The Structural Irrelevance of Privacy: A Provocation

John Buschman
The Structural Irrelevance of Privacy: A Provocation

John Buschman

ABSTRACT
A recent library institute on privacy noted that “privacy . . . is crucial to free speech, freedom of thought, and equal access to information,” now challenged by the “mass collection of . . . data,” and that “our profession has been slow to respond [to this] threat.” The failure is broader: a theoretical approach to privacy unmoored from contemporary reality. It is the context of what has been known for some time that reveals the shortcomings of privacy theories. This article will review where our current theories come from: the broader field of information ethics and its intellectual framing of privacy issues. The article will review theoretical and historical insights that should inform our ideas about what privacy is and when it is effectively absent or invaded. These insights provide a much more informative context for democratic values, concluding with recommendations to blend the two traditions and move privacy forward.

A recent call for papers (CFP) on privacy for a library institute states that “privacy . . . is crucial to free speech, freedom of thought, and equal access to information”—a set of professional “core values” challenged by “the digital nature of today’s information sources . . . allow[ing] for mass collection of . . . data”—and that “our profession has been slow to respond [to this] threat to our mission” (http://librarywriting.blogspot.com/2014/11/call-for-proposals-privacy-and.html). The argument here is that the failure is broader than that: not as a professional failure on the part of librarianship and/or library and information science (LIS) but rather in the form of a blinkered theoretical approach that produces concepts of privacy that can seem unmoored from contemporary reality. The CFP’s reference to the ability to collect data in the mass is of course the key, but that is by no means a new insight, and it is the context of what else has been known for some time that reveals the shortcomings of privacy theories. To make this case, this article will look at the context from which our current theories about privacy spring: the broader field of information ethics and its intellectual framing of privacy issues. The article will then move to a constellation of historical and theoretical insights that could have—and now should—inform our ideas about what privacy is and, more importantly, when it is effectively absent or invaded. Although they can be dealt

1. For brevity and consistency the term “LIS” will be used to refer to the various areas of librarianship, library schools, and libraries—and their literatures.
with only in brief here, these insights provide a much more informative context for the democratic values that the CFP seeks to explore and extend. The article will conclude with some preliminary conclusions to move theories of privacy and the practices to protect it in LIS forward.

The Development of Information Ethics

Our task begins with acknowledging an axiom: privacy, intellectual freedom, democracy, and information ethics are deeply interconnected. The CFP quoted earlier simply echoes longstanding American Library Association policy in asserting the “essential” link between privacy and the exercise of First Amendment rights and harkens back to the 1939 Library Bill of Rights (the name itself is a self-conscious association with democratic constitutional rights) to assert an “ethical imperative . . . to guard against impediments to open inquiry. . . . When users recognize or fear that their privacy or confidentiality is compromised, true freedom of inquiry no longer exists” (http://www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy). In terms of historical development, modern concepts of privacy were coterminous with the development of democracy—from social contract theories (and the property and other related rights one gave up or held on to when consenting to join government and society) up to jurisprudential definitions of a right of privacy in the nineteenth and twentieth centuries. In other words, for very many years privacy was, in theoretical terms, predominantly political in nature, focused on what government could and could not do and know about the person and the citizen while still protecting liberty and remaining democratic. However, in the twentieth century the governmental, economic, productive, and bureaucratic imperatives of fighting two global wars gave rise to the military-industrial complex, and a sociopolitical shift took place in the process: “The modern business corporation [now] displayed most of the distinguishing marks of a political order” (Wolin 2004, 374–75). In other words, politics and the state were no longer necessarily the exclusive sites where fundamental public issues such as community or privacy were worked out. They shifted instead to technological and productive (economic) settings. In those settings over the course of the past 40 years or so, a growing governmental bias toward the information industry and informational property rights developed hand-in-hand with corporate practices of monitoring work activity and ever more intense harvesting and use of data on customers—dramatically altering the terrain of privacy (Zuboff 1993; Harris, Hannah, and Harris 1998; Leiss, Kline, and Jhally 2000; Winter 2009; Buschman 2012). These developments were coterminous with a theoretical shift toward computer and information ethics: that philosophically inflected word

2. There is an enormous literature that further explores and establishes these relationships (see, for example, Frické, Mathiesen, and Fallis 2000; Rootes 2003; Budd 2006; Pressley 2013; Richards and Cornwell 2013; Rubel 2014).

