LEGAL STUDIES RESEARCH PAPER SERIES

PAPER NO. 12-03-06

March 2012

THE PERILS OF SOCIAL READING

by

Neil M. Richards
Professor of Law

Washington University in St. Louis
SCHOOL OF LAW

The Perils of Social Reading

Neil M. Richards
Professor of Law
Washington University School of Law
nrichards@wustl.edu

Our law currently treats records of our reading habits under two contradictory rules – rules mandating confidentiality, and rules permitting disclosure. Recently, the rise of the social Internet has created more of these records and more pressures on when and how they should be shared. Companies like Facebook, in collaboration with many newspapers, have ushered in the era of "social reading," in which what we read may be "frictionlessly shared" with our friends and acquaintances. Disclosure and sharing are on the rise.

This Article sounds a cautionary note about social reading and frictionless sharing. Social reading can be good, but the ways in which we set up the defaults for sharing matter a great deal. Our reader records implicate our intellectual privacy – the protection of reading from surveillance and interference so that we can read freely, widely, and without inhibition. I argue that the choices we make about how to share have real consequences, and that "frictionless sharing" is not frictionless, nor it is really sharing. Although sharing is important, the sharing of our reading habits is special. Such sharing should be conscious and only occur after meaningful notice.

The stakes in this debate are immense. We are quite literally rewiring the public and private spheres for a new century. Choices we make now about the boundaries between our individual and social selves, between consumers and companies, between citizens and the state, will have unforeseeable ramifications for the societies our children and grandchildren inherit. We should make choices that preserve our intellectual privacy, not destroy it. This Article suggests practical ways to do just that.

Word Count: 16,800 words, including footnotes

The Perils of Social Reading

Neil M. Richards[*]

TABLE OF CONTENTS

[*] Professor of Law, Washington University School of Law. For helpful discussions about these issues and comments on earlier drafts, thanks to Marvin Ammori, Adam Badawi, Scott Baker, Danielle Citron, Woody Hartzog, John Inazu, Pauline Kim, Jonathan King, Chris Libertelli, Bill McGeveran, Wendy Niece Richards, Dan Solove, and Chris Wolf. Thanks also to my faculty assistant Rachel Mance and my research assistants Joanna Cornwell and James Hollis.

INTRODUCTION

Sharing, we are told, is cool. At the urging of Facebook and Netflix, the House of Representatives recently passed a bill to "update" an obscure 1988 law known as the Video Privacy Protection Act ("VPPA").[1] Facebook and Netflix wanted to modernize this law from the ancient VHS era, arguing that its protection of video store records stood in the way of innovation in sharing movie recommendations among friends. The Netflix Amendments would have allowed companies to obtain a single, durable consent to share all movies viewed automatically and perpetually on Facebook and other social networks. The bill stalled in the Senate after a feisty committee hearing,[2] but given the vast changes in technology and social norms since 1988, some modernization of our video privacy law is inevitable.

The VPPA is just the start; merely one part of a much larger trend towards "social reading." The Internet and social media have opened up new vistas for us to share our preferences in films, books, and music. Services like Spotify and the Washington Post Social Reader already integrate our reading and listening into social networks like Facebook, providing what CEO Mark Zuckerberg calls "frictionless sharing."[3] Under a regime of frictionless sharing, we don't need to choose to share our activities online. Instead, everything we read or watch automatically gets uploaded to our Facebook or Twitter feed. As Zuckerberg puts it, "Do you want to go to the movies by yourself or do you want to go to the movies with your friends? You want to go with your friends."[4] Music, reading, web-surfing, and Google searches, in this view, would all seem to benefit from being made social.[5]

[1] H.R. 2471, 112th Cong. (2011).

[2] *The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century: Hearing on H.R. 2471 Before the Subcomm. on Privacy, Technology and the Law of the S. Comm. on the Judiciary, 112th Cong.* (2012).

[3] Alexia Tsotsis, *Live from Facebook's 2011 F8 Conference [Video]*, TECHCRUNCH (Feb. 20, 2012, 11:50 PM), http://techcrunch.com/2011/09/22/live-from-facebooks-2011-f8-conference-video/ (Zuckerberg said "[t]hese new apps will focus on 'Frictionless Experiences,' 'Realtime Serendipity' and 'Finding patterns'").

[4] Evgeny Morozov, *The Death of the Cyberflâneur*, NEW YORK TIMES, Feb. 5, 2012, at SR2.

[5] See also JEFF JARVIS, PUBLIC PARTS: HOW SHARING IN THE DIGITAL AGE IMPROVES THE WAY WE WORK AND LIVE 43-62 (2011) (extolling the values of sharing and "publicness").

Not so fast. This Article sounds a cautionary note against "frictionless sharing" and "social reading." The sharing of book, film, and music recommendations is important, and social networking has certainly made it easier. But a world of automatic, always-on disclosure should give us pause. What we read, watch, and listen to matter, because they are how we make up our minds about important social issues – in a very real sense, they are how we make sense of the world.

What's at stake is something I and other privacy scholars call "intellectual privacy" – the idea that records of our reading and movie watching deserve special protection compared to other kinds of personal information.[6] The films we watch, the books we read, and the web sites we visit are essential to the ways we try to understand the world we live in. Intellectual privacy protects our ability to think for ourselves, without worrying that other people might judge us based on what we read. It allows us to explore ideas that other people might not approve of, and to figure out our politics, sexuality, and personal values, among other things. It lets us watch or read whatever we want without fear of embarrassment or being outed. This is the case whether we're reading communist or anti-globalization books; or visiting web sites about abortion, gun control, cancer, or coming out as gay; or watching videos of pornography, or documentaries by Michael Moore, or even "The Hangover 2."

I'm not arguing that we should never share our intellectual preferences. On the contrary, sharing and commenting on books, films, and ideas is the essence of free speech. We need access to the ideas of others so that we can make up our minds for ourselves. Individual liberty has a social component. But when we share – when we speak – we should do so consciously and deliberately, not automatically and unconsciously. Because of constitutional magnitude of these values, our social,

[6] Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387 (2008). For a partial list of other scholars who have adopted this framework, see, e.g., JULIE COHEN, THE NETWORKED SELF (2012); DANIEL J. SOLOVE, NOTHING TO HIDE (2011); Pauline Kim, *Electronic Privacy and Employee Speech*, 87 CHI.-KENT L. REV. (forthcoming 2012); William McGeveran, *Mrs. Mcintyre's Persona: Bringing Privacy Theory To Election Law*, 19 WM. & MARY BILL RTS. J. 859 (2011); Paul Ohm, *Massive Hard Drives, General Warrants, And The Power Of Magistrate Judges*, 97 VA. L. REV. IN BRIEF 1 (2011); Christopher Slobogin, *Citizens United & Corporate & Human Crime,* 14 GREEN BAG 2D 77 (2010).

technological, and legal norms should support rather than undermine our intellectual privacy. At a practical level, always-on social sharing of our reader records provides less valuable recommendations than conscious sharing, and it can deter us from exploring ideas that our friends might find distasteful. Rather than "over-sharing," we should share better, which means *consciously*, and we should expand the limited legal protections for intellectual privacy rather than dismantling them.

The stakes in this debate are immense. We are quite literally rewiring the public and private spheres for a new century. Choices we make now about the boundaries between our individual and social selves, between consumers and companies, between citizens and the state, will have unforeseeable ramifications for the societies our children and grandchildren inherit.

My argument here has four parts. In Part I, I explain our law's conflicted treatment of reading records. I explain the background and theory of the VPPA, and show how its robust protection of video rental privacy is at odds with our minimal legal protections for books, music, and web-browsing. I also show how the rise of the social Internet is putting ever-greater pressure on this contradiction, presenting us with a choice between default settings for the privacy of what we read – between confidentiality and disclosure. In Part II, I argue that important constitutional values are at stake in the choice between these two regimes. The most important of these is intellectual privacy – the ability to think and read freely without monitoring or interference. Drawing on literature, sociology, and the work of library and information science professionals, I show how a meaningful measure of intellectual privacy in our reader records is essential to protect our critical civil liberties of privacy and free speech. In Part III, I demonstrate the dangers of a model of frictionless sharing for reader records, both in its threat to intellectual privacy, and its diminished value of sharing on its own terms. Finally, in Part IV, I sketch out what a legal regime protecting both intellectual privacy and conscious sharing could (and should) look like, identifying four principles that laws dealing with reading records should embrace.

I. TWO MODELS FOR SOCIAL READING

How should the law treat our "reading records," broadly defined, such as books read, movies watched, web pages browsed, and search engine queries? Our law currently provides two conflicting answers.

Depending upon the type of records and the jurisdiction, we currently use two models in a rather haphazard way. On the one hand, in a few areas, special protection is given to reader records, for which confidentiality of information is the norm. These include movie records under the federal VPPA, but also numerous state laws regulating library records and a few for bookstores. On the other hand, most reader records are treated to very little legal protection, often no more than the promises web sites make in their privacy policies. For these records, disclosure is the norm.

A. Confidentiality Rules

One way our law treats reader records is through confidentiality rules. Confidentiality rules recognize that information is frequently shared with others with the expectation that our confidantes keep the information to themselves.[7] They place obligations on the people and organizations who receive our information not to disclose it without our consent.[8] Familiar examples of confidentiality rules include professional duties of confidentiality imposed on doctors,[9] lawyers,[10] accountants,[11] and ministers.[12] Confidentiality rules often recognize that sharing of information with trusted confidantes is important, and that an assurance of confidentiality is necessary in order to enable full and frank sharing of information. For example, rules of this sort encourage us to tell our doctors potentially embarrassing medical details so that they can assemble a complete clinical picture to treat our ailments better.[13] We

[7] *See* Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123 (2007).

[8] Id.

[9] *See* AMERICAN MEDICAL ASSOCIATION, CODE OF MEDICAL ETHICS: FUNDAMENTAL ELEMENTS OF THE PATIENT-PHYSICIAN RELATIONSHIP, Opinion 10.01(4) (1992).

[10] *See* MODEL RULES OF PROF'L CONDUCT R. 1.6 (1983).

[11] AMERICAN INSTITUTE OF CPAS, CODE OF PROFESSIONAL CONDUCT § 301.

[12] *See, e.g.*, THE NATIONAL CATHOLIC RISK RETENTION GROUP, MODEL CODE OF PASTORAL CONDUCT § 2, *available at* http://www.virtus.org/virtus/pastoralconduct.pdf (stating "[i]nformation disclosed to a Pastoral Counselor or Spiritual Director during the course of counseling, advising, or spiritual direction shall be held in the strictest confidence possible").

[13] Mark O. Hiepler & Brian C. Dunn, *Irreconcilable Differences: Why the Doctor-Patient Relationship is Disintegrating at the Hands of Health Maintenance Organizations and Wall Street*, 25 PEPP. L. REV. 597, 609 (1998) ("[o]ne of the key aspects of an "ideal" doctor-patient relationship is open and honest communication"); Beata Gocyk-Farber, *Patenting Medical Procedures: A Search for a Compromise Between Ethics and Economics*, 18 Cardozo L. Rev. 1527, 1547 (1997) ("[a] potential intrusion on

also protect the honest discussions essential to healthy marital relationships by preventing spouses from being called to testify each other in many legal matters.[14] Confidentiality rules of these sorts can be waived by the client or spouse, but they set a default norm of nondisclosure.

