

Orienting privacy literacy toward social change

Orienting
privacy
literacy

Priya C. Kumar

*College of Information Sciences and Technology, Pennsylvania State University,
University Park, Pennsylvania, USA*

Received 9 June 2023
Revised 11 September 2023
Accepted 27 October 2023

Abstract

Purpose – This article advocates that privacy literacy research and praxis mobilize people toward changing the technological and social conditions that discipline subjects toward advancing institutional, rather than community, goals.

Design/methodology/approach – This article analyzes theory and prior work on datafication, privacy, data literacy, privacy literacy and critical literacy to provide a vision for future privacy literacy research and praxis.

Findings – This article (1) explains why privacy is a valuable rallying point around which people can resist datafication, (2) locates privacy literacy within data literacy, (3) identifies three ways that current research and praxis have conceptualized privacy literacy (i.e. as knowledge, as a process of critical thinking and as a practice of enacting information flows) and offers a shared purpose to animate privacy literacy research and praxis toward social change and (4) explains how critical literacy can help privacy literacy scholars and practitioners orient their research and praxis changing the conditions that create privacy concerns.

Originality/value – This article uniquely synthesizes existing scholarship on data literacy, privacy literacy and critical literacy to provide a vision for how privacy literacy research and praxis can go beyond improving individual understanding and toward enacting social change.

Keywords Privacy literacy, Data literacy, Critical literacy, Datafication, Surveillance capitalism, Libraries

Paper type Conceptual paper

Introduction

Data-driven systems increasingly structure societies, economies and governments (Cohen, 2019; Zuboff, 2019). Many people remain unaware of what data these systems extract and how institutions use data, raising significant questions about privacy (among other things) (Arora, 2019; Cohen, 2013). Specifically, the concern is that such systems are “dedicated to prediction but not necessarily to understanding or to advancing human material, intellectual, and political well-being” (Cohen, 2013, p. 1927). One response calls for educational efforts that increase people’s understanding, or literacy, of digital data flows (Livingstone *et al.*, 2020; Pangrazio and

© Priya C. Kumar. Published by Emerald Publishing Limited. This article is published under the Creative Commons Attribution (CC BY 4.0) licence. Anyone may reproduce, distribute, translate and create derivative works of this article (for both commercial and non-commercial purposes), subject to full attribution to the original publication and authors. The full terms of this licence may be seen at <http://creativecommons.org/licences/by/4.0/legalcode>

The author presented preliminary versions of this work at the 2022 annual conference of the Association of Internet Researchers (AoIR) and the 2019 ACM CHI workshop “Standing on the Shoulders of Giants: Exploring the Intersection of Philosophy and HCI.” The author thanks the organizers and participants of both events for their enthusiasm and feedback. The author also thanks Kelley Cotter for deepening my understanding of literacy and for generously providing comments on this manuscript. Finally, the author thank the anonymous reviewers for their feedback, which strengthened this work.



Sefton-Green, 2020). Yet literacy does not operate autonomously: teaching someone to understand something does not automatically improve their life (Graff, 2010; Street, 2003). Privacy literacy scholars and practitioners thus need to orient their research and praxis toward social change. In this article, **I advocate that privacy literacy research and praxis aim to mobilize people toward changing the technological *and* social conditions that nudge subjects toward advancing institutional, rather than community, goals.**

This is an ambitious vision. But privacy is too valuable, and datafication too formidable, to demand anything less. While some scholars suggest that privacy is too narrow a concept to successfully mobilize against data extraction (Hagendorff, 2018; Zuboff, 2019), this article demonstrates that a more thorough understanding of privacy – both its origins as a concept and its purpose in human life – renders privacy a worthy rallying point around which to resist datafication. The article begins by explaining how the conditions of datafication threaten privacy. Next, it draws on privacy scholarship and theory to argue that privacy is a valuable rallying point around which to resist datafication. It then shifts focus to literacy, articulating the connection between data literacy and privacy literacy. Following that, the article identifies three ways that scholars and practitioners have conceptualized privacy literacy and offers a shared purpose that orients privacy literacy research and praxis toward social change. Finally, the article concludes by explaining how critical literacy can help scholars and practitioners enact this vision of privacy literacy. I hope that scholars and practitioners can use this paper as a roadmap to connect with other like-minded efforts and to strengthen their own work in service of protecting the privacy necessary for shared human flourishing.