3. Again, there is an enormous literature on this (see, for example, Benhabib 1992; Wolin 2004, 252; Moore and Unsworth 2005; Roessler 2006; Alfino 2013; Moore 2013; Pressley 2013; Richards and Cornwell 2013).
came to characterize working theories of privacy developed to deal with the issues that arose in those very same technological, economic, and organizational contexts (Bynum 2008; Carbo and Smith 2008; Bynum 2010).

As a result, information ethics has come to cast privacy concerns as a series of philosophical issues as opposed to its former political and public framing. As Rafael Capurro puts it, “a self-referential process ethics is an unending quest on explicit and implicit use of the moral code, that is to say of respect or disrespect, with regard to individual and social communication. In other words, ethics observes the ways we communicate with each other as moral persons and the ways this moral identity is understood” (in Carbo and Smith 2008, 1111). Along with the acknowledged founders and leaders of the field—Luciano Floridi and Capurro—many information ethics theorists are “philosopher[s] of information first and then a contributor to information ethics as a natural development of [their] philosophical explorations” (Sturges 2009, 245). This is not meant to denigrate their accomplishments, but it will become clear in the next section that those perspectives have shaped contemporary theoretical constructions of privacy. In short, privacy-theory-as-shaped-by-information-ethics has become much more depoliticized and preoccupied with philosophical concerns (e.g., analytical precision in definitions and context, individual moral and ethical states, and foundational issues of the reasoning process).

The Effects on Privacy Theory

This thesis can best be illustrated with some examples from the literature:

- Privacy has been theorized as a fundamental moral and ethical good, or conversely, a right—drawing fully on the rich philosophical traditions of debate on the priority of the good over the right and vice versa from Plato to John Rawls (Alfino and Mayes 2003; Moore and Unsworth 2005).
- Privacy theories have been rooted in the utilitarian philosophy of John Stuart Mill, in Immanuel Kant’s moral duty, and in epistemology and normative theory (Rootes 2003; Fallis 2007; Himma 2007).
- Floridi posits an “information ontology [of the] individual as constituted by her information” (in Ess 2009, 163) and that “right and wrong . . . essentially refer to what is better or worse for the infosphere” (in Doyle 2010, 164)—a macroethical construction meant to expand the “moral circle” in much the same way that concepts of the intrinsic value of life were expanded by the philosophical idea of the biosphere; privacy is thus “ontological friction” restricting the flow of information for him (Doyle 2010, 173, 164–65; Floridi 2010).
- Privacy as a primary good philosophically implicates intellectual property and “access relation[s]”: restrictions for owners of the property versus freedom for speakers, think-
ers, and inquirers and control of information deemed private (Mathiesen 2004). Thus, privacy is extended “from the conditions needed for reasoning [and agency] to the conditions needed to . . . control information about [oneself]” (Alfino and Mayes 2003, 11).

- Privacy is mediated through the philosophical concept of “non-human moral agents” (Siponen 2004, 282), conducted through both networks and the governing capacities of information algorithms that can—and do—take and make meaning from one’s participation amid enormous traffic (Van den Hoven 2010, 63–64; Stahl 2011). In the process, terms such as “moral,” “agent,” and “meaning” have been philosophically extended beyond humans.

- There are persistent debates over the analytical precision and philosophical legitimacy of core concepts that surround privacy: the distinctions drawn between ethics, information ethics, and computer ethics; the distinctions between ethics and moral and normative reasoning; and the definition of information (Alfino and Mayes 2003; Mathiesen 2004; Himma 2007).