Confidentiality rules have also been placed on reader records. The most famous of these rules is the VPPA, known colloquially as the "Bork Bill." As discussed earlier, the VPPA prohibits video stores from sharing the video rental histories of their customers without their consent.[15] The law came about when Michael Dolan, a reporter from the alternative *Washington City Paper,* went to Potomac Video in Washington and obtained and published the rental records of Supreme Court nominee Robert Bork's family. Ironically enough, Dolan's intent was to expose Bork because of Bork's public rejection of the right to privacy.[16] Dolan's article, "The Bork Tapes," was subtitled "Never mind his writings on *Roe vs. Wade*. The inner workings of Robert Bork's mind are revealed by the videos he rents."[17] Dolan argued that Bork's 146 film rentals revealed him to be a boring and middlebrow Anglophile, afraid of sex and violence, who watched mainly movies starring men, and who was better suited to being a "Supreme Couch Potato" than Supreme Court justice.[18] The article

patients' privacy may adversely affect honesty and openness in the doctor-patient relationship, where honest disclosure by the patient of his condition is often the key to successful treatment").

[14] For example, the spousal communications privilege prevents communications from a person to their spouse being introduced against them at trial. The separate marital privilege allows a person to prevent their current spouse being called as a witness against them. The theory behind both privileges is that the damage which would occur to marital relationships in the absence of the privileges is greater than the harm to the truth-seeking process which the privileges cause. GEORGE FISHER, EVIDENCE 836 (2d ed. 2008). *See* Wolfle v. U.S., 291 U.S. 7 (1934) (holding to this effect).

[15] Video Privacy Protection Act, 18 U.S.C. § 2710(b)(1) (1988) ("[a] video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person").

[16] Michael Dolan, *The Bork Tapes Saga*, *available at* http://theamericanporch.com /bork2.htm. For Robert Bork's views on constitutional minimalism, *see* Robert H. Bork, *Neutral Principles and Some First Amendment Problems*, 47 IND. L.J. 1 (1971); ROBERT H. BORK, THE TEMPTING OF AMERICA: THE POLITICAL SEDUCTION OF THE LAW (1990).

[17] Michael Dolan, *The Bork Tapes: Never mind his writings on Roe vs. Wade. The inner workings of Robert Bork's mind are revealed by the videos he rents*, WASHINGTON CITY PAPER, Sept. 25, 1987, at 56, available at www.theamericanporch.com/bork5.

[18] Id.

ended with a threat to disclose the viewing habits of other politicians, describing the project as a possible "life's work."[19]

Despite the fact that the juiciest disclosure in the Bork files was merely John Hughes's *Sixteen Candles* (presumably rented not by Bork, but by his teenage daughter),[20] a horrified Congress quickly passed the VPPA, perhaps fearing the disclosure of more interesting film preferences should politicians be targeted next. The VPPA's legislative history reveals a real concern for the privacy of reader records, broadly defined. The Senate Report justifies the protection of rental records on the grounds that they reveal the core of who we are as individuals. It argues that our "right to privacy protects the choice of movies that we watch with our family in our own homes. And it protects the selection of books that we choose to read. These activities are at the core of any definition of personhood. They reveal our likes and dislikes, our interests and our whims. They say a great deal about our dreams and ambitions, our fears and our hopes. They reflect our individuality, and they describe us as people."[21]

As enacted, the VPPA requires that anyone in the business of the "rental, sale, or delivery" of "prerecorded video cassette tapes or similar audio visual materials" may only disclose the sale or rental records of a customer "with the informed, written consent of the consumer given at the time the disclosure is sought."[22] The statute also requires that law enforcement seeking access to video rental records must provide a warrant supported by probable cause that the "records or other information sought are relevant to a legitimate law enforcement inquiry."[23] It also includes a private right of action allowing any "person aggrieved" by a knowing disclosure of records by a video service provider

[19] Id.

[20] See id. ("Bork's taste in actresses isn't as clearly defined, although there are a few repeaters: (Meryl Streep (Out of Africa, Plenty), Grace Kelly (courtesy of her appearances in a spate of Hitchcock's films), Better Midler (Down and Out in Beverly Hills, Ruthless People), and Molly Ringwald (Pretty in Pink, Sixteen Candles). In light of guest appearances by Mae West (My Little Chickadee) and Madonna (Desperately Seeking Susan), I'd have to say Judge Bork likes his women American, self-possessed, and confident, and capable of private passion, however reserved they may be in public.")

[21] S. REP. 100-599 (1988).

[22] 18 U.S.C. § 2710.

[23] 18 U.S.C. § 2710(b)(3).

to recover the greater of actual damages or $2,500 in liquidated damages, plus punitive damages and attorneys' fees where appropriate.[24]

Courts applying the VPPA have read it broadly. In *Amazon.com v. Lay*, the North Carolina Department of Revenue demanded as part of a tax investigation that Amazon.com reveal "all information for all sales to customers with a North Carolina shipping address" from 2003 to 2007."[25] A federal district court held that the request violated the VPPA because it would have required Amazon to disclose the titles of individual movies purchased by its North Carolina customers. Such disclosure would be in violation of Amazon's confidentiality obligation under the VPPA, and would threaten its customers' First Amendment rights of intellectual freedom.[26]

Other courts have read the VPPA's private right of action to apply not only against video stores, but to those who induce or solicit breaches of video record confidentiality. Thus, in *Dirkes v. Borough of Runnymeade*, a police department investigating a claim of misconduct by one of its officers obtained the names of pornographic films that the officer and his wife had rented from "Videos to Go," their local video store.[27] The court held not only that the video store had violated the VPPA, but that the private right of action applied to "all parties who are in possession of personally identifiable information as a direct result of an improper release of such information."[28]

Another federal law providing a confidentiality rule for video is the Cable Communications Policy Act of 1984. This statute prohibits cable television service providers from disclosing personal information about their subscribers' habits "without the prior written or electronic consent of the subscriber concerned."[29] Like the VPPA, the Cable Act provides for a private right of action for actual damages, or liquidated damages of the

[24] 18 U.S.C. § 2710(c).

[25] Amazon.com v. Lay, 758 F.Supp.2d 1154, 1159 (W.D. Wash. 2010).

[26] Id. at 1170.

[27] 936 F.Supp. 235 (D.N.J. 1996). But see *Daniel v. Cantell*, 375 F.3d 377 (6th Cir. 2004) (holding that law enforcement officials who are investigating a case do not count as video tape service providers under the VPPA).

[28] *Dirkes*, 936 F.Supp. at 240.

[29] 47 U.S.C. § 551.

greater of $1,000 or $100 per day of violation. Also like the VPPA, plaintiffs can recover punitive damages and attorneys' fees.[30]

State law sometimes provides even greater protections than the federal VPPA. Video rentals in Connecticut and Maryland, for example, are considered confidential, and cannot be sold, with criminal fines and imprisonment for unlawful disclosure.[31] California, Delaware, Iowa, Louisiana, New York, and Rhode Island have also enacted video privacy laws.[32] Michigan's video privacy law is broader than the VPPA, and protects records of book purchases, rentals, and borrowing as well.[33]

Books are sometimes better protected under state law than videos. In Colorado, the state constitution's free speech guarantee has been interpreted to limit government access to bookstore records.[34] Perhaps the strongest book privacy law is California's new Reader Privacy Act, which took effect on January 1, 2012.[35] This Act places a confidentiality rule on reading records, broadly defined to include emerging technologies such as e-books. It prohibits the disclosure of reader information except where stringent requirements are met, such as a court order for disclosure to government, or to a private entity only where the user has given her "informed, affirmative consent to the specific disclosure for a particular purpose.[36]

In addition to these video and book statutes, most states protect the confidentiality of library records from sale or other disclosure.[37] For a

[30] Id.

[31] CONNECTICUT GENERAL STATUTE § 53-450; MARYLAND CODE ARTICLE 27 § 583; MARYLAND CODE, CRIMINAL LAW, § 3-907.

[32] *See* CAL. CIV. CODE § 1799.3 (2012); DEL. CODE ANN. tit. 11, § 925 (2012); LA. REV. STAT. ANN. § 37:1748 (2012); N.Y. GEN. BUS. LAW § 670 (2012); R.I. GEN. LAWS § 11-19-32 (2012).

[33] MICH. COMP. LAWS § 445.1712 (1988

[34] See Tattered Cover, Inc. v. City of Thornton, 44 P.3d 1044, 1053 (Colo. 2002) ("Search warrants directed to bookstores, demanding information about the reading history of customers, intrude upon the First Amendment rights of customers and bookstores because compelled disclosure of book-buying records threatens to destroy the anonymity upon which many customers depend.").

[35] CALIF. CODE ANN. § 1798.90 (2012).

[36] CALIF. CODE ANN. § 1798.90(c)(3) (2012).

[37] Library records confidentiality is protected in at least forty-eight states and the District of Columbia. For a catalogue of such statutes, see Anne Klinefelter, *Library Standards for Privacy: A Model for the Digital World?*, 11 N.C.J.L. & TECH. 553 (2010).

typical example, the Missouri library confidentiality statute provides that "no library or employee or agent of a library shall be required to release or disclose a library record or portion of a library record to any person or persons," except where the person gives written request to the disclosure or subject to a court order.[38] Moreover, the scope of what constitutes a "library record" is very broad, covering any book, films, music, art works, or any "other library property which a patron may use, borrow or request."[39]

B. Disclosure Rules

Confidentiality rules for reader records live in a haphazard and piecemeal relationship to another set of rules for which the disclosure of reader records is the default. In fact, although reader confidentiality rules can be robust where they apply, they remain a minority position for the vast majority of records pertaining to reading and internet usage. Most reader records at the federal and state level receive no special protection. For these records, disclosure is the norm, subject only to two constraints – the *self-interest* of the record holder, and *contracts* between parties such as privacy policies.

Consider, in this regard, the treatment of book purchase records under federal law. Although the "Bork Bill" led to the protection of video sale and rental records under the VPPA, there is no federal statute regulating the disclosure of book purchases. For example, during the Independent Counsel investigations of President Clinton that led to his impeachment, the Independent Counsel sought to compel Kramerbooks in Washington, D.C. to release Monica Lewinsky's book purchase records. Kramerbooks refused on the grounds that it would hurt its business and infringe Lewinsky's First Amendment rights.[40] These arguments met with some success, but they did not stop the Independent Counsel from obtaining the records directly from Lewinsky. Ultimately, the Special Prosecutor Kenneth Star was able to get Lewinsky to concede that she had purchased erotic literature for Bill Clinton, including Nicholson Baker's

[38] MO. REV. STAT. § 182.817 (2012).

[39] MO. REV. STAT. § 182.815 (2012).

