profit from analyzing user data or sharing it with business partners. It is thus no surprise that the video rental industry lobbied for exceptions to make disclosure easier under the VPPA. As of a 2012 VPPA amendment, companies may now obtain blanket consent for future disclosures of a customer's rental history, where they previously had to obtain consent on a case-by-case basis.[193]

3. Library Policies and Practices Cannot Protect Data Collected by Non-Library Actors

Librarians' policies and practical mechanisms for protecting privacy are ineffective as to data collected by third parties. Deletion of circulation records upon return of an item only works when the library itself holds the circulation records. Likewise, an authentication system allowing patrons to utilize third-party databases without using personal IP addresses or having to disclose personally identifiable information does not work when the third party in question requires users to disclose personally identifiable information to complete the transaction, as Amazon does.

Some libraries have adopted the practice of notifying their patrons that they are outside the aegis of the library's confidentiality policies when they check out a Kindle e-book. For example, the Wisconsin Public Library Consortium posted a firmly worded notice on its own webpage to warn its patrons before they click through to Overdrive, and it succeeded in convincing Overdrive to feature a version of the notice on the website Overdrive itself displays to users within the consortium.[194] While this practice does not change what Amazon does with the data—perhaps it even accelerates self-censorship by patrons who would rather not be monitored—

---

[191] *Id.*

[192] *See* Kaminski, *supra* note 47, at 19 ("Companies have realized . . . that VPPA is a hurdle to their business models.").

[193] *Compare* Video Privacy Protection Act of 1988, Pub. L. No. 100-618, 102 Stat. 3195, Sec. 2(b)(2)(B), *with* Video Privacy Protection Act Amendments Act of 2012, Pub. L. No. 112-258, 126 Stat. 2414, Sec. 2. The VPPA, as amended, is codified at 18 U.S.C. § 2710.

[194] Michael Kelley, *Overdrive, Amazon Privacy Disclaimer Pops Up in Wisconsin; in Virginia, Questions About Catalog Disparities*, THE DIGITAL SHIFT (Dec. 9, 2011), http://www.thedigitalshift.com/2011/12/ebooks/overdrive-amazon-privacy-disclaimer-pops-up-in-wisconsin-in-virginia-questions-about-catalog-disparities/.

it reduces the likelihood that a patron will tender his reading interests to Amazon without realizing it. Notwithstanding the pains libraries have taken to protect patrons against government monitoring, however, many major library systems have not adopted practices like this that would alert users to commercial monitoring.[195]

D. Libraries Cannot Provide Kindle Books Except Through Amazon

One might ask why libraries do not simply opt out of dealing with Amazon to avoid exposing patrons to these privacy risks. The difficulty is that libraries struggle to remain relevant, and doing so requires supplying the burgeoning demand for e-books.[196] Amazon's Kindle commands the largest share of the e-reader market, and Amazon exercises considerable legal, technical, and economic leverage to control the terms on which libraries and users may load content onto the Kindle platform.[197]

1. Libraries Lack Bargaining Power in E-Book Licensing

Libraries had no opportunity to negotiate terms with Amazon. Literally. Amazon began offering Kindle e-books through Overdrive, a service to which libraries had previously subscribed to offer e-book lending for other devices, without disclosing or pre-clearing the details of how the borrowing would work. Because the pre-existing model for downloading e-books to non-Kindle devices did not require the reader to disclose any

[195] Neither the Los Angeles Public Library—a large library system with over 17 million visitors, 18 million items circulated, and 142 million website hits in the 2008-2009 fiscal year, *see Los Angeles Public Library Annual Report 2008-2009*, LIBRARY FOUNDATION OF LOS ANGELES (2009), http://www.lfla.org/annual-report/index.php—nor Yale University's library provided a similar notice when I personally completed the Overdrive check-out process. Todd Gilman, a Yale librarian, has commented that patrons with privacy concerns "shouldn't read on devices that require them to log in to third-party vendor Web sites like Amazon," reasoning that there is no problem with the Amazon borrowing arrangement because Kindle owners chose to enter a relationship with Amazon when they acquired a Kindle. *See* Parry, *supra* note 137.

[196] *See* DAVID R. O'BRIEN, URS GASSER & JOHN PALFREY, E-BOOKS IN LIBRARIES: A BRIEFING DOCUMENT DEVELOPED IN PREPARATION FOR A WORKSHOP ON E-LENDING IN LIBRARIES, 23-24 (2012), *available at* http://cyber.law.harvard.edu/publications/2012/ebooks_in_libraries (describing patron demand for e-books); David Sarno, *Libraries Reinvent Themselves as They Struggle To Remain Relevant in the Digital Age*, L.A. TIMES (Nov. 12, 2010), http://articles.latimes.com/2010/nov/12/business/la-fi-libraries-20101112.

[197] *See infra* Section III.D.2.

information to a third party,[198] Overdrive's handling of Kindle e-books came as a surprise.[199]

This lack of opportunity to negotiate is an unusual example because it lacks even the pretense of giving libraries any say in how borrowing for the Kindle would work. It is nonetheless emblematic of the power dynamics at play when libraries seek access to digital materials like e-books. Foremost among libraries' disadvantages is the loss of the first sale doctrine for materials that are licensed (like e-books) rather than purchased (like hardcopy books).[200]

The first sale doctrine permits the lawful owner of a copy of a copyrighted work to dispose of the work as he sees fit, for example by lending or reselling.[201] The doctrine allows libraries to avoid price discrimination: even if publishers offered a higher priced "library edition,"

---

[198] *See supra* notes 131-133 and accompanying text.