The entanglement of information ethics and LIS meant that the LIS literature exhibited similar themes (e.g., Kant, moral theory, and individual autonomy) in its founding debate. The themes of that original debate bear a close relationship to the issues that still preoccupy the information ethics literature in LIS cited here. The philosophy-inflected influence of information ethics tends to narrow the focus to the epiphenomena of LIS and shapes privacy considerations—“Who should have access to what information” in the library’s organizational context?—and then plumbs the particulars in depth (Fallis 2007, 24). The list of issues in the CFP noted at the beginning of this article illustrates this limitation as well: how we talk to students, faculty and administrators about privacy and what we can learn from them about its future, the Library Code of Ethics and its relevance, assessment, individual student privacy, and lesson plans for teaching students about privacy.

This focus on an individual’s workaday epiphenomena is reflected at a deeper level in contemporary information ethics theory. Helen Nissenbaum posits “contextual integrity” as a definition of privacy: appropriateness in a plurality of contexts governs who should have access to what information—what should be private and when (Hull, Lipford, and Latulipe 2011, 290–91). What you tell your accountant is very different from what you tell a coworker, and some information is meant to be shared (coworker), some shared within bounds (accountant), and some not at all (psychologist). At the same time, she has argued for a concept of “privacy in public”—the ability to be out and about with a reasonable degree of assurance

---

4. Robert Hauptman raised initial ethical concerns in the mid-1970s about individual librarians’ approach to answering questions with potentially lethal results being mixed up with professional values of privacy and neutrality; Hauptman was answered a decade later by Robert Dowd, who queried reference librarians about free-basing cocaine; his analysis argued that librarians should not infringe upon his privacy and autonomy (Rootes 2003).
of privacy and who should have access to any information that has been collected (Bynum 2008). Adam D. Moore (2011) posits privacy as “what we have no business knowing” and illustrates his point with an item of clothing covering an unsightly scar: to snatch that away would be a violation of a person’s right to privacy and right to determine who sees/knows about that part of his or her body. As different as these approaches are, what they have in common is the basic question “Who should have access to what information?” Privacy is frequently limited to an individual’s information and a specific institutional context of control over sharing, up to the intensely specific and personal issue of an item of clothing.

Again, this is not to dismiss these concerns, but as Julie Cohen (2012–2013, 1906) has noted, “privacy’s bad reputation has deep roots in privacy theory [and its] roots in the tradition of liberal individualism, which supplies . . . the conventional understanding of the self that privacy is thought to protect. [That] self . . . is not the autonomous, precultural island that the . . . model presumes”—it has been largely undermined by new philosophical approaches and the technological data collection and manipulation capacities that the CFP noted. Mark Alfino (2015) characterizes the limitations: privacy theory has “modeled moral autonomy at the individual level. . . . But intellectual freedom is a fundamentally social phenomenon,” and even individual cognition is now thought to be social in nature—and by extension, so is privacy. In combination with the recognition that privacy is no longer framed in political (democratic, public) terms, these two approaches point us toward the tradition of social inquiry that blends philosophical and “empirical orientation[s] in practical social theory and practical social inquiry [to] promot[e] democratic norms,” recognizing that the “political sphere [is] increasingly functionalized to the market and its reified social relationships” (Bohman 2015) in the era of Big Data. The broader contexts and theory that follow will flesh that idea out.

Privacy: Facts on the Ground

Despite the preoccupations noted, information ethics theory hasn’t entirely stuck its head in the sand when it comes to privacy and its broader contexts. Capurro early on argued that these issues needed policy and action by information professionals in their public roles and organizational settings (Capurro 1985; Carbo and Smith 2008), and Floridi situates microethics—issues such as privacy—in relationship to his macroethics of information ontology and the infosphere: “It shifts the locus of a violation of privacy away from conditions tied to an agent’s personal rights involving control and ownership . . . to conditions affecting the information environment” (Tavani 2010, 267). As noted, there is a constellation of perspectives that situate privacy well beyond the context that information ethics provides. While the implications of each cannot be explored in full here, an overview will reveal compelling reasons to reconsider privacy beyond the constructions currently prevalent.