[40] David Streitfeld & Bill Miller, *Quest for Book Buys Faces High Bar*, WASH. POST, Apr. 10, 1998, at B01.

phone sex novella *Vox* and Walt Whitman's *Leaves of Grass*.[41] But the important lesson for present purposes is that if it had wanted to, or if its commercial interests favored disclosure, Kramerbooks could have made any of its records public free of any legal obligation. It could do so tomorrow, as well. Unlike in the case of Robert Bork's viewing habits, the disclosure of Presidential reading habits did not prompt the passage of a "Clinton Bill" placing a federal confidentiality rule on book purchase records.

In the online environment, disclosure rules apply to book sales as well. Moreover, with the rise of electronic reading, bookstores, websites, search engines, and other electronic media companies collect vastly more data than old-fashioned libraries and bookstores.[42] Kindle, for example, tracks "most highlighted" passages on its e-books.[43] Kindle's parent company, Amazon.com, is able to use cookies and other technologies to track not just what books, films, and other products its customers purchase, but what they browse on the site and for how long.[44] Federal electronic privacy law regulates government access to this information, but as a general matter does not prevent companies from disclosing such records to other private entities.[45]

On web sites, targeted advertising is fuelled by a variety of technologies and companies intended to track the web-surfing habits of Internet users to enable "behavioral" personalized advertisements.[46] Consider the ubiquitous Facebook "like" and "recommend" buttons that appear on over 900,000 news, lifestyle, and sports websites across the Web.[47] When a Facebook user clicks the "like" button, the embedded

[41] OFFICE OF INDEPENDENT COUNSEL, COMMUNICATION FROM KENNETH W. STARR, INDEPENDENT COUNSEL, TRANSMITTING A REFERRAL TO THE UNITED STATES HOUSE OF REPRESENTATIVES FILED IN CONFORMITY WITH THE REQUIREMENTS OF TITLE 28, UNITED STATES CODE, SECTION 595(C), nn.79, 698 (1998).

[42] Richards, *Intellectual Privacy*, supra note 6, at 388.

[43] Rebekah Denn, *Is it Creepy that Amazon is Tracking Most-Highlighted Kindle Passages?*, CSMonitor.com (May 3, 2010).

[44] Amazon.com Privacy Notice, effective Nov. 1, 2008, available at http://www.amazon.com/gp/help/customer/display.html?nodeId=468496#examples.

[45] *See* 18 U.S.C. § 2701 *et seq*. (2012).

[46] *See* Chip Bayers, *The Promise of One to One (A Love Story): The Honeymoon's Over. A New Look at the Web's True Power to Serve and Sell You*, WIRED, May 1998; Adam Ostrow, *'Like' it or Not, Online Ads are Getting Personal*, CNN (Jan. 28, 2011).

[47] Byron Acohido, *Facebook Tracking Is Under Scrutiny,* USA TODAY, Nov. 11, 2011.

software application sends the information back to Facebook in order to publish the event on the user's News Feed. But how did Facebook know in the first place which user clicked the button? The answer is that Facebook often knows which of its users are on which pages throughout the web in order to serve up their personalized buttons in the first place.[48] As the *New York Times* puts it, "Facebook is collecting a vast amount of data about the Web travels of some 800 million people worldwide with the buttons, unbeknownst to most of them. And other social networks are starting to do the same."[49] A key design feature of Facebook makes its tracking and profiling even more problematic. Unlike traditional behavioral advertising, which is linked to a cookie on a computer that may have several users, Facebook accounts are linked to a person's real name, a requirement that the company strenuously defends.[50] For example, it recently deactivated the account of author Salman Rushdie for his failure to call himself "Ahmed Rushdie," the name which appears on his passport.[51] For many of its users, then, Facebook knows what they are reading, and it knows them precisely by name.

When disclosure is the default rule, the only constraints on disclosure – contract and self-interest – are of limited effectiveness. Many if not most websites have a "privacy policy," which states what kinds of information they collects, uses, and discloses to others. Privacy policies are mandated by California law, and strongly encouraged by the Federal Trade Commission, which oversees unfair and deceptive data use by companies.[52] Nevertheless, the evidence suggests that few users read the often dense legal or technical language contained in privacy policies.[53]

[48] Riva Richmond, *As 'Like' Buttons Spread, So Do Facebook's Tentacles*, NEW YORK TIMES, Sept. 27, 2011.

[49] Id.

[50] See http://www.facebook.com/legal/terms ("Facebook users provide their real names and information.").

[51] Somini Sengupta, *Rushdie Runs Afoul of Web's Real-Name Police*, NEW YORK TIMES, November 14, 2011. After Rushdie criticized Facebook (ironically enough) on Twitter, Facebook restored his account under the "Salman Rushdie" name. Id.

[52] CAL. CIV. CODE § 1798.83(b)(1)(B) (2012); FEDERAL TRADE COMMISSION, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 6 (2010) ("[i]n the mid-to-late 1990s, the FTC encouraged companies to implement the fair information practice principles of notice, choice, access, and security and undertook enforcement efforts related to claims companies made in their privacy notices").

[53] Jensen, C., & Potts, C., *Privacy Policies As Decision--making Tools: An Evaluation of Online Privacy Notices,* Proceedings of the 2004 Conference on Human

As Woodrow Hartzog points out, "it has become a truism that virtually no one reads standard-form online agreements," especially privacy policies.[54] Moreover, as online contracts of mass adhesion, there is no bartering or dickering over privacy terms, and the terms in privacy contracts are drafted by companies almost entirely to their benefit.[55] A 2007 review of the contract cases in which consumers alleged that websites had breached their privacy policies found that courts frequently find for the websites notwithstanding privacy promises.[56] The FTC has engaged in a few unfair and deceptive trade practices actions against companies for breaching their privacy policies,[57] but whatever the legal effect of privacy policies, companies remain free to change their terms at any time, as Google did on March 1, 2012.[58]

Corporate self-interest is also a limited and fickle constraint on disclosure of personal information. When a company's interests align with those of customers, as when the government of North Carolina sought to inspect Amazon purchases for tax compliance, companies can certainly be expected to keep records confidential.[59] Other times, companies might fight government disclosure when it is good for business, as Kramerbooks did in resisting the Monica Lewinsky subpoenas.[60] But this is only a limited protection. For example, when

Factors in Computing Systems (2004); Jensen, C., Potts, C., & Jensen, C., Privacy Practices of Internet Users: Self-reports Versus Observed Behavior (2005); Andy Greenberg, *Who Reads the Fine Print Online? Less Than One Person in 1000*, FORBES (Apr. 8 2010, 3:15 PM), http://blogs.forbes.com/firewall/2010/04/08/who-reads-the-fine-print-online-less-than-one-person-in-1000/.

[54] Woodrow Hartzog, *Website Design as Contract*, 60 AM. U. L. REV. 1635, 1642 (2011).

[55] Hartzog, *Website Design as Contract*, supra note 54, at 1648.

[56] Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control Over Personal Information?*, 111 PENN. ST. L. REV. 587, 594-97 (2007).

[57] *See, e.g., In re Sears Holdings Mgmt. Corp.*, F.T.C. Docket No. C-4264 (F.T.C. Aug. 31, 2009)*; In re Google Inc.*, F.T.C. File No. 1023136 (Oct. 24, 2011); *In Re Facebook, Inc.*, F.T.C. File No. 0923184 (Dec. 5, 2011); *FTC v. Toysmart.com, LLC*, No. 00-11341-RGS (D. Mass. July 21, 2000); *In re Gateway Learning Corp.*, F.T.C. File No. 042-3047 (Dec. 28, 2004); *In re* Zango, Inc., F.T.C. File No. 0523130 (Mar. 9, 2007); *In re* DirectRevenue LLC, F.T.C. File No. 0523131 (June 27, 2009).

[58] See http://www.google.com/policies/.

[59] *Cf. Amazon.com*, 758 F.Supp.2d.

[60] John P. Martin, *Principle at Stake, Store Owner Says*, WASH. POST (May 29, 1998); David Streitfeld & Ann Gerhart, *Bookstores Have Defenders, Skeptics in Bind Over Subpoenas*, WASH. POST, Apr. 3, 1998, at F01.

Justice Department subpoenaed the search terms of millions of Internet users from most of the big search engine companies in 2006, all of the major search engines except Google provided the information willingly.[61]

When the government is not seeking records, self-interest is an even weaker constraint. In our data-driven Internet economy, there is economic value in information, which provides incentives to collect, amass, and analyze ever-larger quantities of ever-more granular data. The value of information means that many companies have aggressively pushed against existing legal requirements imposed by statute, contract, and the FTC. One consequence of this aggressiveness has been the large number of high-profile privacy scandals, most notably Google Buzz and Facebook Beacon.[62] Netflix recently settled a $9 million class action for breaching its confidentiality obligations under the VPPA at the same time as it was lobbying Congress to change the VPPA to allow the automatic sharing of movie preferences.[63]

When money is in information disclosure, it should be no surprise that the trend towards data aggregation and disclosure has begun to affect reader records. Records of web-browsing have been amassed by targeted advertising companies like DoubleClick (a subsidiary of Google) and Alexa (a subsidiary of Amazon) for well over a decade.[64] But in recent years, stimulated by the rise of social networking platforms, even reader records have been made more public. Facebook has once again been a leader in this trend, seeking to share such preferences by integrating

[61] Joseph Menn & Chris Gaither, *U.S. Obtains Internet Users' Search Records*, L.A. TIMES, Jan. 20, 2006, at A1.

[62] See, e.g., William McGeveran, *Disclosure, Endorsement, and Identity in Social Marketing*, 2009 U. ILL. L. REV. 1105 (Facebook Beacon); James Grimmelmann, *Privacy as Product Safety*, 19 WIDENER L.J. 793 (2010) (Google Buzz).

[63] See Jeff Roberts, *Update: Netflix Pays $9 Million To Settle Video Privacy Lawsuit*, Feb. 10, 2012, available at http://m.paidcontent.org/article/419-netflix-pays-9-million-to-settle-video-privacy-lawsuit/. Eriq Gardner, Netflix Settles Privacy Class Action Claims for $9 Million, The Hollywood Reporter, Feb. 14, 2012, available at http://www.hollywoodreporter.com/thr-esq/netflix-settles-privacy-class-action-290065.

[64] Erick Schonfeld, *(Founder Stories) DoubleClick's Kevin O'Connor: We Were Netscape's Profits*, TechCrunch.com (Aug. 18, 2011), http://techcrunch.com/2011/08/18/founder-stories-oconnor-netscape/ (DoubleClick was launched on February 24, 1996); About Alexa Internet, http://www.alexa.com/company (last visited Feb. 23, 2012) (Alexa was founded in April 1996 and that "[s]ince then, Alexa has created one of the largest Web crawls, and developed the infrastructure to process and serve massive amounts of data").

sharing applications into the Facebook experience. For example, the company recently integrated Spotify's music service into its social network, which defaults to sharing all the music a person listens to with their social connections. Neflix has also begun to share movie-watching habits on Facebook in Britain, but it was barred from doing so in the United States by the VPPA, which is why it sought to have the VPPA amended to make sharing easier.