[199] While libraries might have subsequently negotiated for different terms, Amazon has considerable power to dictate the terms on which books may be offered for the Kindle owing to its control over the platform. *See infra* Section III.D.2.

[200] *See* O'BRIEN ET AL., *supra* note 196, at 10 ("[M]ost publishers . . . only license, but do not sell, e-books to libraries."). For a description of how the licensing model deprives libraries and other readers of rights they would have held as e-book owners, see generally Matthew Chiarizio, Note, *An American Tragedy: E-Books, Licenses, and the End of Public Lending Libraries?*, 66 VAND. L. REV. 615 (2013); Rachel Ann Geist, *A "License To Read": The Effect of E-Books on Publishers, Libraries, and the First-Sale Doctrine*, 52 IDEA 63 (2012); Michael Seringhaus, *E-Book Transactions: Amazon "Kindles" the Copy Ownership Debate*, 12 YALE J.L. & TECH. 147 (2009).

Many scholars question the validity of copyright holders' attempts to evade the first sale doctrine by casting certain transactions as licensures rather than sales. *See, e.g.*, 2 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 8.12(B)(1)(d)(i)(III) (2013) (questioning the licensure classification where the user acquires a physical copy of the work); Brian W. Carver, *Why License Agreements Do Not Control Copy Ownership: First Sales and Essential Copies*, 25 BERKELEY TECH. L.J. 1887, 1954 (2010) ("The invented notion of 'licensing' software, where that means transferring perpetual possession of a copy but retaining title to the copy, is both incoherent and not found in the Copyright Act."); Seringhaus, *supra*, at 198-203 (arguing e-book transactions should be understood as sales rather than licensures because of the cultural importance of books, policy concern relating to copyright exhaustion, problems of information costs, distinctions between e-books and software, the destruction of secondary markets, and commercial practices that lead consumers to believe they own their e-books); *see also* 2 NIMMER & NIMMER, *supra*, § 8.12(E) (exploring the application of first sale rights to digitally downloaded copies). These points go beyond the scope of this Article, however; I use the discussion of licensure and loss of first sale rights here to illustrate the power dynamics at play between libraries and publishers, two camps who accept the restrictions allegedly imposed by the licensing model at the present time.

[201] 17 U.S.C. § 109 (2012); 2 NIMMER & NIMMER, *supra* note 200, § 8.12(B); *see id.* § 8.12(B)(1)(a) ("[A] library that owns a legitimate copy of a work may lend it to patrons without infringing the copyright owner's distribution right.").

the library could always purchase and lend the consumer edition or even a used copy. Libraries may lend a hardcopy book until it literally falls apart—and even then a library may re-bind the book[202]—making the per-use cost for a popular book quite the bargain. Thanks to the first sale doctrine, libraries may also liquidate old books through fundraising sales, helping libraries purchase new materials. All the while, of course, librarians' professional norms and state privacy laws protect the intellectual privacy of patrons reading the books.

The same factors do not hold true for e-books when they are distributed via licensure rather than sale.[203] Without the benefit of the first sale doctrine, publishers can charge one price for the license to a "consumer edition," which prohibits lending, and a higher price for a "library edition."[204] Accordingly, "publishers can, and do, charge libraries more than the average consumers."[205] Even though libraries pay more for e-books than hardcopy books, the publishers typically simulate the limits of hardcopy books by limiting circulations to one patron at a time per license.[206] Moreover, the e-books may be subject to an obsolescence scheme such as a limit on the number of times a book may be circulated,[207] or a requirement that the library pay an ongoing subscription fee to a particular circulation service or else lose access to all the titles it has licensed, notwithstanding the fact it may have already paid for the individual titles.[208]

All that is to say: On top of a what seems like a bad economic deal—higher prices and greater restrictions on e-books as compared to hardcopy books—librarians also compromise their patrons' intellectual privacy by endorsing arrangements like the one with Amazon. These poor results reflect libraries' lack of bargaining power.

---

[202] 2 NIMMER & NIMMER, *supra* note 200, § 8.12(C).
[203] *See* sources cited *supra* note 200.
[204] Geist, *supra* note 200, at 92-93.
[205] *Id.* at 93; *see* Jill Vejnoska, *Grasping the E-Book Era*, ATL. J. CONST. (Apr. 1, 2012), http://www.ajc.com/news/lifestyles/grasping-the-e-book-era/nQSgk/ ("Random House recently raised the purchase price for e-books to library wholesalers by as much as 300 percent—generally charging anywhere from $65 to $85 for a new hardcover title.").
[206] *See* O'BRIEN ET AL., *supra* note 196, at 14.
[207] For example, HarperCollins requires libraries to renew licenses for e-books after they have been checked out 26 times. *Id.* at 8. Other major publishers, including Macmillan and Simon & Schuster, simply refuse to license e-books for library use. *Id.* at 9.
[208] *See id.* at 15, 17 (describing "platform maintenance fees" and subscription fees); Geist, *supra* note 200, at 93.

2. Amazon Locks Libraries and Readers into Its Products and Services Using Legal, Technical, and Economic Leverage

To the extent Amazon's business practices with respect to Kindle e-book borrowing are more invasive than libraries or their patrons would prefer, it might seem libraries could turn to competing e-book vendors. While there is an intuitive appeal to letting the market regulate e-book privacy practices,[209] a market solution assumes that libraries and their patrons are free to move away from Amazon as book supplier, or the Kindle as e-reader. In practice, they are not.