To begin, this is not a new issue. In the massive buildup to World War II, men had to register for the draft, and prior to that, Social Security issued unique ID numbers that enabled
the convenience of pay-as-you-go payroll taxes—both sea changes in the ability to track the citizen population on a national scale; civilian conscription to steer men and women into sectors of the war workforce to alleviate labor shortages was also seriously considered (Goodwin 1995, 331–32; 487–88). Twenty years later, in the mid-1960s, there was a logical extension of these trends in a federal plan to consolidate all collected data under one government-issued individual identification number, provoking cries of “big brother” (Bynum 2008). Our current concerns are actually decades old—a point made at the time (Bynum 2010, 29–30).

Second, as the site of working through privacy issues has moved from politics to organizational, technological, and economic settings, the site of privacy’s invasion has moved to those settings as well. Under novel political and jurisprudential theories concerning the changed relationship between democracy, prosperity, and terrorism post-9/11, the revelations of Edward Snowden and Chelsea Manning have demonstrated the existence of massive government spying, but these have direct parallels in the data gathering of Apple, Microsoft, Amazon, Verizon, Google, and Facebook. “Information about yourself is like currency” (Murphy 2014), and “surveillance is the business model of the internet” (Schneier in Gillmor 2014). Most corporate data gathering and tracking practices, if conducted by government, would provoke even more protest, and we in fact know that these companies cooperated with the efforts of the National Security Administration (NSA) (Chen 2011; Hull et al. 2011; Lee 2013; Tiessen and Elmer 2013; Fister 2014; Gillmor 2014; LaFrance 2014; Vijayan 2014; Savage 2015).

Third, scale is important: we worry about privacy and library vendors, systems, and networks (and rightly so), but the three largest publishers (Reed Elsevier, Pearson, and Thomson Reuters) have less than 9% of the revenue of the three largest technology companies noted earlier (Apple, Google, and Microsoft). This actually significantly overstates the case: the big publishers’ net income is about 5.5% that of the three top technology companies, and their brand value is minuscule compared to that of the technology companies—and libraries represent only a sliver of the Reed/Pearson/Thomson markets. The products we provide to our publics are slivers of slivers of slivers in economic terms, and the importance of the privacy of their use is proportionally diminished as a concern (Caldwell-Stone 2012). Witness the recent news story of Pearson’s monitoring of social media and the resulting deletion of posts if the company thought examination questions and answers were being passed along (Brown 2015).5

5. This point was made repeatedly at the recent Information Ethics Roundtable conference (http://ier2015.org/schedule).


7. On the Liblicense list there was, dispiritingly, the normal parsing of “legitimate” business interests played off against privacy in this particular case. See the discussion string at http://listserv.crl.edu/wa.exe?A2=ind1503&L=LIBLICENSE-L&D=0&F=50131 and http://listserv.crl.edu/wa.exe?A2=LIBLICENSE-L&D=65366D1502.
Jo Ann Oravec (2015) gives an overview of the thoroughgoing lack of privacy in the depth and breadth of surveillance now present in the academic context.

Fourth, within this context, “our sense of agency [and] our sense that what we think about public policy matters” has changed (Fister 2014). The sheer scale of economic influence on policy, the sheer scale of technological storage and sifting capacity, and the sheer scale of what government and corporations can afford to do to track and identify markets and threats has swamped a sense of self and privacy (Cohen 2012–2013) constructed by information ethics. In the course of these developments, we perhaps have changed: “Digital playgrounds made us think that privacy was over, an archaic notion, an out-of-fashion luxury good we could no longer afford if we want to be part of the 21st century”—an attitude wholeheartedly encouraged governmentally in the name of safety and economically in the name of convenience (Madden 2012; Fister 2014; Murphy 2014). The result is an asymmetry: technology and its marketing messages have penetrated every single space (homes, classrooms, churches), knitting together a global consumer experience, yet at the same time the human and environmental destruction engendered by the neoliberal consumer economy—up to and including contemporary forms of wage slavery that power low-cost consumption—goes missing: it remains strangely private (Miller 2006, 2014). LIS experiences its own not-dissimilar asymmetries: we fuss about privacy invasions in the monitoring of e-books or of our networks and patron records (Caldwell-Stone 2012; Jaeger, Bertot, and Gorham 2013) while leaders simultaneously urge us to “leave our moral compass at the door” on issues such as privacy (Bolt 2014) and exploit marketing methods up to and including patron records to shape services and collections and “save” libraries (Estabrook 1996; Koonitz, Gupta, and Webber 2006). Time and again experts and blue-ribbon panels find that libraries and librarians—and the privacy and equity that they embody—are valued as part of community, but at the same time leaders continually declare the need to “rebrand” and “reenvision” the institution (Bolt 2014). Perhaps it is time to plumb this context a bit more.