Newspapers are also getting into the reading habits disclosure business. Besides placing tracking cookies, Facebook "like," and Google "Plus One" buttons next to their articles, leading newspapers such as *The New York Times, The Washington Post*, and *The Guardian* have created "social reader apps." These software applications plug in to both news websites and Facebook News Feeds, listing all news articles read through the app on Facebook, and showing what Facebook "friends" are reading on the news websites.[65]

Our law is thus in a muddle when it comes to reader records. It speaks with two inconsistent voices at once. It would violate federal law for Amazon to disclose movie rentals, but not book purchases or web browsing. A bookstore in California cannot disclose its customer's records, but one in New York can. Facebook can disclose what music we listen to and what news articles we read, but not which films we watch. The rise of social media platforms has increased the importance of the issue, as well as the problems caused by our law's inconsistency. At least for reader records, we need to figure out whether and when disclosure rules or confidentiality rules should be our default settings. Answering this question requires us to understand what values are at stake in our choice. It is to this question that we now turn.

II. WHY READER PRIVACY MATTERS

Why does it matter if our reading habits are disclosed to our friends? What's at stake in the choice between default rules for social reading?

---

[65] *Help: Times Reader*, NYTIMES.COM, http://www.nytimes.com/content/help/extras/reader/reader.html#readerq01 (last visited Feb. 23, 2012); *The Washington Post Social Reader*, Washingtonpost.com, http://www.washingtonpost.com/ socialreader (last visited Feb. 23, 2012); *Guardian Facebook App: FAQ*, Guardian.co.uk, http://www.guardian.co.uk/info /2011/sep/22/guardian-facebook-app-faq (last visited Feb. 23, 2012).

Recall Mark Zuckerberg's defense of "social" with which this Article opened, in which he argued that doing things with our friends is better than doing things alone.[66] He's only partially correct. We often do want to go to the movies with our friends; it's fun and it's social (even for law professors). Often we go to movies we don't really want to see, because we'd rather be with our friends than see the film we'd choose on our own. Our friends might not approve of our film, and it might even turn out that we like their movie after all. Besides, we can always watch the movie we really wanted to see alone, or at home when it leaves the theaters. So far, so good.

Social reading takes us a step further. Not only are our friends with us when we watch movies at the cinema, but they're now there when we watch movies on our computers, and also when we *read* on our computers. They never leave. An always-on regime of "frictionless sharing" means we are *always* at the movies with our friends, even when we don't want to be. It means we'll always watch the movie they choose, and we won't choose the movie we want to see if they'd make fun of us for it. We might never get to see that film we're curious but shy about. This is the case whether our film is fluffy like "Gnomeo and Juliet," political like "Bowling for Columbine," racy like "Black Swan," or something even more explicit. If we're always with our friends, we're never alone, and we never get to explore ideas for ourselves. Of course, the stakes here go beyond movies, to reading, web-surfing, and even thinking.

A completely social model for reading and exploring ideas gives us no space for contemplation, no space for thinking differently. We might, to use a current buzzword, be able to "crowd-source" our preferences, but when the crowd can see our own preferences by default, we are driven to conformity and the mainstream by social pressures.[67] Writ large, this risks driving thought, belief, and public discourse to our Facebook News Feed, hardly the best venue for thoughtful, idiosyncratic, contemplative individuality. Or public discourse.

[66] See supra note 4.

[67] Richards, Intellectual Privacy, supra note 6, at 403-04; Julie E. Cohen, *Examined Lives: Information Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1426 (2000).

A. Intellectual Privacy and Reading

There is an important value at stake in the social reading and sharing debate that has been overlooked. That value is our ability to think and read freely for ourselves, free of the watchful gaze or disapproval of other people, so that we can make up our minds for ourselves. In order for this to happen, we need to preserve spaces for solitary, private reading and thinking, a value I and other scholars have called "intellectual privacy."[68] My purpose here is not to repeat the theory. Instead I want to extend it and show its special applicability to reading in general, and social reading in particular.

Intellectual privacy rests on the idea that new ideas often develop best away from the intense scrutiny of public exposure; that people should be able to make up their minds at times and places of their own choosing, and that a meaningful guarantee of privacy – protection from surveillance or interference – is necessary to promote this kind of intellectual freedom. It rests on the idea that free minds are the foundation of a free society, and that surveillance of the activities of belief formation and idea generation can affect those activities profoundly and for the worse.[69]

How does intellectual privacy work? Writers have long noted the intuition that when we are watched, our behavior inclines to the mainstream, the inoffensive, and the "normal." This is the idea behind Jeremy Bentham's famous image of the Panopticon, a circular prison designed around a central surveillance tower that could see into all of the cells and give the prisoners a constant sense of surveillance.[70] The wardens could watch any prisoner at any time, but the individual prisoners had no idea when or even if they were being watched. The purpose of this arrangement was to create an environment of permanent surveillance in the minds of the prisoners so they would behave in the manner that the wardens desired.[71] As Bentham himself put it, "[t] o be incessantly under the eyes of the inspector is to lose in effect the power to do evil and almost the thought of wanting to do it."[72] The insight is clear – when we're being watched, we act and think differently.

[68] See sources cited supra note 6.

[69] Richards, *Intellectual Privacy*, supra note 6, at 403-04.

[70] Jeremy Bentham, *Panopticon*, in THE PANOPTICON WRITINGS (Verso 1995).

[71] Id.

[72] Jeremy Bentham, Panopticon, in THE PANOPTICON WRITINGS (Verso 1995).

The most striking illustration of the Panopticon in Western Culture is George Orwell's description of the mechanics of surveillance in his novel *Nineteen Eighty-Four*.[73] Orwell famously depicted a society of total surveillance by the state, intended to produce not just obedience on the part of the people, but uniformity of thought. In Orwell's society, it was not just a crime to express dissent against the state, but also a crime merely to think such an idea – a "Thoughtcrime." Orwell's fictitional state – personified by the sinister image of "Big Brother" – achieved its control over the minds of its people through old-fashioned methods such as human informers and a secret police, but also though the technology of the "telescreen." This omnipresent device operated like a modern videoconferencing device – broadcasting propaganda outwards, but also monitoring all that happened within view of its cameras. Orwell describes the operation of the telescreens as experienced by his protagonist, Winston Smith as follows:

> The telescreen received and transmitted simultaneously. Any sound that Winston made, above the level of a very low whisper, would be picked up by it, moreover, so long as he remained within the field of vision which the metal plaque commanded, he could be seen as well as heard. There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live – did live, from habit that became instinct – in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized.

By eliminating any vestige of intellectual privacy in this and other ways, Big Brother sought – successfully in Orwell's novel – to shrink the freedoms of thought and speech through surveillance, and thereby to eliminate any possibility of intellectual or political freedom for the people under its sway.[74]

---

[73] GEORGE ORWELL, NINETEEN EIGHTY-FOUR, at 4 (1949).

[74] In an influential book, Daniel Solove has argued that the best way to understand the problem of consumer databases is not through the Orwell metaphor, but by reference to a different literary metaphor – the description of inexplicable bureaucracy Franz

At one level, it would seem obvious that surveillance chills and deters free thinking and reading. This is the long-standing insight of Bentham and Orwell. But there is also rich empirical evidence that people under surveillance change their behavior towards the ordinary and the inoffensive. Over the last twenty years, a burgeoning academic literature of "surveillance studies" in sociology and other fields has attempted to document the effect of surveillance on a wide variety of human activities.[75] Although the starting point for this body of work has been the classic image of the Panopticon, this literature has explored and illustrated the normalizing effects of surveillance in a wide variety of settings. These scholars have studied the effects on behavior from (for example) state monitoring of welfare recipients or the use of undercover policing and closed-circuit television systems to deter such things as sex in public places, public urination, and crime in general.[76] Other scholars have documented the effects and implications of electronic and other forms of "new surveillance" in our increasingly information-based society.[77] Sociologist James Rule has noted that the information surveillance provisions of the Patriot Act of 2001 and the warrantless monitoring of telephone calls by the National Security Agency could be used to monitor

Kafka's *The Trial*. DANIEL J. SOLOVE, THE DIGITAL PERSON (2005). I have mostly agreed with this approach elsewhere, though I am less willing than Solove to reject the power of the Orwellian metaphor. See Neil M. Richards, *The Information Privacy Law Project*, 94 GEO. L.J. 1087, 1128-32 (2006). My purpose here is to use the metaphor to illustrate a simple proposition – when we are watched, we act differently, and when we are watched while we are reading, we read differently.

[75] See generally DAVID LYONS, SURVEILLANCE STUDIES: AN OVERVIEW (Polity 2007).

[76] E.g., Brandon Welsh and David P. Farrington, *Effects of Closed-Circuit Television on Crime*, 587 ANNALS OF THE AMERICAN ACADEMY OF POLITICAL AND SOCIAL SCIENCE 110 (May, 2003); Kevin Walby, *Police Surveillance of Male-with-Male Public Sex in Ontario*, 1983-94, in SURVEILLANCE: POWER, PROBLEMS, POLITICS (Sean P. Hier & Josh Greenberg eds. 2010); GARY MARX, UNDERCOVER: POLICE SURVEILLANCE IN AMERICA (1988); JOHN GILLIOM, OVERSEERS OF THE POOR (2001); MIKE MCCAHILL, THE SURVEILLANCE WEB, (2002); TIM NEWBURN & STEPHANIE HAYMAN, POLICING, SURVEILLANCE, AND SOCIAL CONTROL (2002); KENT UNNELL, PISSING ON DEMAND (2004).

[77] See, e.g., KEVIN D. HAGGERTY AND MINAS SAMATAS, EDS., SURVEILLANCE AND DEMOCRACY (2010); Kevin Haggerty and Amber Gaszo, *Seeing Beyond the Ruins: Surveillance as a Response to Terrorist Threats*, 30 CANADIAN J. SOCIOLOGY 169 (2005); DAVID LYON, THE ELECTRONIC EYE: THE RISE OF SURVEILLANCE SOCIETY (1994); OSCAR GANDY, THE PANOPTIC SORT (1993); JAMES B. RULE, PRIVATE LIVES AND PUBLIC SURVEILLANCE (1974); ALAN F. WESTIN, PRIVACY AND FREEDOM (1967).

political dissent.[78] Rule has suggested that surveillance of personal data could be used "to punish and intimidate" critics of the government.[79]

The deterrent effects of public or private-sector surveillance can sometimes be a good thing. For example, we put police in marked (or unmarked) cars to encourage people to obey the law and stop them from speeding or engaging in robbery. We have teachers proctor exams to prevent cheating, and we have neighborhood watch programs to deter theft. Surveillance can deter unpopular bad behavior as well as unpopular good behavior. As sociologist David Lyons puts it, "surveillance is not unambiguously good or bad."[80] To use but one example, a recent study of the use of CCTV in holding cells found that the presence of a camera restrained the violent behavior of both police and arrestees.[81] Louis Brandeis himself remarked shortly after publishing "The Right to Privacy"[82] that private surveillance could be beneficial at keeping wrongdoers in check. The initial draft of his "sunlight is the best of disinfectants" aphorism expresses the point eloquently. Concerned about wrongdoing by fraudsters, Brandeis noted that "[i]f the broad light of day could be let in upon men's actions, it would purify them as the sun disinfects."[83]

Surveillance deters bad *behavior*. But when we are talking about freedom of the mind, bad *ideas* don't exist. As Justice Powell famously put it, "[u]nder the First Amendment, there is no such thing as a false idea."[84] And keeping out those who would monitor our reading and private writing is essential if we want to explore or generate new ideas, a

[78] JAMES B. RULE, PRIVACY IN PERIL: HOW WE ARE SACRIFICING A FUNDAMENTAL RIGHT IN EXCHANGE FOR SECURITY AND CONVENIENCE (2007).