Libraries have little choice but to offer e-books for the Kindle. The move toward offering e-book services is a step libraries have taken in order to remain relevant.[210] Because Amazon is the biggest player in the e-book market—over 70% of e-book purchases in 2010-2011 were from Amazon, an increase of 60% over the prior year[211]—this move requires offering books for the Kindle.

And Amazon has designed the Kindle so that any library wishing to offer e-books for the Kindle must deal directly with Amazon. Amazon does this by limiting the Kindle's functionality to certain file formats. Specifically, Amazon has designed the Kindle so that publishers can utilize digital rights management ("DRM") technology only for books formatted in Amazon's proprietary file formats.[212] The Kindle can read books in other, non-proprietary formats, but it does not support DRM protection for them.[213]

DRM compatibility matters because publishers insist on DRM protection for books offered through libraries.[214] DRM technology gives the publisher the technical means to control the use of an e-book, for example,

---

[209] This premise relies on the assumption that market forces are equipped to select for an optimal privacy regime, an assumption scholars have called into doubt. *See, e.g.*, Julie E. Cohen, *Irrational Privacy?*, 10 J. TELECOMM. & HIGH TECH. L. 241, 243 (2012) ("[D]ysfunction in privacy markets has a dynamic aspect. Over time, people can be expected to (over)disclose more and more information, both because they have become inured to disclosure and because the equilibrium in the marketplace has tipped toward disclosure as a condition of market entry . . . ."); Paul Ohm, *Branding Privacy*, 97 MINN. L. REV. 907, 952 (2013) ("Privacy seems to be a market for lemons where promises are easy to make and quality is difficult to inspect. As with all such markets, there seems to be little incentive to compete for privacy.") (footnote omitted).

[210] *See* sources cited *supra* note 196.

[211] RÜDIGER WISCHENBART, CARLO CARRENHO & VERONIKA LICHER, THE GLOBAL EBOOK MARKET: CURRENT CONDITIONS & FUTURE PROJECTIONS 9 (revised Oct. 2012).

[212] *See E-Reader Privacy Chart, 2012 Edition*, *supra* note 145.

[213] *Id.*

[214] O'BRIEN ET AL., *supra* note 196, at 26.

by deleting an e-book when the lending period is over.[215] These mechanisms address publishers' concern about potential piracy of their works given users' ability to download books for free from the library. Even though libraries or individual users might technically be able to circumvent these measures,[216] such circumvention could give rise to civil or criminal liability under the Digital Millennium Copyright Act ("DMCA").[217] Because publishers insist on DRM, and DRM files for Kindle are available only using the proprietary format available from Amazon, libraries cannot utilize an alternate supplier for Kindle e-books.

Given that Amazon has a lock over the Kindle device and its file formats, one might suggest that patrons themselves switch to a different e-reader. This too is a difficult proposition, because the Kindle is by design a "sticky" platform. As noted above, Amazon sells most Kindle books in a proprietary format. E-books in this format cannot be read on a competitor's device.[218] Again, while it is technically feasible to convert these files into a format readable on other devices,[219] the act of conversion would require circumventing DRM protections and subject the reader to possible criminal and civil penalties under the DMCA.[220] Accordingly, any user who contemplated a switch from the Kindle to another device would risk losing all e-books they had ever purchased for the Kindle, because they simply would not be compatible with a competing device such as Barnes & Noble's nook.[221]

---

[215] *Id.* at 10.

[216] Matthew Friedman, Comment, *Nine Years and Still Waiting: While Congress Continues to Hold Off on Amending Copyright Law for the Digital Age, Commercial Industry Has Largely Moved on*, 17 VILL. SPORTS & ENT. L.J. 637, 672 (2010).

[217] *See* 17 U.S.C. §§ 1201-1205 (2012).

[218] Friedman, *supra* note 216, at 669 n.173; *see E-Reader Privacy Chart, 2012 Edition*, *supra* note 145 (stating that Amazon's proprietary AZW format cannot be read on the Barnes & Noble nook, Kobo, or Sony Reader).

It is possible that developments in technology and distribution models will mitigate the compatibility problem. Amazon now permits some devices, like the iPad and Android phones, to run apps that support Kindle e-books, and these devices also feature apps that support e-books in other formats. *See generally* John P. Falcone, *Kindle vs. Nook vs. iPad: Which E-Book Reader Should You Buy?*, CNET, http://news.cnet.com/8301-17938_105-20009738-1/kindle-vs-nook-vs-ipad-which-e-book-reader-should-you-buy/ (last updated Dec. 17, 2012) (surveying the e-reader apps available for various devices).

[219] Friedman, *supra* note 216, at 672.

[220] *See* 17 U.S.C. §§ 1201-1205.

[221] Cory Doctorow, *A Whip To Beat Us With*, PUBLISHERSWEEKLY.COM (Mar. 30, 2012), http://www.publishersweekly.com/pw/by-topic/columns-and-blogs/cory-doctorow/article/51292-cory-doctorow-a-whip-to-beat-us-with.html ("If [customers'] e-books have no DRM, they can simply switch. But if they are DRM-locked, switching platforms could mean abandoning their e-books."). To contrast this situation with that of

* * *

Granted, readers today can avoid the problems highlighted above by visiting a library to seek a hardcopy book. Doing so may entail a loss in time and convenience relative to downloading an e-book, but the reader nonetheless has the option to engage in a private intellectual pursuit. This answer, however, is contingent on an information ecology where hardcopy books are relatively plentiful. The situation a decade from now could easily be quite different. If publishers perceived an economic (or legal) advantage in licensing e-books as opposed to selling hardcopy books, they might capitalize on it by moving towards exclusive e-book production. The ability to collect detailed reading habits and use them for marketing purposes in one format, but not the other, could provide one such reason.[222] The next Part examines updated approaches to confidentiality designed to meet the needs of the networked information ecology.