The Broader Theoretical Context of Privacy

Manuel Castells (1996, 32) early on saw that “the flows of images/sounds/messages created . . . specialized audiovisual universes [intertwined with] worldwide networks of information and entertainment.” In such an environment “the way you communicate is [to] fashion a ‘package of stimuli’ that will ‘resonate’ with what is already and continuously communicated. The search for the ‘responsive chord’ . . . crowd[s] out all other impulses” (Rosen 1992, 23)—essentially the postmodern condition as mediated technologically. In turn, postmodern thinkers responded to this context by promoting “experiments in human living” in the cause of liberation, decentering authoritative concepts of human good, and encouraging contest among so-

---

8. Library leadership often simply seeks to ape these trends and their implications (Buschman 2003).
cial arrangements (Mara 2003, 739–40). The results challenged the primacy of science as an overarching explanatory paradigm, introduced a strong sense of cultural relativism, and revealed the power of the random and the constructed nature of experience and knowledge (Dervin 1994; Mara 2003). The lack of privacy—others’ possession of uncomfortable or private facts in this new environment—changed: it is no longer about what should be private or even its facticity; it is now a contest over how the information is known and understood, an interpretive battle.

Examples are not hard to find. Targets of right-wing media find that their words, deeds, history, and purported vast and harmful influence are fitted to storyline needs for current plots to destroy American culture and the economy—sometimes decades after the “facts” (Piven 2011). Bruno Latour (2004, 226–27) identified the apotheosis of the interweaving of these two trends in the “artificially maintained scientific controversy” around global warming: the postmodern unveiling of the scientific construction of facts has been co-opted by the political right to posit an “illusion of prejudices . . . hidden behind . . . objective statements” on the science of global warming; the “bad guys can use any weapon at hand, naturalized facts when it suits them and social construction when it suits them.” Postmodern conditions have redefined fundamental concepts, making clusters of values such as privacy, freedom of information, intellectual freedom, and rational inquiry in the library and educational settings largely irrelevant (Postman 1988; 1992, 48). We are a very long way from any intelligible idea of privacy when it consists of a battle-and-barter system over meaning situated within a resonant flow of messages.

This context deeply affects democratic politics—and thus the ability to repoliticize the issue of privacy. As Cohen (2012–2013, 1913) put it in her discussion of privacy, “Networked information technologies mediate our experiences . . . in ways directly related to both the practice . . . and the capacity for citizenship, and so they configure citizens [perhaps] even more directly than [our] institutions do. . . . The capacity for democratic self-government is defined in part by what those technologies . . . allow, and by exactly how they allow it.” Put simply, contemporary politics is postmodern: “Now fundamentally dependent upon the skilled manipulation of messages and symbols,” interpretations of political “personalities are . . . often decisive” for politics and the direction of the state (Castells 1996, 32–33). Jürgen Habermas (1970, 96; 1989, 171–72) identified this state of affairs as “systematically distorted communication”: beliefs and values “maintain their legitimacy despite the fact that they could

9. Frances Piven’s situation (Glenn Beck highlighting an article she cowrote in 1966) brings to mind Faulkner’s famous quotation—“The past is never dead. It’s not even past”—and the motivations behind the European Commission’s “right to be forgotten” (http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten) as a new version of privacy. More fundamentally, basic facts are the object of persistent misrepresentations and misperceptions, such as the responsibility for the 9/11 bombings (Shenkman 2008).