[79] Id. at 63-64.

[80] LYONS, THE ELECTRONIC EYE, supra note 80, at 5.

[81] TIM NEWBURN & STEPHANIE HAYMAN, POLICING, SURVEILLANCE, AND SOCIAL CONTROL (2002).

[82] Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890). See generally Neil M. Richards, *The Puzzle of Brandeis, Privacy, and Speech*, 63 VAND. L. REV. 1295 (2010) (exploring Brandeis's conflicting views on free speech and privacy).

[83] Letter from Louis D. Brandeis to Alice Goldmark (Feb. 26, 1891), *in* 1 Letters of Louis D. Brandeis 100 (Melvin I. Urofsky, ed., 1975). Brandeis' famous "sunlight … is the best of disinfectants" aphorism can be found in LOUIS D. BRANDEIS, OTHER PEOPLE'S MONEY—AND HOW THE BANKERS USE IT 92 (1914).

[84] Gertz v. Robert Welch, Inc, 418 U.S. 323, 339-40 (1974).

fact our law has long recognized in subtle and sometimes underappreciated ways. The philosopher Timothy Macklem explains that "[t]he isolating shield of privacy enables people to develop and exchange ideas, or to foster and share activities, that the presence or even awareness of other people might stifle. For better and for worse, then, privacy is sponsor and guardian to the creative and subversive."[85] When there is protection from surveillance, new ideas can be entertained, even when they might be deeply subversive or threatening to conventional or orthodox views. If we value a pluralistic society or the cognitive processes that produce new ideas, then some measure of intellectual privacy, some respite from cognitive surveillance, is essential. Any meaningful freedom of speech requires an underlying culture of vibrant intellectual innovation. Intellectual privacy nurtures that innovation, protecting the engine of expression—the imagination of the human mind.

Of course, thinking for ourselves has a social component. As a number of intellectual property scholars have demonstrated, the generation of ideas frequently depends on access to the ideas of others who have come before.[86] In a free society, access to new ideas (whether we agree with them or not) requires the ability to read freely and without constraint.[87] This kind of sharing is an essential part of the exchange of ideas. It can help us to know what other people believe, and to read their ideas and watch their films – either ones they have produced themselves, or the works of others they find influential, or challenging, or pernicious. We need to be able to read freely in this sense as well.

But we also need to be able to read privately. Oversight or interference with our reading habits can curtail our willingness to read freely and to experiment with ideas that others might think deviant, laughable, or embarrassing. The freedom of intellectual exploration has been recognized in several places in American law, although under a number of different names. Most famously, in *Stanley v. Georgia*, the

[85] TIMOTHY MACKLEM, INDEPENDENCE OF MIND 36 (2006).

[86] See, e.g., Jessica Litman, *The Public Domain*, 39 EMORY L.J. 965, 965-66 (1990); JAMES BOYLE, SHAMANS, SOFTWARE, AND SPLEENS: LAW AND THE CONSTRUCTION OF THE INFORMATION ECONOMY ch.6 6 (1997); JAMES BOYLE, THE PUBLIC DOMAIN: ENCLOSING THE COMMONS OF THE MIND (Yale 2008); LAWRENCE LESSIG, FREE CULTURE (2004).

[87] E.g., Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981, 981–82 (1996); Julie E. Cohen, *DRM and Privacy*, 18 BERKELEY TECH. L.J. 575, 575 (2003).

Supreme Court held that a prosecution for the possession of obscenity in a home violated the First Amendment because of the fundamental need for privacy surrounding an individual's intellectual explorations.[88]

> Whatever may be the justifications for other statutes regulating obscenity, we do not think they reach into the privacy of one's own home. 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.[89]

Stanley dealt with a prosecution for obscenity, and involved state interference with reading habits. But the right to read requires protection from other private actors as well as the state. Federal prosecutions based on reading are rare, but the coercive effects of monitoring by our friends and acquaintances are much more common. We are constrained by peer pressure in our actions at least as much as by the state. Moreover, records collected by private parties can be sold to or subpoenaed by the government, which has shown a voracious interest in all kinds of personal information, particularly records related to the operation of the mind or political beliefs.[90] Put simply, the problem of intellectual privacy transcends the public/private divide, and this is particularly true in the context of reading.

Although the right to read has been underappreciated and under-theorized,[91] it is increasingly under threat in the modern age of networked communications and access to information. In terms of making information and ideas broadly available, the Internet has opened up new horizons of access, on a scale that is unprecedented in human history. The rise of laptops, smart phones, tablets, and electronic books means that more and more of what we read is being mediated by electronic technologies. But these technologies have a potential dark side: while they open up new opportunities to read and interact with new ideas, they

[88] 394 U.S. 557 (1969)

[89] Id. at 565.

[90] Richards, *Intellectual Privacy*, supra note 6, at 427-28 (providing examples).

[91] A preliminary discussion of this idea can be found in Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981, 981–82 (1996) and Julie E. Cohen, *DRM and Privacy*, 18 BERKELEY TECH. L.J. 575, 575 (2003). Cohen develops her ideas in COHEN, THE NETWORKED SELF, supra note 6.

also create records of reading habits and intellectual explorations. The collection and sharing of social reading data makes those explorations public. And the act or threat of publication drives us to the mainstream.

Perhaps even worse, it turns us from discoverers into self-advertisers, risks a switch from engaging in real discovery and self-exploration to curating our intellectual habits to fit the hive mindset of current style. We might be willing to accept this if we're talking about the cut of jeans, colors of nail polish, or even kinds of music, but when it comes to reading, thinking, and believing, we risk losing our individuality to the tyranny of majoritarian preferences. To the tyranny of the social.

B. Librarians and Intellectual Freedom

If intellectual freedom requires both privacy of reading and free reading of the work of others, how should we strike the balance between privacy and access for the digital age? A compelling answer to this question comes from a somewhat unlikely source – the work of librarians.

It might seem odd at first to rest a theory of intellectual freedom for the digital age in librarians. After all, librarians aren't often thought of as particularly imaginative or innovative. But this stereotype is wrong. Librarians are our first and oldest information professionals, with special expertise in the issues intellectual records raise. Librarians have been struggling with the problems of reading records for centuries, as custodians of books and the records of who has been reading them.[92] Article 11 of the 1939 Code of Ethics for Librarians maintained that "it is the librarian's obligation to treat as confidential any private information obtained through contact with library patrons."[93] The current version of the Code states that "[w]e protect each library user's right to privacy and confidentiality with respect to information sought or received and resources consulted."[94]

---

[92] 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, 802 (2006).

[93] Code of Ethics for Librarians, Art. 11 (1939), quoted in American Library Association, *Privacy: An Interpretation of the Library Bill of Rights*, in THE AMERICAN LIBRARY ASSOCIATION INTELLECTUAL FREEDOM MANUAL 192 (7th ed. 2002) (hereinafter "INTELLECTUAL FREEDOM MANUAL").

[94] Code of Ethics for Librarians, Art. 3 (1995), available at www.ala.org/alaorg/oif/ethics.html.

Modern library theory about intellectual freedom and the right to read is embodied in the American Library Association ("ALA")'s 1948 "Library Bill of Rights" and in a series of official interpretations of that document spanning the period from World War II to the Patriot Act.[95] The Library Bill of Rights itself was the culmination of decades of work by librarians as they attempted to understand the purpose of their profession and the duties of information stewardship that came along with it.[96] Although earlier librarians may have thought of themselves as moral guardians of society with a special responsibility to "elevate" the lower classes,[97] the Library Bill of Rights represents a very different understanding of the relationship between librarian and patron. The original 1948 Library Bill of Rights and its subsequent amended versions conceive of the library as a means of fostering the intellectual freedom of library patrons.[98] Affirming that "all libraries are forums for information and ideas, the Library Bill of Rights consists of six principles to guide the provision of library services:

> I. Books and other library resources should be provided for the interest, information, and enlightenment of all people of the community the library serves. Materials should not be excluded because of the origin, background, or views of those contributing to their creation.
>
> II. Libraries should provide materials and information presenting all points of view on current and historical issues. Materials should not be proscribed or removed because of partisan or doctrinal disapproval.
>
> III. Libraries should challenge censorship in the fulfillment of their responsibility to provide information and enlightenment.
>
> IV. Libraries should cooperate with all persons and groups concerned with resisting abridgment of free expression and free access to ideas.

---

[95] See Judith F. Krug, The ALA and Intellectual Freedom: An Overview, in INTELLECTUAL FREEDOM MANUAL, supra note 93, at 14-20.

[96] Id.

[97] EVELYN GELLER, FORBIDDEN BOOKS IN AMERICAN PUBLIC LIBRARIES, 1876–1939: A STUDY IN CULTURAL CHANGE, at xv (1984); WAYNE A. WIEGAND, THE POLITICS OF AN EMERGING PROFESSION: THE AMERICAN LIBRARY ASSOCIATION 1876–1917, at 9–10 (1986).

[98] INTELLECTUAL FREEDOM MANUAL, supra note 95, at 25-27.

> V. A person's right to use a library should not be denied or abridged because of origin, age, background, or views.
>
> VI. Libraries that make exhibit spaces and meeting rooms available to the public they serve should make such facilities available on an equitable basis, regardless of the beliefs or affiliations of individuals or groups requesting their use.[99]

Recognizing that the Library Bill of Rights is a living document, the ALA and its Office of Intellectual Freedom (OIF) have clarified its meaning through a series of "Interpretations." These explain the application of the ALA's commitment to intellectual freedom, the right to read, and free access to ideas in particular contexts, such as library usage, censorship, governmental intimidation, and equality of access.[100]

Most important for present purposes are a series of ALA policies on the privacy and confidentiality of library records. The distinction between the two is significant. Patron "privacy" in the words of several influential librarians, "is the right to engage in open inquiry without having the subject of one's inquiry scrutinized by others." But recognizing that an important part of the librarian's professional mission is to help patrons find information, the policies also recognize the value of "confidentiality," the keeping of such information private on the patron's behalf.[101] In 1971, the ALA adopted a "Policy on Confidentiality of Library Records."[102] As amended today, the policy requires that libraries adopt a policy stating that circulation records identifying patrons by name are confidential, advise all librarians that records shall only be released pursuant to a valid court order, and that such court orders shall be resisted up to the limits of the law.[103]

---

[99] Library Bill of Rights, Adopted June 19, 1939, by the ALA Council; amended October 14, 1944; June 18, 1948; February 2, 1961; June 27, 1967; January 23, 1980; inclusion of "age" reaffirmed January 23, 1996, available at http://web1.ala.org/ala/issuesadvocacy/intfreedom/librarybill/index.cfm.

[100] INTELLECTUAL FREEDOM MANUAL, supra note 93, at vi-vii.