IV. THE CONTENT-DEFINED APPROACH TO CONFIDENTIALITY

The library confidentiality regime fails to account for third parties like Amazon because it is an actor-defined approach to confidentiality. It assumes an information economy where the only transactions that implicate library records are two-party transactions between a library and its patron. This was a valid assumption before the advent of networked distribution models, meaning a system directed at regulating libraries' conduct worked for the better part of the twentieth century. Simple two-party transactions are increasingly rare today, however. Libraries now facilitate access to content via third parties like Amazon. In e-commerce beyond the library, third parties play roles ranging from content provider, to advertising partner, to eavesdropper.[223] Third parties like these now threaten to take advantage of loopholes inherent to actor-defined confidentiality regimes because they fall outside the regulated class of actors.

The solution to this problem is a content-defined approach. It requires defining confidentiality obligations so they trigger upon the collection or use of a particular type of information that society intends to protect. The remainder of this Part articulates this approach in greater detail and explains why it is superior to alternatives such as an institution-defined

---

hardcopy books, it would be unheard of to think you might lose every hardcopy book you ever ordered from Amazon simply because you stopped shopping at Amazon and became a Barnes & Noble customer.

[222] *Cf.* Geist, *supra* note 200, at 84 (arguing software designers and publishers are moving towards *licensing* digital media, rather than *selling* copies, because doing so allows them to deprive customers of the rights they would otherwise have under the first sale doctrine).

[223] *See supra* notes 50-54 and accompanying text.

approach or the mere expansion of the actor-defined approach to additional actors.

A. Building a Content-Defined Regime

It would be possible to avoid the slippery issue of defining exactly who was within a proposed confidentiality regime by instead focusing on the type of information we intend to protect. The concerns animating the library confidentiality regime, for example, are those of reader privacy. A content-defined regime would identify the types of reading records that merit protection, and then impose duties of confidentiality on all entities who held such records.

Setting a workable definition of reader records is not without its challenges, but Neil Richards provides a helpful starting point. He argues the "key should be whether the records reveal the operation of our minds in thinking, reading, or otherwise trying to make sense of the world privately."[224] These records would certainly include an individual's book-reading or film-watching habits, which society has previously attempted to protect through various library privacy statutes, reader privacy laws, and the Video Privacy Protection Act ("VPPA").[225] They would likely also include Internet search histories given the detailed picture they paint of users' inquiries and reading choices,[226] despite the fact that existing laws have not recognized the same kind of privacy interest in these materials. But this definition would not cover other types of e-commerce, such as purchasing office supplies. Nor would it include all media; one might protect audiobooks and podcasts because they implicate the same type of content as textual materials, but not music.[227]

California's Reader Privacy Act of 2011[228] is a partial instantiation of this approach. The Act currently restricts the disclosure of any records linking an individual with "the rental, purchase, borrowing, browsing, or viewing" of particular books by any "book service," defined as a commercial entity that makes more than 2% of its revenues from selling or renting books.[229] The scope of the regulation is defined primarily with reference to the regulated record type: personally identifiable reading

[224] Richards, *Perils of Social Reading*, *supra* note 4, at 720.
[225] *Id.*
[226] *Id.*
[227] *See id.* While e-commerce that does not implicate reader privacy may raise other privacy concerns, those considerations fall outside the discussion of a reader privacy regime.
[228] CAL. CIV. CODE §§ 1798.90-1798.90.05 (West Supp. 2013).
[229] *Id.*

records. It is defined only in small part by reference to the covered actors, setting a low monetary threshold for an entity to be considered a book service.

The revenue requirement nonetheless risks creating the loopholes inherent to an actor-defined regime. It is possible to imagine entities who would process book transactions—thereby gaining the ability to collect reading records—without being covered under the California law. Perhaps a company would loan books for free, but make money from aggregating and selling its readers' preferences. Or perhaps a third party would wirelessly deliver books that people purchased. In doing so, it might learn users' reading habits without qualifying as a book service so long as it received no cut of the sales revenues. A broader statute could eliminate these lingering problems by regulating disclosure of individuals' reading history by any commercial entity. Full stop. The statute need not limit itself to particular types of businesses.

B. The Institution-Defined Alternative

An alternative way to address the problem of third parties would be an institution-defined approach. Such an approach would identify certain institutions where confidentiality is important and impose obligations on all actors who collected records in that context, thereby vindicating the contextual integrity of privacy norms within these institutions.[230] An institution-defined approach to library confidentiality would mean imposing the obligations currently expected of librarians on third parties like Amazon who provide library services or otherwise become involved in library transactions.

While the institution-defined approach is an improvement over the actor-defined approach, it nonetheless lags behind a content-defined approach in protecting information in new contexts. A regime protecting all library transactions might solve the intra-library problem of third parties, but it would not constrain extra-library actors like booksellers or the Google Books project. Policymakers would have to make the express decision to protect reading in these new institutional contexts even though the same fundamental privacy interests were at stake.