not be validated if subjected to rational discourse” (Schroyer in Held 1980, 256). Latour’s global warming illustration demonstrates this concept well. We inhabit an environment of “an increasing substitution of images for words, [the] inter-mingling of categories such as advertising, politics, entertainment [and] information. . . . The banal coalesces with the unreal [and] the highly personalized, consumeristically polished bizarre,” as Habermas (1985, 97) puts it. Thus, it is in the illusion of democracy—consumer choice, public opinion, and the rituals of voting and elections under conditions of systematically distorted communication—where “critical discussion . . . tends to give way to ‘exchanges about tastes and preferences’” that are utilized “as marketable forms for the public services provided in a culture of consumers” (Habermas 1989, 171). The idea of consumer choice is actively conflated with citizenship, and thus “the state has to ‘address’ its citizens like consumers,” making politics an exchange of symbols, “a stylized show,” and a spectacle of “managed integration” (Habermas 1989, 195, 206–7). Privacy is best understood within an environment that obviates democratic political solutions to address these concerns.

**Conclusion**

The historical and theoretical contexts presented here point to issues far more troubling than snatching an article of clothing, access to information gathered in a library database or gathered about an individual moving about in public (camera surveillance), or privacy as a moral right or an ethical duty of a given profession or institution. The past 75 years of technological and economic history indicate that privacy is no longer primarily a political issue with traditional political solutions at the same time that the structures of information gathering and information correlating have advanced exponentially. There is a seemingly tacit agreement that the information will be gathered in the first place: Google or Amazon or the NSA will track purchase and travel and communication and viewing and searching patterns. The capacity to invade privacy (as we have conceived it) by the state and corporations is now inarguable. When (not if) the (private) information is known, its meaning is a matter of framing and spin. Information ethics is a diverse endeavor, but this picture fundamentally challenges privacy theory as the field has constructed it. With the locus of privacy having shifted to economic and technological sites—that is, in the realms of corporate policy—traditional democratic political solutions seem also to be out of reach. I write this conclusion the morning after watching *Citizenfour* with its chilling, dispiriting implications. This framework is no doubt less airtight than presented here, and it is in the gaps that a discussion of marrying information ethics’ ideas about privacy to these insights needs to begin. Hannah Arendt (1972, 4) reminds us that the “political virtues” have never really been edifying: for as long as there have been politics, secrecy and deception (and invasions of privacy, I would add) have been prominent, but we have the freedom to think about facts and their facticity (such as the existence of privacy) and affirm or deny or change them collectively. Privacy has perhaps
always and ever been under threat of being swamped by the communal, the social, the organizational, and the technological. As we have theorized it, privacy is too private: our thinking about it must account for the “social and historical options which face rational persons” in the situations in which they actually find themselves (Mara 1985, 1054–55).

Privacy and autonomy and agency are individual and collective, and their maintenance in classrooms and libraries through an understanding of what can be done in those spaces is important: “stocks of knowledge” can be used collectively to reveal historical agency and assert change for the better (Den Heyer 2006, 91). Privacy so conceived might be productively married with Ulrich Beck’s (2007) ideas about another form of agency: “the power to . . . refuse to make a purchase [that] cannot be delimited.” Consumption blurs borders, and the exotica of the world is “globally cannibalized, re-staged and consumed as products for mass markets”; in the process a “public that knows no frontiers” is created—both through media and through uncontrollable migrations—creating a “new reflexivity” (Beck 2004, 151). This takes the form of a “risk-sensitive public [who are] unpredictable consumers, amongst whom a chain reaction can be triggered by the merest hint of plausible evidence” of lead in paint on children’s toys, genetically modified food, the shakiness of an investment, diseased beef, a new and highly communicable serious disease, etc.; thus, “incalculable consumer markets . . . can destroy billions of dollars of investment overnight” (Beck 2001, 269–70). In other words, neoliberal economic globalism has worked, and produced a global and cosmopolitan public responsive to risks and highly interconnected.