[101] Candace Morgan, Deborah Caldwell-Stone, & Daniel Mach, *Privacy and Confidentiality in Libraries*, in INTELLECTUAL FREEDOM MANUAL, supra note 93, at 402.

[102] American Library Association, *Policy on Confidentiality of Library Records*, adopted Jan. 20, 1971.

[103] American Library Association, *Policy on Confidentiality of Library Records*, adopted Jan. 20, 1971, as amended July 2, 1986.

The ALA's fullest exploration of reader privacy and its relationship to intellectual freedom is its 2002 document "Privacy: An Interpretation of the Library Bill of Rights."[104] Recognizing at the outset that "privacy is essential to the exercise of free speech, free thought, and free association," the Interpretation makes two separate commitments to user privacy and confidentiality. The first commitment deals with the rights of library users. This interprets Article IV of the Library Bill of Rights' commitment to free access as giving library users as much control as possible to select, access, and use library material. It asserts that "[l]ack of privacy and confidentiality has a chilling effect on users' choices. All users have a right to be free from any unreasonable intrusion into or surveillance of their lawful library use."[105] Moreover, the policy maintains that patrons have the right to use a library without any inferences made between their reading habits and their behavior.[106]

The policy's second commitment deals with the responsibilities of librarians and library users to each other. It declares that because "[t]he library profession has a long-standing commitment to an ethic of facilitating, not monitoring, access to information," libraries must take care to collect only that personal information that is necessary to the provision of mission-critical library services. Moreover, the commitment to intellectual freedom means that everyone in a library, whether librarian or fellow user "has a responsibility to maintain an environment respectful and protective of the privacy of all users."[107]

Beyond the Library Bill of Rights, the ALA has engaged in advocacy to protect reader privacy. A 2009 position paper declared that "the impulse to be curious, to read, and to learn is essential for the health of our democracy and our economy."[108] The paper also recognized the critical relationship between intellectual privacy and political freedom. It explained that "[t]he freedom to read and receive ideas anonymously is at

[104] American Library Association, *Privacy: An Interpretation of the Library Bill of Rights*, available in INTELLECTUAL FREEDOM MANUAL, supra note 93, at 190.

[105] Id. at 192-93.

[106] Id. at 193.

[107] Id. at 193-94

[108] AMERICAN LIBRARY ASSOCIATION, RALLYING AMERICANS TO DEFEND THEIR RIGHTS IN A DIGITAL AGE: A POSITION PAPER ON INFORMATION PRIVACY, 4, 5 http://www.privacyrevolution.org/images/uploads/ALA_privacy_position_paper_MARo9_2.pdf/.

the heart of individual liberty in a democracy. It ensures a person's right to gain knowledge and form opinions according to his or her own conscience. It is the foundation for self-determination and meaningful participation in the political process."[109] Crucially, the OIF also articulated the importance of privacy to avoid the chilling effect on reading caused by surveillance:

> When the right to privacy is eroded or stripped away, people are more likely to abandon or curtail their exploration of unpopular and unorthodox points of view. This chilling effect puts the intellectual development of our citizenry at risk. The very character of the American mind, which is premised on open inquiry, is thereby robbed of the free flow of ideas that makes innovation possible.[110]

The OIF has made this argument through more direct advocacy activities as well. In response to section 215 of the Patriot Act, which allowed secret access to library records, the ALA worked with the American Booksellers' Association and other groups to found the Campaign for Reader Privacy and try to overturn the law.[111] More recently, the OIF has sponsored "Choose Privacy Week," designated for May 2012, an initiative designed to give "individuals the resources to think critically and make more informed decisions about their privacy."[112]

Intellectual privacy theory and library ethics reveal the values behind confidentiality rules for reader records. They illuminate the reasons why they should be treated specially and also some of the dangers of disclosure. They also reveal a central paradox of reader privacy: we need intellectual privacy to make up our minds, but we often need the assistance and recommendations of others as part of this process, be they friends, librarians, or search engines. The norms of librarians suggest one successful and proven solution to this paradox.

---

[109] Id.

[110] Id.

[111] http://www.readerprivacy.org/

[112] *Vision*, Privacyrevolution.org, http://www.privacyrevolution.org/index.php/our-story/vision/ (last visited Feb. 24. 2012).

III. THE DANGERS OF "FRICTIONLESS SHARING"

If the norms of librarians represent one approach to the paradox of reader privacy, the model of "social reading" described in part I.B represents another. Frictionless sharing is the idea that a one-time consent by a consumer using a web site or application can be used to allow the automatic disclosure of their reader records to their friends or followers on social networks. According to proponents of frictionless sharing, we benefit from learning what our friends are reading, watching, or listening to. By sharing our intellectual interests with our friends automatically, we are all better off, as we all discover more content that we like. We learn what they are reading, and they learn what we are reading. Along these lines, the argument goes, the law should make it easier for us to share, rather than harder. Besides, if we don't want to share, we don't have to.[113]

This simple argument has a seductive appeal, but it is deeply flawed. Sharing is of course important to the exchange of ideas. Very often, what social networks call "sharing," the law would call "free speech." But just because some sharing can be good, it doesn't follow that all sharing is good. How we share matters. There are just three problems with making frictionless sharing of reader records our default: Frictionless sharing isn't frictionless, it's not really sharing, and it's corrosive of intellectual privacy and intellectual freedom.

A. Frictionless Sharing Isn't Frictionless

What is "frictionless sharing" really? Putting its branding to one side for a moment, it's really no more than the idea that we can (and should) change the default setting of our reader records from a confidentiality default to a disclosure default. It thus changes our relationship to our reader records. Under a confidentiality default, our records are private until we consciously decide to make them public. A shift to frictionless sharing means that our reader records are published without our doing anything.

Sharing becomes much easier under such a regime because it becomes automatic. We don't have to designate that we want to share a

[113] For arguments along these lines, see Susan Crawford, *The Pandora's Box of Privacy*, WIRED, Feb. 2, 2012; Jules Polonetsky & Christopher Wolf, *Viewers Should Be Able to Share Their Playlists*, ROLL CALL, Nov. 29, 2011.

movie we've seen or a book we've read – it's done for us by the software. But what if we watch a movie or read an article that we don't want published to the world? Assuming that our social reading service allows us to opt out of sharing, we now have to go and perform that opt-out. That takes effort – friction, if you will. So frictionless sharing doesn't eliminate the friction associated with sharing of our reader records, it just shifts it from the friction required to click a "like" or "share" button to the friction required to unpublish something. Especially if we think that almost everyone will want to keep something private, this is more work for everyone. And as anyone who has tried to tweak privacy settings will know, even if such an option is available, it can be very difficult to make it work properly.[114]

Consider a real-world example from Facebook. One day in November 2011, I noticed on Facebook that one of my (male) law professor colleagues had used the Washington Post Social Reader App to read an article entitled "Porn That Women Like: Why Does It Make Men So Uncomfortable?"[115] When I asked him about it, he was horrified, as he hadn't realized that he had signed up for the social reader app, much less broadcast his embarrassing reading data to dozens if not hundreds of his professional acquaintances. (For all of Mark Zuckerberg's talk of going to the movies with our "friends," Facebook's crude definition of friendship often goes well beyond the people we'd want to see a film with.[116]) After an hour of helping my colleague delete the automatic status update, unsubscribe from the reader application, and otherwise curate his Facebook News Feed, we were able to "un-share" his reader records. But that's friction.

More generally then, the shift to a disclosure norm requires us to worry about inadvertent disclosure of things we don't want made public. Even if it doesn't deter us from exploring ideas our friends might find

[114] See James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137, 1184-87 (2009) (collecting examples and empirical studies).

[115] J. Bryan Louder, *Porn That Women Like: Why Does It Make Men So Uncomfortable?*, SLATE.COM, Nov. 17, 2011, available at hwww.slate.com/blogs/xx_factor/2011/11/17/porn_that_women_like_why_does_it_make_men_so_uncomfortable_.html. It's also available on the social reader app, of course, but I wouldn't advise you get it there. Neither would my colleague.

[116] Cf. Zadie Smith, *Generation Why?*, NEW YORK REVIEW OF BOOKS, Nov. 25, 2010 (making a similar point).

objectionable, foolish, or deviant, it still means we have to go to the effort of curating our public reader profiles to keep those records private. As one technology blogger puts it aptly, "frictionless sharing isn't frictionless after all. All it does is trade the small friction of having to choose what to share with the large friction of having to think about whether what you're about to do will be shared."[117]

B. Frictionless Sharing Isn't Sharing

A second problem with frictionless sharing is that it isn't really sharing, at least not in the way that we might understand sharing of reader records as a valuable activity. Recall the role sharing plays in the theory of intellectual privacy – we want to make up our minds about something, and we want to know what other people think about it. In an offline world, we might seek out our close confidantes such as our friends, romantic partners, mentors, teachers, or a librarian. We would ask them not only whether they've read something about the topic we're interested in, but also if it was any good. This kind of sharing has two qualities – it is *conscious* rather than merely passive, and it is *recommended* rather than merely read.

Now consider exploration in an online space with social sharing, but not frictionless sharing. This is the world of blogs, of the Facebook "Like" and Google "+1" buttons – a world of recommendations, but a world of conscious recommendations. We know that our friend Danielle likes (or dislikes) an essay on cyber-bullying because she blogs about it. We know that our friend Greg likes a band because he tells us on Facebook. We know that our friend Jonathan finds an article on cloud computing insightful because he links to it on his Twitter feed. These recommendations – these *conscious* recommendations – are valuable not just because our friends have read them, but because they have read them, thought about them, and chosen to publish them for us, possibly even with commentary.

Frictionless sharing just isn't as good. It isn't conscious, and it comes with no recommendations. It's merely streamed out by software, a data exhaust pipe of personal information devoid of context or real content. Because it isn't conscious, it isn't really sharing. If conscious

[117] Nick Bradbury, *The Friction in Frictionless Sharing*, January 30, 2012, available at nick.typepad.com/blog/2012/01/the-friction-in-frictionless-sharing.html.

sharing is like getting reference help in the library, frictionless sharing is like wandering the stacks unaided by any point of reference. Sometimes we might discover something we like in the stacks – something we didn't know we wanted. But probably not. And anyway, we're not really in a library; we're just in someone else's datastream.

C. Frictionless Sharing Undermines Intellectual Privacy

A defender of frictionless sharing might argue at this point that it might not matter that frictionless sharing is inconvenient and useless. If people want to share their data effortlessly, they should be able to do it. If some people want to waive their intellectual privacy, then so be it, as it won't affect those of us who care about these things.[118] Let's call this argument "Live and Let Share." This is another seductive argument for frictionless sharing, but it is unpersuasive for three reasons.

The first problem with the "Live and Let Share" argument has to do with how the decisions we make now about social reading will affect us over the long term. Proponents of "Live and Let Share" sometimes create the impression that such a regime is natural and inevitable. It is not. It is merely one possible end state that our future Internet or Internets may reach.