Notwithstanding this concern, the institution-defined approach has appeal because it can be partially realized through private contracting. Libraries have expressly invited third parties like Amazon to participate in library transactions, thereby giving these parties the opportunity to collect

[230] *See* Nissenbaum, *supra* note 49, at 138 (arguing "the benchmark of privacy is contextual integrity").

reader records directly from patrons. As a condition of such access, libraries could insist that these third parties protect patrons' reading records under a set of obligations that conformed to librarians' own.[231]

Amazon's own Privacy Notice provides a starting point for structuring this contractual approach. Right now it states that any information Amazon shares with a particular class of third-party subsidiaries will be governed by privacy policies at least as protective as Amazon's own.[232] It is silent as to information the customer might directly share with the subsidiaries in the course of the transaction. The contract could be re-configured to state that any information the subsidiaries obtained regarding users' reading habits over the course of a book-purchase transaction, whether from Amazon, the customer, or another third party involved in the transaction, would be governed by privacy policies at least as protective as Amazon's own. The difference is subtle, but the transaction-based approach would establish confidentiality in these settings as a comprehensive regime that followed the user through the transaction.

An important limitation of the contractual approach is that it does little to regulate the conduct of uninvited third parties, due to lack of privity. If a patron borrows e-books using his home Internet connection, for example, an Internet service provider might obtain a full transcript of any e-books borrowed or downloaded, yet have no relationship to a library or bookseller.[233] The same could be said of a sophisticated third-party cookie designed to track the recipient's browsing activities.[234] Or a company (call it "Big Brother") might design an e-reader designed to monitor all e-books downloaded to its device, yet Big Brother could avoid contracting with the libraries or retailers from whom the user might acquire the e-books.[235] The

---

[231] Woodrow Hartzog also proposes a contractual model of confidentiality, which he calls "chain-link confidentiality." Hartzog, *supra* note 54. Under his approach, the user's initial disclosure of personal information would be accompanied by a confidentiality agreement that permitted subsequent disclosure to third parties so long as those disclosures were accompanied by a similar agreement; in that way confidentiality would continue in a viral fashion down the chain of disclosures. *Id.* at 659. The key difference in my approach is that it is not concerned with binding downstream recipients, but rather with binding parties involved in the initial transaction, *i.e.*, the intra-institutional third parties described in Section I.C.3, *supra*.

[232] *Privacy Notice*, *supra* note 130 ("We share customer information only as described below and with subsidiaries Amazon.com, Inc. controls that *either are subject to this Privacy Notice or follow practices at least as protective as those described in this Privacy Notice*.") (emphasis added).

[233] *See supra* note 53 and accompanying text.

[234] *See supra* note 54 and accompanying text.

[235] This feature is not science fiction: EFF's *E-Reader Privacy Chart, 2012 Edition*, *supra* note 145, indicates that the Barnes & Noble nook can track "sideloaded content."

proposed approach would not cover these situations notwithstanding a library or retailer's efforts to draft effective confidentiality agreements.

Another limit is that the contractual approach assumes pro-privacy actors have sufficient negotiating power to obtain these terms. The library example suggests this will not always be so.[236] Yet many powerful information providers recognize the social and business value to protecting users' privacy. Even taking a cynical view, information companies want to maintain control of user data, and contractual arrangements like these are one way to maintain control.[237]

C. The Limits of Adding New Actors to an Actor-Defined Regime

An actor-defined approach could work, in theory. There would be no uncovered third parties—extra-institutional or intra-institutional—if the framers of a confidentiality regime could perfectly identify all the actors who would come into contact with the content being protected.

But perfect identification is unattainable in practice. A rough sense of the actors involved may have been sufficient in a pre-networked world where it was relatively clear what sorts of actors traded in what sorts of information. The dynamics at play in e-commerce, however, make it difficult to identify the relevant actors in advance: putative two-party transactions are often multi-party transactions, many of the parties involved are obscured because they operate in the background, and the particular parties may change overnight because new business models come and go rapidly in digital commerce.

Moreover, even if the relevant parties are known, there must be political will for policymakers to act. Such will seems lacking: while prior scholarship points out numerous loopholes whereby sensitive data goes unprotected in the hands of uncovered parties under existing federal law, there are few signs that policymakers are working to close these loopholes.[238]

---

[236] *See supra* Section III.D.

[237] *Cf.* Picker, *supra* note 7, at 11 ("Google would almost certainly prefer not to disclose [its users'] information, since disclosing the information gives up the control that Google has from its exclusive access to the information."). *But see* Richards, *Perils of Social Reading*, *supra* note 4, at 701 ("Corporate self-interest is also a minimal and often fickle constraint on disclosure of personal information.").

[238] *See* Asay, *supra* note 3, at 325-327 (identifying loopholes due to the "sectoral approach" in several extant federal privacy laws); Simmons, *supra* note 3, at 976-978 (identifying loopholes in the Right to Financial Privacy Act and the Electronic Communications Privacy Act whereby the government can obtain records ostensibly protected by these acts so long as a party covered by one of these acts first discloses the records to a non-covered "fourth party").

A content-defined approach avoids these identification and response problems by allowing society to commit itself in advance to protecting a certain kind of information. As an alternative, an institution-defined approach allows society to commit to protecting information within trusted institutions. Both these approaches offer flexibility and comprehensiveness that are lacking from actor-defined approaches.