This suggests a practical point of entry. LIS could pursue a form of collective privacy protections—backed by tort law because it is built into standard contracts negotiated collectively. LIS attempts collective solutions for cost savings through group purchasing (http://nerl.org/about, http://www.valenj.org/about/overview), through usage data for electronic resources (http://www.niso.org/workrooms/sushi), and in standard fair-contract language (http://nerl.org/working-nerl). The field also attempts to shift the balance of power in copyright (http://creativecommons.org, https://openaccess.commons.gc.cuny.edu) and in making the hurdles to desirable and enforceable contract provisions and language simpler to enact in legal terms (http://www.niso.org/workrooms/seru). Additionally, easy-to-implement resources to assist in the protection of privacy (http://academicworks.cuny.edu/lacuny_conf_2015/7) can be as much a feature of LIS work as directories of open-access journals. Corporate information vendors respond to risks and market demands—that is what they do. Privacy as a collective goal pursued collectively would look very much like a variation on these existing initiatives.

11. The progress of marriage equality or the current debates over police treatment of African American men or symbols of the Confederacy are potent examples.

12. Consumption represents about 70% of the US economy, for instance, and is the engine of most advanced economies (https://www.stlouisfed.org/publications/regional-economist/january-2012/dont-expect-consumer-spending-to-be-the-engine-of-economic-growth-it-once-was).
tapping into the risk-sensitive nature of both users concerned about privacy and the vendors
in protecting their markets—at least as a beginning.

Habermas (1987, 20) posits that there are smaller public spheres of rational inquiry “grounded
in something more stable than just the content of particular ideas [and] anchored . . . in the
scientific process itself.” By science Habermas means something more like the pragmatists’
“community of investigators” keeping alive the “productive power of discursive disputes [and
rational] arguments” (1987, 21), not the brutal rationalism that has produced NSA and Google
algorithms of control and monitoring. In other words, there are always political spaces that
can be created that sidestep some of the problems noted earlier. I am suggesting that LIS
address privacy as one such rational community. Our problems are global—migration, climate
change, economy, labor, inequality, disease, and privacy—and the solutions cannot be individ-
ual. Our notions of privacy and the agency it engenders—and where that action takes place—
need to pull up alongside these ideas. The many initiatives in the CFP initially cited are not
casual efforts—it is important to delete patron borrowing records, but such action should be
joined with a set of purposes informed by the broader theoretical understanding of privacy
outlined here as a beginning.

References
Freedom: Concepts, Cases and Theories, edited by Mark Alfino and Laura Koltutsky. Sacramento, CA: Li-
brary Juice.
at the annual meeting for the Information Ethics Roundtable, School of Library and Information
Studies, University of Wisconsin–Madison, April.
Alfino, Mark, and G. Randolph Mayes. 2003. “Reconstructing the Right to Privacy.” Social Theory and Prac-
tice 29 (1): 1–18.
.signandsight.com/features/603.html.
Benhabib, Seyla. 1992. “Models of Public Space: Hannah Arendt, the Liberal Tradition, and Jürgen Ha-
bermas.” In Habermas and the Public Sphere, edited by Craig Calhoun. Cambridge, MA: MIT Press.
Brown, Emma. 2015. “Debate over Test Security vs. Student Privacy Rages in the Age of Social Media.”


Murphy, Kate. 2014. “We Want Privacy, but Can’t Stop Sharing.” *New York Times*, October 5.


---

John Buschman: dean of university libraries, Seton Hall University. Buschman was previously associate university librarian for scholarly resources and services at Georgetown University; prior to that he was at Rider University for 19 years. He is the author of Dismantling the Public Sphere: Situating and Sustaining Libraries in the Age of the New Public Philosophy (2003). His most recent book is Libraries, Classrooms, and the Interests of Democracy: Marking the Limits of Neoliberalism (2012). He holds a BS in history and sociology and an MLS from Ball State University, an MA in American studies from St. Josephs University, and a doctor of liberal studies from Georgetown University. E-mail: john.buschman@shu.edu.