The conditions of datafication

Data-driven systems quantify human experiences – transforming them into data – and generate value from that data. This process of datafication requires extracting information from and about people, often through networked digital devices, apps and platforms, analyzing the data and using the results to make decisions and/or sell products and services. The data extracted from people becomes a form of capital, yielding wealth and/or power to those who accumulate it. Indeed, while datafication raises many important concerns related to knowledge production, it exists primarily as a vehicle for wealth production and thus must be addressed as a matter of political economy (Cohen, 2019).

Such extraction intensifies privacy concerns, but the technology companies that drive datafication downplay its extractive dimension by calling what they do with data “sharing.” Their privacy policies typically contain a section on sharing with third parties, which can include other businesses owned by the same company, service providers, advertisers and government agencies. Yet these policies lack clarity about what specific types of data companies distribute to third parties, making it difficult for people to understand where their data may flow (Kumar, 2016). Nevertheless, people must accept these legalese-laden, boilerplate terms to use the services, which gives private companies immense leeway to tilt the consumer relationship in their favor (Cohen, 2019; Richards, 2022).

In addition to perpetuating such asymmetrical relations, the rationale of accepting the terms of service turns decisions about data governance into matters of individual responsibility (did you read the terms?) and choice (do you agree?). This reflects a broader shift of privacy protection as the duty of individuals rather than governments or corporations (Baruh and Popescu, 2017; Hagendorff, 2018; Matzner *et al.*, 2016; Solove, 2013). But even when people do take steps to manage their information, such as by adjusting privacy settings, these strategies do little to curtail platforms’ access to data. Indeed, there’s not much people can do to limit data flows. Social buttons such as Facebook’s “Like” and “Share” not only funnel data from across the Web into Facebook, but they also track individuals as they traverse the Web (Gerlitz and

Helmond, 2013). Other dominant platforms, including Google, Amazon, Microsoft and Apple, use similar tracking features, and opting out is impossible (Hill and Mehrotra, 2019).

Pervasive data tracking exposes people to surveillance from corporations, governments and peers. The dangers of this surveillance include individual consequences ranging from reputational harm to imprisonment or even death, and societal ramifications such as concentrated private corporate power, eroded public governance and exacerbated inequality (Benjamin, 2019; Browne, 2015; Cohen, 2019; Crawford, 2021; Eubanks, 2017). For business scholar Shoshana Zuboff (2019), this surveillance threatens human nature by giving platforms the power to subvert free will and modify human behavior as they see fit. It portends the death of individuality and the disappearance of autonomy, leaving people with no refuge or escape from the surveillance apparatus. She contends that a concept like privacy, while “vital [...] nonetheless fall[s] short in identifying and contesting the [...] unprecedented” logic of surveillance capitalism (Zuboff, 2019, p. 14). However, I argue that the problem lies not with the insufficiency of privacy itself, but with the liberal foundations upon which privacy has been conceptualized in regulation and public discourse. To explain why this is problematic, the next section delves into privacy scholarship and theory.

Loosening privacy from its liberal foundations

Privacy is an “essentially contested” concept, containing multiple meanings that cannot be resolved into a singular core idea (Mulligan *et al.*, 2016). Privacy encompasses:

[...] (among other things), freedom of thought, control over one’s body, solitude in one’s own home, control over personal information, freedom from surveillance, protection of one’s reputation, and protection from searches and interrogation (Solove, 2008, p. 1).