* * *

A content-defined approach to confidentiality allows society to make good on its commitment to protecting particular types of sensitive information. It protects such information within existing, trusted institutions, and it also reaches to new contexts where the same type of information is at issue. But such an approach does not necessarily answer the question of *how* the information should be protected, which may change according to context. The next Part explores this challenge.

V. TAILORING CONFIDENTIALITY TO CONTEXT: READER PRIVACY OUTSIDE THE STACKS

Context matters. The effectiveness of a confidentiality regime depends on the norms and incentives of the parties regulated. Accordingly, while a content-based approach may identify all the parties and contexts to which confidentiality should apply, it may not shed light on how these parties and contexts should be regulated.

This Part illustrates this point by showing what would happen if the extant library confidentiality regime were extended to non-library actors. Successful confidentiality regimes often rely on longstanding ethical or professional commitments,[239] and in many cases these commitments pre-date any formal legal recognition.[240] The library regime is no exception.[241]

---

[239] The physician-patient relationship, a paradigmatic example of a strong confidentiality regime, is supported by an ancient code. The Hippocratic Oath states: "Whatever I may see or hear in the course of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself holding such things shameful to be spoken about." LUDWIG EDELSTEIN, THE HIPPOCRATIC OATH 3 (1943). Moreover, the Supreme Court recognizes that the attorney-client privilege, another paradigmatic example, "is the oldest of the privileges for confidential communications known to the common law." Upjohn Co. v. United States, 449 U.S. 383, 389 (1981).

Societal recognition of communications as confidential also plays an important role. *See* Richards & Solove, *supra* note 3, at 140-42 (contrasting early fears about the confidentiality of the U.S. postal service with the security that ensued after American society came to regard mail as "sacred").

[240] Journalism provides an example. Federal courts have refused to recognize a First Amendment or federal common law privilege protecting reporters from compulsion to disclose confidential sources to a grand jury. *See* United States v. Sterling, 724 F.3d 482,

Libraries' protection of reading records is effective because librarians as a profession are committed to reader privacy and lack incentives to exploit user data; the protections they afford go beyond what the law requires. Protecting reader privacy among non-library actors therefore demands a set of interventions better tailored to their norms and motives.[242] By examining what these interventions might look like, this approach builds on prior scholarship calling for the translation of librarians' normative commitments into obligations that protect reader privacy in other contexts.[243]

A. Establishing a Non-Disclosure Baseline

The obligation not to disclose protected records is the minimum requirement of a functioning confidentiality regime. This obligation is a formal requirement of many library privacy laws, though not all of them,[244] and librarians' norms and policies supply the obligation where the laws are lacking.[245]

Interestingly, this baseline obligation is often compatible with information-age companies' business interests. User information is the lifeblood of such companies, and they do not want to surrender or even sell

---

492, 499 (4th Cir. 2013); In re Grand Jury Subpoena, Judith Miller, 438 F.3d 1141, 1147, 1149-50 (D.C. Cir. 2005); *see also* Branzburg v. Hayes, 408 U.S. 665, 667 (1972) (finding no such protection under the First Amendment). Reporters nonetheless go to great lengths to protect their sources, often choosing to be jailed for contempt while they challenge the legitimacy of being compelled to testify. *See* Elizabeth Coenia Sims, *Reporters and Their Confidential Sources: How* Judith Miller *Represents the Continuing Disconnect Between the Courts and the Press*, 5 FIRST AMEND. L. REV. 433, 447 (2007).

[241] To be sure, librarians were sometimes forced to compromise their commitment to intellectual freedom before state laws recognized that libraries should be protected from open-records requests and certain law-enforcement requests. Yet librarians' ethical commitments pre-dated the enactment of these laws and librarians sometimes acted in defiance of the law when they thought patron privacy was unduly compromised. *See* Section II.A, *supra*. Even today librarians institute arguably aggressive policies to delete patron records with an eye towards protecting patron privacy against records requests that, despite being objectionable to librarians, might be deemed legal. *See supra* notes 120-122 and accompanying text.

[242] *See supra* Section III.C.2 (explaining how these normative commitments compel libraries to protect information in ways commercial entities do not).

[243] *See* Klinefelter, *supra* note 38, at 561 (calling for reader protections that achieve "the same combined effect" as existing library practices, normative commitments, and statutes); Richards, *Intellectual Privacy*, *supra* note 4 at 437 ("Intellectual-privacy values can be encoded through law and social norms to affect the incentive structures of businesses holding intellectual records.").

[244] *See supra* notes 109-114 and accompanying text.

[245] *See generally* Sections II.A & II.C, *supra*.

this information to potential competitors.[246] This concern has led companies to structure the sharing of data in ways that protect against actual disclosure of user data. For example, when these companies share data with their advertising partners, they often conceal customer information within a "black box."[247] What this means is that a company like Amazon or Google passes a partner's advertisements to consumers who match a certain profile without telling the partner any personal details about those consumers (although the partner is likely to learn certain details if the consumer actually clicks through the ad and becomes a customer).[248] This practice strikes a compromise between commercializing a user's data and preventing it from leaking downstream to additional parties.