As we think in policy terms about the rise of social networks, we must not forget that we are, as a society, setting important default rules for the future. Right now, our technological, social, and legal choices are open. We can create the social Internet in a variety of different ways because it hasn't been created yet. But this window will not stay open forever. The defaults we select now as a society will become harder to change over time. We will create the social Internet, it will take a specific form, and it will then be harder to change. In *The Master Switch*, Tim Wu shows how twentieth century information empires, including the telegraph, telephones, cable television, and radio followed a common pattern of destabilizing birth, maturity, stagnation, and replacement by a new destabilizing technology.[119] Wu calls this process "The Cycle," and he shows how again and again new information networks start out in a state

[118] In fact, they have made this argument. E.g., Jules Polonetsky & Christopher Wolf, *Viewers Should Be Able to Share Their Playlists*, ROLL CALL, Nov. 29, 2011.

[119] TIM WU, THE MASTER SWITCH: THE RISE AND FALL OF INFORMATION EMPIRES (2011).

of openness and uncertainty, only for information empires to rise as powerful entities exert control over the technology. In Wu's story, new technologies disrupt existing information empires, only to become empires themselves, which then get disrupted by new technologies.[120] But the form these empires take matter, not just in terms of who makes money and who doesn't, but because industrial structure affects the exercise of fundamental values like free speech and privacy more than we often realize.[121] Wu's main argument is one about the shape information empires take, but there is another point which is equally important. When a new information network is in its early stages, early tentative decisions about the structure of the network tend to become fixed principles. This is true of decisions in privacy law as well. Daniel Solove and I have shown elsewhere how decisions by William Prosser about the basic structure of the four "privacy torts" have proven remarkably resistant to change, even when those privacy torts became ineffective over time.[122] But before industrial or legal norms ossify, there is often a window of opportunity when the basic defaults of the system are up for grabs.

We are in such a window of opportunity for reader privacy right now. We are living through what media historian Paul Starr calls a "constitutive moment" – a contingent choice in the development of a new media.[123] The communications network we are creating right now is not destined to take any particular, natural form. It will instead be the product of the numerous social, cultural, economic, technological and legal choices we are making right now, often without realizing it. The decisions we make – legal, technological, and industrial – over the next few years will set the general defaults for how and when this information will flow over the second-generation Internet we are all in the process of creating.[124] Our decisions today about how easily we want reader records to flow will thus affect us all for a very long time.

[120] Id. at 10-12.

[121] Id. at 121-23.

[122] Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CALIF. L. REV. 1997 (2010).

[123] PAUL STARR, THE CREATION OF THE MEDIA 3 (2004).

[124] JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET: AND HOW TO STOP IT 199 (2008).

A second problem with the "Live and Let Share Argument" is that under a regime of disclosure norms, there is no guarantee that users who wish to exercise their right to intellectual privacy will be given a meaningful choice. For example, what if a service like Facebook required frictionless sharing as a condition of using the service? The "choice" in this instance would be the choice to not use the service. Over time, such a choice may become as empty as the "choice" not to use the Internet has become today.

The public debate on frictionless sharing has taken place to date in the context of movies and music. Very few people seem irritated, for example, that Spotify shares our musical preferences with our friends, and those that do are mostly annoyed by the volume of sharing rather than its sensitivity.[125] From this perspective, we might wonder why we can't share the films we watch on Netflix if we can share the music we listen to on Spotify.[126]

These kinds of arguments miss the point – the intellectual privacy issues intertwined with the collection and disclosure of reader records. Consider instead if we were talking about disclosing other kinds of intellectual or reader records – your web browsing, or Google searches, or email. Would we want to engineer our social Internet by placing disclosure rules on these kinds of personal information? Certainly not. Even advocates of radical sharing concede that web browsing, search, and email should be private. Jeff Jarvis, an outspoken academic evangelists for sharing, disclosure and "living in public" concedes that despite his love of "living in public," even he "wouldn't particularly want you watching when I surf the web."[127] In part, the problem is that our reading habits might be taken out of context – we might draw the wrong conclusions from the fact that someone has read an article (such as the article on male porn stars discussed earlier).[128] But just as severe a problem is that we might draw the right conclusions – that someone is reading articles we

[125] E.g., John Paul Titlow, *Why I Shut Off Facebook's Spotify Integration, ReadWriteWeb*, Nov. 22, 2011, available at http://www.readwriteweb.com/archives/why_i_shut_off_facebooks_spotify_integration.php.

[126] See Susan Crawford, *The Pandora's Box of Privacy*, WIRED, Feb. 2, 2012; Jules Polonetsky & Christopher Wolf, *Viewers Should Be Able to Share Their Playlists*, ROLL CALL, Nov. 29, 2011. (making this argument).

[127] JARVIS, supra note 5, at 40.

[128] Cf. id. (making a similar point).

don't like because they are flirting with or even embracing ideas we find dangerous or offensive. Intellectual privacy theory rests on the idea that ideas matter, but that we should all be free to engage with ideas – any ideas – on our own terms and with meaningful guarantees that we will not be watched or interfered with. Our commitment to intellectual freedom demands no less.

There is no guarantee that a system of social reading premised on the value of frictionless sharing would increase intellectual freedom. Under a set of frictionless disclosure rules, web sites, search engines, e-readers, and mobile apps could all offer "free" services in exchange for our reader information. Indeed, some might argue that this is exactly the kind of Internet that is being created while we are dazzled by Angry Birds and the social features of the new web.

But we need not make this choice. We do not have to allow consumer information transactions to take place on these terms, and we should require the option of confidentiality rules for particularly important kinds of reader data.[129] We can certainly disagree about what this category contains. (Music, for example, might be a borderline case.) But we need to think about this category, about what's in it, and about why protecting it matters. Intellectual privacy theory provides useful answers to these questions.

The third problem with the "Live and Let Share" argument has to do with the nature of choice. Even if we agree that we should provide the option of a confidentiality rule, why can't we just set the defaults to require people to opt in to confidentiality and opt out of sharing? The problem is that default rules are sticky, and they shape behavior. If we are concerned about the automatic over-sharing of reader records, we should place the default rules in places that protect intellectual privacy and which require conscious, rather than automatic, sharing. In their book *Nudge*, Richard Thaler and Cass Sunstein demonstrate repeatedly that people generally take the default settings in many areas of life, even when there is an opportunity to choose a different option.[130] For example, the default placement of healthy food in a cafeteria or supermarket affects the buying

[129] Neil M. Richards, *The Information Privacy Law Project*, 94 GEO. L. J. 1087, 1137-38 (2006); see also Richards & Solove, supra note 7.

[130] Richard H. Thaler and Cass R. Sunstein, *Nudge: Improving Decisions About Health, Wealth, and Happiness* (2008).

patterns (and health) of consumers.[131] If we place the healthy food in places people look first, they buy and then eat more healthily. But if we put the junk food there, the same people buy more of that instead. Thaler and Sunstein call this insight "choice architecture."[132] They find again and again in the social science literature evidence of how the design of systems is not neutral, but has a real effect on behavior, which can be manipulated by the way choices are structured. Other law and economics scholars have made similar findings, even for parties who are much more sophisticated than consumers accepting "click-wrapped" privacy defaults.[133]

Technology companies understand this point and act on it. If a company wants to encourage disclosure of personal information, it will set the default to share. Even when there is an opportunity to opt out, more people will share than if the default were confidentiality with an opportunity to choose sharing. We see this business practice illustrated by the way social readers are set up. For example, the default setting for many social readers is to display a default of sharing to some large public as the default. Facebook's default privacy settings similarly default to share one's information to the world. The stickiness of default rules thus undermines the idea of completely free choice in a consumer context. Default settings matter. Invocation of simple choice-based mantras like the "Live and Let Share" argument doesn't change that fact. Put simply, when the stakes are as important as intellectual privacy and the default is a disclosure rule, even a simple opt-out from frictionless sharing is not enough.

IV. PROTECTING READER PRIVACY THROUGH LAW

Let's recap the argument so far. First, our law treats reader records haphazardly under two conflicting types of rules, confidentiality and disclosure. Second, reader records deserve special protection under law because they implicate our intellectual privacy, an insight that librarians have understood for decades. Third, the rising spectre of frictionless sharing and automatic social reading threatens our

[131] Id. at 1-2.

[132] Id. at 3.

[133] Omri Ben-Shahar & John A. E. Pottow, *On The Stickiness Of Default Rules*, 33 FLA. STATE L. REV. 651 (2006); Brett McDonald, *Sticky Defaults and Altering Rules in Corporate Law*, 60 S.M.U.L. Rev. 383 (2007).

intellectual privacy and intellectual freedom. We should therefore protect reader records better and more coherently than we do currently. We should extend confidentiality rules like the VPPA and the California Reader Act rather than making disclosure easier.

But even if you're not convinced of this strong form of my argument, there is a weaker form: Reader records raise special issues and are deserving of special treatment by our law. We currently have a haphazard approach to reader records, and the rise of social media is making the inconsistent approach we take to these records even more of a problem.

In either instance, changes to the laws regulating the sharing of reader records are inevitable. But what form should the law take, and what principles should guide its reform? How should the law think about reader records? This Part suggests four concrete principles that should guide the future development of the law, norms, and code governing reader records.[134]

My proposals draw on the idea, familiar to data privacy lawyers, of codes of fair information practices.[135] These are schemes that regulate the collection, use, and disclosure of certain kinds of information. The original fair information practices were drawn up by the U.S. government in the early 1970s to deal with the problem of government databases.[136] The idea became highly influential and has been used as the basis for data privacy laws around the world, including the EU Directive that governs all data processing in Europe.[137] It is also an idea that retains vitality – in February 2012, President Obama called for a "Privacy Bill of Rights," an

[134] Cyberlaw and privacy scholars have long recognized the regulatory effect of social norms and computer code in addition to traditional legal rules. See LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (2000); Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553 (1998); Joel R. Reidenberg, *Rules of the Road for Global Electronic Highways: Merging Trade and Technical Paradigms*, 6 HARV. J.L. & TECH. 287, 296 (1993).

[135] For an overview of such codes, see Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149, 1166-68 (2005).

[136] Paul M. Schwartz, *Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy-Control, and Fair Information Practices*, 2000 WISC. L. REV. 743, 779.

[137] Council Directive 95/46, art. 8, 1995 O.J. (L 281) 38 (EC).

enforceable code of conduct for consumer data directly modeled on the fair information practices tradition.[138]

Most scholars agree that there is a global consensus on the key fair information practices. Joel Reidenberg summarizes this consensus as having four elements: (1) *data quality standards*, which ensure that data is acquired legitimately and is used in a manner consistent with the purpose for which it was acquired; (2) *transparency standards*, such as giving individuals meaningful notice regarding how their information is being used; (3) *special protections for sensitive data,* such as requiring affirmative consent before such data may be used or disclosed; and (4) *enforcement* of the standards.[139] My proposals draw on this tradition and extend it to reader records.

A. Reader Records Are Sensitive Data

As librarians have recognized for decades, and as intellectual privacy theory makes clear, reader records are special. Privacy protections for the records of our intellectual activities are particularly important so that we can explore ideas and information freely. Technology has opened up new ways to explore and read, but it has also created more numerous and more detailed records of our reading. How should we deal with such important personal information?