The goodwill associated with protecting privacy is also important to many companies. Altruistic motives aside, customers typically prefer privacy, meaning a company's privacy commitments may help it compete for business.[249] Privacy commitments directed against government monitoring may be particularly appealing for such companies. Because most companies are unlikely to profit by being overly cooperative with law enforcement requests for records, a commitment to insist on proper process prior to disclosure would actually serve the company's business interests by attracting customers. It would simultaneously provide an important safeguard against government overreaching. Further interventions building on this motive might remove barriers that currently insulate companies from accountability to their customers, i.e., by curtailing gag orders or similar

[246] *See* Picker, *supra* note 7, at 11.
[247] *Id.*
[248] *See id.*; *Interest-Based Ads*, *supra* note 144 ("We do not provide any personal information to advertisers or to third party sites that display our interest-based ads. However, advertisers and other third-parties (including the ad networks, ad-serving companies, and other service providers they may use) may assume that users who interact with or click on a personalized ad or content are part of the group that the ad or content is directed towards (for example, users in the Pacific Northwest who bought or browsed for classical music).").
[249] Some experts predict that U.S. tech companies will lose billions of dollars in revenues due to the loss of privacy-sensitive customers in the wake of disclosures regarding NSA surveillance, especially foreign customers who find little comfort in the NSA's assurances that their programs are directed only towards non-Americans. *See* James Temple, *NSA Effort Could Cost Tech Firms*, S.F. CHRON., Aug. 9, 2013, at C1. Reactions like this are not a new phenomenon: public outrage and a drop in sales also followed the (allegedly inaccurate) report that Kramerbooks agreed to disclose Monica Lewinsky's book-buying records to Ken Starr during his investigation of President Clinton in 1997. *See* Schaufenbuel, *supra* note 38, at 189.

mechanisms that require companies to cooperate with intelligence or law enforcement operations without notifying their customers.[250]

This analysis is not true, of course, for all entities. Jon D. Michaels has identified companies who cooperate with government investigations in exchange for preferential treatment.[251] And this is to say nothing of companies that aggregate consumer data for sale to the government or other private parties.[252] To account for these entities, an extra-library regime would need to formally prohibit disclosures of reading records; it could not leave this obligation to the regulated entities' discretion.

B. Protecting Users from Abuse of Notice and Consent

The library regime allows librarians to disclose a patron's records subject to the patron's consent.[253] Common sense requires this sort of allowance so that patrons can release their own records. Librarians could theoretically abuse this feature by conditioning the use of library materials on patrons' blanket permission to disclose their circulation records, but they do not because—library ethics aside—there is no motive for them to do so. Unlike commercial entities, libraries generally do not attempt to monetize user data.

If this feature of the library regime were applied to other information providers, however, it could easily swallow the baseline obligation of non-disclosure. Providers like Amazon have numerous financial incentives to exploit customer information. To ensure their ability to do so, these companies already condition use of their materials on customers' agreement to terms of use permitting various disclosures of the data.[254] While such consent may be voluntary in a strictly legal sense—setting aside the doubts raised when such terms are buried in fine print or obscured by dense legal verbiage[255]—it is not voluntary in a practical sense when the user lacks alternative means to access the same information.

---

[250] Many major tech companies—Facebook, Google, Microsoft, and Yahoo included—actively seek greater permission to disclose the types of national security requests they have received, apparently in an attempt to salvage their customers' goodwill. *See* Claire Cain Miller, *Tech Giants File Suit over Spying on Users*, N.Y. TIMES, Sept. 10, 2013, at B3.

[251] Jon D. Michaels, *All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror*, 96 CAL. L. REV. 901, 915-16 (2008).

[252] *See generally* Simmons, *supra* note 3.

[253] *See supra* notes 117-118 and accompanying text.

[254] *See supra* notes 142-150 and accompanying text (describing Amazon's terms).

[255] *See* Richards, *Perils of Social Reading*, *supra* note 4, at 721-22.

Protecting private reading therefore requires a regime stronger than the typical notice-and-consent model. If reading records are to remain protected, then users must have the right to access information while denying information providers the permission to disclose or otherwise exploit their reading habits.

The Video Privacy Protection Act ("VPPA") provides a viable alternative. While the VPPA allows consumers to consent to any number of uses for their data, it provides that access to video rentals cannot be conditioned on such consent.[256] Under this model, consent for subsequent disclosures must either be in exchange for bonus features, or clearly understood by the consumer as a gratuity.

One underappreciated benefit of the VPPA's approach, which requires users to opt-in to a company's use of their data, is that it forces the industry to explain to consumers *why* they should agree to give up their privacy. Applying this approach more broadly would have the potential to spark a conversation about the value of privacy compared to whatever gains could be realized by permitting a company to make various uses of customer data. This sort of churn might yield privacy practices that better reflected people's valuation of their privacy.

C. Regulating Data Retention

One great but underappreciated protection provided by the library regime is its deletion of circulation records once materials are returned.[257] The mere retention and internal exploitation of reading records may stifle free inquiry, in part because the stockpiling of data puts records at risk of subsequent disclosure. Recognizing these concerns, the library approach all but guarantees that there will be no future misuse of information by the library, and no undesirable disclosures to the government, other companies, or one's local community.

This feature is not a formal requirement of the law—except in a select few states[258]—but an outgrowth of libraries' normative commitments. While comprehensive protection of reader privacy may demand limits to the retention of user records, many information providers would find these limits difficult to swallow: discussions of privacy typically take for granted

[256] 18 U.S.C.A. § 2710(b)(2)(B)(i) (West Supp. 2013) (requiring that consent be "in a form distinct and separate from any form setting forth other legal or financial obligations"); *id.* § 2710(b)(2)(B)(iii) (requiring the rental company to provide "an opportunity, in a clear and conspicuous manner, for the consumer to withdraw [his consent] on a case-by-case basis").

[257] *See supra* Section II.C.

[258] *See supra* note 121.

that various services can collect, retain, and internally exploit users' data.[259] Jane Bambauer raises the stakes further by arguing companies have a First Amendment right to data collection, an argument that would invalidate privacy laws that could not withstand heightened constitutional scrutiny.[260]

Such a move nonetheless has precedent. The VPPA already requires the rental industry to delete personally identifiable information collected in the course of providing video rentals as soon as practicable.[261] We also see this move applied to a wider array of records in an arena where society has made particularly strong commitments to privacy: the protection of children on the Internet. The FTC, pursuant to its rulemaking authority under the Children's Online Privacy Protection Act of 1998 ("COPPA"),[262] now requires parental consent before a website can collect personally identifiable data from children.[263] It also mandates that service providers "shall retain personal information collected online from a child for only as long as is reasonably necessary to fulfill the purpose for which the information was collected" and then delete it.[264] If society is serious in its commitment to protecting reading records, a similar approach may be warranted.

That being said, a regime that dictates mandatory, nearly immediate deletion of records may go beyond what is necessary. Consumers might sometimes prefer to allow information providers to retain records because

---

[259] *But see* MAYER-SCHÖNBERGER, *supra* note 122, at 177-78 (describing voluntary efforts by major search engines like Google and Yahoo to discard personal identifiers in search queries after a specified number of months, and Amazon's option allowing users to exclude prior purchases on an ad-hoc basis from the set it considers when making recommendations); *see also Improve Your Recommendations*, *supra* note 143 (describing the options for curating one's recommendations on Amazon).

[260] *See* Jane R. Bambauer, *Is Data Speech?*, 66 STAN. L. REV. ___ (2014) (forthcoming), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2231821. This forthcoming article is quite provocative and has already drawn replies from scholars who take a contrary view. See, for example, Neil Richards' argument that the "data is speech" position paves the way for a style of digital Lochnerism whereby industry could invoke the First Amendment to immunize itself from all manner of regulation, NEIL M. RICHARDS, INTELLECTUAL PRIVACY ch. 5 (forthcoming 2014); Neil M. Richards, *Why Data Privacy Law Is (Mostly) Constitutional* (SSRN Elec. Library, Working Paper No. 2,335,196, 2013), http://ssrn.com/abstract=2335196) (previewing the arguments from chapter 5 of Richards' forthcoming book); and Andrew Tutt's argument conceding that many privacy regulations would likely be subject to heightened scrutiny under extant First Amendment doctrine, but that the better approach would reject such scrutiny and recognize these regulations as protecting individuals' speech rights, Andrew Tutt, *The New Speech*, 41 HASTINGS CONST. L.Q. 235 (2013).

[261] 18 U.S.C. § 2710(e) (2006).

[262] 15 U.S.C. §§ 6501-6506 (2012).

[263] 16 C.F.R. § 312.5 (2013).

[264] 78 Fed. Reg. 3972, 4012 (Jan. 17, 2013) (to be codified at 16 C.F.R. § 312.10).

they derive value from personalized recommendations or the ability to review their research histories. As with disclosure, the real test should be whether readers retain meaningful control over their privacy. Viktor Mayer-Schönberger offers an elegant approach to this problem: he recommends that users be allowed to set an "expiration date" for their data at the time they complete a transaction.[265] The alternative might be to give users the right to request deletion of certain records on an ad-hoc basis after their transactions, but this approach carries the risk that consumers will ignore or forget this option much as they do in other settings where they have a right to opt out.[266] The expiration-date approach would ameliorate the under-utilization problem by integrating the retention decision into the transaction itself.

CONCLUSION

The challenges of reader privacy in the digital age cannot be answered with solutions developed for a pre-networked world. The library confidentiality regime is an actor-defined regime, and as such it has proven unable to protect against intrusions by the non-library intermediaries who now facilitate reading both inside and outside the library.

To address such intrusions, I propose we move beyond the actor-defined approach to confidentiality to one based on content. While my approach is grounded in a discussion of reader privacy, its concerns cut across subject matter. Actor-defined obligations are ineffective in the digital age because they cannot account for the third parties ubiquitous in electronic transactions, even within trusted institutions. Scholars, policymakers, and private parties could overcome this problem by targeting their interventions to particular types of content without bogging themselves down with the decision of which actors to regulate. This approach would not only maintain confidentiality within institutions where the need for protection has been recognized, but also provide a vehicle for extending these commitments to new contexts where the same privacy interests are at stake.

---

[265] *See* MAYER-SCHÖNBERGER, *supra* note 122, at 178-95.

[266] *See, e.g.*, Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1879, 1885 & n.16 (2013) (discussing a study where "only 0.5% of banking customers had exercised their opt-out rights"); *see also* MAYER-SCHÖNBERGER, *supra* note 122, at 178 ("Amazon already offers its customers a way to exclude specific book purchases from the information base used for recommendations. But users have to locate and navigate to a specific web page to do so. It would be much easier if at the time of purchase customers are given a chance to enter an expiration date for such transaction information.").

But a content-defined approach should not compel us to lose sight of context. Whereas an actor-defined regime speaks to a particular industry with practices that are already known, a content-defined regime must speak to a number of different actors with differing normative commitments and business incentives. As the library example shows, important protections are often supplied by norms rather than formal obligations, and replicating these protections among actors with different norms presents its own set of challenges. By obviating the determination of who should be regulated, the content-defined approach throws these challenges into sharp relief and provides the means for better aligning our privacy commitments with the realities of the information age.