The idea of fair information principles perspective can supply an answer: reader records should be recognized as a new category of "sensitive data." Sensitive data is personal information that is particularly important, susceptible to abuse, or data of the kind which would cause people great harm if it were disclosed or misused.[140] As noted above, when sensitive data is involved, stronger procedural protections are warranted. Although there is no single definition of sensitive data, the EU Data Protection Directive understands the term as including, for example, "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the

[138] See Executive Office of the President, *Consumer Data Privacy In A Networked World: A Framework For Protecting Privacy And Promoting Innovation*, 9 (Feb. 23,. 2012), available at http://www.whitehouse.gov/sites/default/files/email-files/privacy_white _paper.pdf (acknowledging the importance of fair information practices).

[139] Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 514–15 (1995).

[140] Reidenberg, supra note 139, at 514-15.

processing of data concerning health or sex life."[141] Reader records can of course be related to politics, philosophy, health or sex. We could squeeze them under this definition easily. But the cleanest way to treat reader records is to recognize them as a separate category of sensitive data, deserving separate and heightened protection on their own terms and for their own special reasons. This insight seems to be implicit in laws like the VPPA and California Reader Privacy Act – the idea that because disclosure of reader records can be harmful, reading records deserve heightened procedural protection compared to other kinds of data.

Reasonable minds can certainly disagree on how broadly we should define "reader records," but intellectual privacy theory helps us identify what matters and what doesn't. At a minimum the definition should include records of electronic books and articles bought, rented, or read; films and videos watched; and internet searches. 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, before we are ready to speak our ideas consciously and intentionally to the public. Music might seem to fall outside the core of this definition, though audio recordings would not – a book on tape is still a book for purposes of intellectual privacy. Work would need to be done in defining the scope of any reader privacy bill, but there are effective models that currently exist – the California Reader Privacy Act, other state reader privacy acts, and library confidentiality laws. One could imagine a statute making Internet searches confidential by treating search engine data like library records, for instance. We often think of the Internet as a library; maybe we should start treating it like one.

B. Reader Privacy Requires Real Notice

From the idea that reader records are sensitive data, other conclusions would follow from a fair information practices perspective. For most online contracts, the law requires merely *notice* of the proposed terms and the *choice* to reject them if they are unacceptable. As then-Judge Sotomayor put it, the test is whether consumers "had reasonable notice of and manifested assent to" the collection of their information.[142] But what do these standards mean? For ordinary kinds of personal data,

[141] Council Directive 95/46, art. 8, 1995 O.J. (L 281) 38 (EC).

[142] Specht v. Netscape Comms. Corp., 309 F.3d 17, 28 (2d Cir. 2002). For purposes of full disclosure, the author represented Netscape in this case.

these standards might be relatively minimal – the fine print on a privacy policy link that is rarely if ever read. Courts tend to uphold these sorts of terms most of the time.[143]

But when we are dealing with sensitive information, the balance changes. When we accept privacy terms for our reader records, we are entering into a contract for sensitive data, which requires a higher standard of notice. Constructive notice might suffice, for example, when we are agreeing to let a gaming web site place a cookie on our computer to identify us when we return, but when we are accepting a regime of reader records disclosure, actual notice should be required. Given the sensitivity of reader records and their importance to our intellectual freedom, holders of reader records should be required to let their clients actually know the terms on which reader records will be stored.

Scholars working at the intersection of law and computer science have suggested novel ways how such notice can occur. Woodrow Hartzog has shown how the design of websites and other electronic interfaces affects the actual level of consumer notice.[144] Other scholars like Ryan Calo and Alessandro Acquisti have shown that certain design features and context affect our awareness that people are disclosing information to us, as well as the circumstances in which we are more likely to disclose.[145] Numerous studies have shown that software that creates the sense that another human being is present (e.g., through the use of anthropomorphic avatars, human faces, eyeballs, etc.) creates a medically measurable visceral response on the part of the user of being watched.[146] Such "visceral notice" could be used creatively to provide meaningful notice at a level warranted by the sensitivity of reader records. If you see the website watching you, you might realize you're not alone, and act accordingly.

---

[143] See Hartzog, supra note 54, at 1642-45 (collecting cases).

[144] Id. at 1650-70.

[145] *See* Victoria Groom & M. Ryan Calo, *User Experience As A Form Of Privacy Notice: An Experimental Study* (forthcoming 2011) (on file with author); M. Ryan Calo, *Against Notice Skepticism in Privacy (And Elsewhere)*, 87 NOTRE DAME L. REV. (Issue #2) (forthcoming Feb. 2012); Alessandro Acquisti & George Lowenstein, *Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information*, 37 J. OF CONSUMER RES. 858, 868 (2011).

[146] M. Ryan Calo, *People Can Be So Fake: A New Dimension to Privacy and Technology Scholarship*, 114 PENN ST. L. REV. 809, 849 (2010); Calo, *Against Notice Skepticism*, *supra* note 145.

C. Reader Privacy Requires Conscious Choice

Similarly, the sensitivity of reader records means that the choice to disclose them must be conscious rather than frictionless. For the reasons explained by intellectual privacy theory and understood by librarians, the risk of disclosure places a chilling effect when we read and research new things. We can protect these processes by giving readers the confidence that their reading patterns will only be disclosed when they choose to disclose them to others. We don't want readers to wonder whether their sensitive information will be disclosed inadvertently or because of poor privacy protections under a disclosure rule. We should give them meaningful guarantees that reader records will be confidential unless they consciously choose otherwise. We should give them what William McGeveran has called "genuine consent,"[147] rather than the fiction imposed by the failure to object or adjust hidden privacy setting. We should go beyond "choice" as passive failure to object to choice as a form of conscious control.

Conscious choice need not be difficult. For the reasons explained in Part I, sharing is an important part how we receive information and ideas, and how we come to learn. But how we share those ideas matters. Unrestricted or poorly-controlled publication of our reading habits can chill our reading, and it can provide less valuable information to others. We should put individual readers in control of how they share. We should encourage a conscious "Hey, read this!" rather than an automatic "He read this."

Even when we consciously choose to share, it should be easy for us to change our minds. The VPPA Bill that recently failed in the Senate would have made it easy for Netflix to turn on the data faucet and share the movies we watched, but it said nothing about whether or how that faucet could be turned off.[148] If we allow easy or even automatic sharing of certain kinds of reader records, we must also ensure that the legal regime that allows us to "opt in" to sharing also allows us to opt out easily if we change our minds.

[147] William McGeveran, *Disclosure, Endorsement, and Identity in Social Marketing*, 2009 U. ILL. L. REV. 1105.

[148] See H.R. 2471, 112th Cong. (2011).

D. The Importance of Confidentiality

Most important in guiding our treatment of reader records, we need to recognize the importance of the idea of confidentiality to this particular problem of privacy. Our records are no longer held by institutions like bookstores and libraries, protected by an overlapping matrix of institutional norms and confidentiality rules. When our records began to be held by video stores in the 1980s, these new creatures lacked the ethical sense of librarians and independent bookstores like Kramerbooks. They also lacked the legal constraint of a confidentiality rule. When the *Washington City Paper* obtained Robert Bork's records, this became clear. We can thus understand the VPPA as the extension of a confidentiality rule to protect intellectual records in a new context.

To hear the advocates of sharing, it's an all-or-nothing proposition. Our information is on or off, open or shut, stored in our heart of hearts or shouted across the rooftops. But that's silly, and it's inconsistent with how we've always lived, whether in the eighteenth century or the twenty-first. We've always shared information, and we've always recognized intermediate states of sharing, somewhere between things being known only to us, and being known to the entire world. Sometimes the law or the rules of etiquette don't intervene to stop the spreading further. When the press is told newsworthy information, it can publish the information, privacy claims notwithstanding.[149]

But sometimes law or norms do intervene, depending upon the nature of the relationship and the sensitivity of the information. Many of these are professional relationships, such as those we have with our priests, accountants, lawyers, doctors, psychologists, or librarians. What these professional custodians of information have in common reveals the two sides of sharing. On the one hand, sometimes we need to share sensitive information with others so that they can help us, whether it's to lower our taxes, remove a nasty rash, find books on a particular topic, or stay out of prison. In order for us to have the benefit of their advice (another kind of shared information), we need to be completely frank and open with them, so we put rules or norms in place that they will keep our information confidential. This is the *information-sharing function of confidentiality*. We share a little, and we get something good in return,

[149] Neil M. Richards, *The Limits of Tort Privacy*, 9 J. TELECOMM. & HIGH TECH. L. 357 (2011).

along with the promise that our sensitive information will go no further. Paradoxically, then, confidentiality can encourage sharing that is conscious *and* valuable.

There's no reason that these tested ideas of confidentiality and information-sharing can't be adapted to the digital environment, the way we adapted them to video stores 25 years ago. We still care about sensitive information, and we're creating a lot more of it every time we use our phones, tablets, or computers. This trend is only going to continue as the "internet of things" networks the computers in our household appliances, cars, and the electrical "smart grid."[150] We might well conclude that much of this information should be shared freely. But we also need to remember that not all information is the same. There are certain categories of sensitive data that we should protect more than others, that warrant confidentiality. Reader records are one such category. And confidentiality rules are a clear solution to the problem that frictionless sharing presents to our intellectual privacy.

Just as we recognized in the past that certain professionals were fiduciaries of our information, so too in the Age of Information should we expand our definition of information fiduciaries to include bookstores, search engines, ISPs, and providers of physical and streamed video. The duties of confidentiality we place on these fiduciaries need not be iron-clad. As discussed earlier, sharing of our intellectual preferences is important, and there may be separate instances where we decide that records should be made public after legal process. But when we place exceptions to the confidentiality of our intellectual records, we should do so in ways that empower the individual to make conscious choices about when to share and when not to. Intellectual privacy demands no less.

CONCLUSION

Ultimately, issues of reader privacy and sharing come down to a value choice. When faced with the choice on where to pitch the default somewhere between total secrecy and total disclosure, we need to decide what values are at stake and how best to advance them in practice. We've heard from the advocates of "sharing" and "social," but I have tried to maintain that in this debate there is a place for the individual, the

[150] Scott R. Peppet, *Unraveling Privacy: The Personal Prospectus & The Threat of a Full Disclosure Future*, 105 Nw. U. L. Rev., at ms.2-5 (forthcoming 2012).

eccentric, and the contemplative as well. When it comes to the issue of how to regulate our reading records, a world of automatic, constant disclosure should give us pause. Sharing of this kind of information can be valuable to companies and individuals, but it must take place in a way that respects intellectual privacy. It must take place in a way that gives individuals conscious and meaningful choice over what they share and when and how they share it.

Social networking technologies have matured to the point where many new things are possible. But we face a moment of decision. The choice between sharing and privacy is not foreordained; there are many decisions we must make about how our reader records can flow, and under what terms. But the choices we make today will be sticky. They will have lasting consequences for the kind of networked society we will build, and whether there is a place in that society for intellectual privacy and for solitary, contemplative, and idiosyncratic reading.

To return to the idea with which this Article started, sharing is cool. But coolness today is not coolness tomorrow, and coolness alone is an insufficient basis on which to engineer our public and private selves. Sometimes coolness is not enough.