Additionally, what is deemed private is historically and culturally contingent. For instance, in ancient Greece and Rome, public nudity and mixed-gender public bathing was acceptable, and in medieval Europe and colonial America, sexual relations typically occurred within earshot or view of other family members or neighbors (Solove, 2008). Privacy practices are similarly contingent. Outside of highly studied Western contexts (Arora, 2019), social media users in the Arab Gulf abide by Islamic concepts of honor, modesty and reputation when managing their online presence (Abokhodair and Vieweg, 2016). In South Asia, where families often share mobile phones, women selectively lock, delete and avoid certain information and apps to avoid patriarchal scrutiny and judgment (Sambasivan *et al.*, 2018). Such shifts across time and space indicate that privacy is not a static idea, but a dynamic practice. Privacy is something people are constantly achieving in the course of social action. Given this, efforts to support privacy may be more effective if they focus not on what privacy *is*, but what privacy *does* (Dourish and Anderson, 2006). However, approaching privacy as ongoing action (i.e. practice) rather than abstract idea (i.e. knowledge) or process (i.e. critical thinking) also requires recognizing privacy as a social, rather than individual, value.

Although scholars have long advocated for a more social understanding of privacy, most policymaking and public discourse treats privacy as individual right (Cohen, 2013; Nissenbaum, 2010; Regan, 1995; Richards, 2022; Solove, 2008, 2013). In this perspective, an individual’s privacy right must be balanced against social interests, positioning privacy as part of a zero-sum game. Such zero-sum framing ignores the collective benefit that privacy offers. When thoughts, intellectual explorations, conversations, transactions or relationships are sheltered by privacy, people can explore new, unorthodox or provocative directions with greater comfort, which in turn fosters creativity, innovation and resistance to dominant perspectives (Cohen, 2013; Richards, 2022; Solove, 2008). Privacy also enables communities who are fighting for social or political change to organize and mobilize, which explains why governments and powerful leaders embrace surveillance and the technologies that enable it (MacKinnon, 2013).

Despite the value privacy offers to individuals and societies, the increasing sophistication of data-driven technologies that facilitate government, corporate and interpersonal incursions into seemingly private actions has prompted many to label privacy as disappearing or dying (John and Peters, 2017; Richards, 2022). Communication scholars John and Peters (2017) contend that worries about the death of privacy have persisted for decades “because the modern right to privacy was born out of the conditions of its violation, not its realization” (p. 293). When lawyers Warren and Brandeis (1890) declared privacy as “the right to be let alone” (p. 193) in an article credited as the foundation of privacy law, they positioned privacy as a negative right – freedom from something, like intrusion, rather than a positive right – freedom for something, like exercising agency.

Warren and Brandeis’s (1890) conception of privacy arose from their concerns about people’s ability to use handheld cameras to (sometimes surreptitiously) document candid moments and publicize them in newspapers, potentially embarrassing upper-class society. Their right to privacy is thus inextricably tied to changing social and technological circumstances, resulting in “a concept that was broken before it was built” (John and Peters, 2017, p. 294). Broken because it only became something to value in the moment social elites felt they were losing it. Such conditions render privacy as something to defend, rather than enjoy. Privacy discourse, with its focus on protecting people’s autonomy in the face of concerns posed by new technologies, embodies this defensive posture (Masur, 2020). Yet movements for change cannot just fight *against* something. They must also stand *for* something [The Red Nation (Albuquerque, New Mexico), 2021]. Shifting privacy from a negative right to a positive right involves more than changing semantics. It also requires shifting the mindset from which we are accustomed to approaching privacy.

The conception of privacy as a right to be protected in the name of self-determination, which has dominated discourse from Warren and Brandeis (1890) through Zuboff (2019), rests on a liberal-humanist foundation of the self as an autonomous individual. However, legal theorist Julie Cohen (2013) argues:

[...] the liberal self who is the subject of privacy theory and privacy policymaking does not exist [...] [T]he self who is the real subject of privacy law and policy is socially constructed, emerging gradually from a preexisting cultural and relational substrate (p. 1904).

Rather than protect autonomy, Cohen (2013) explains that privacy “protects the situated practices of boundary management through which the capacity for self-determination develops” (p. 1904). She characterizes the space in which this capacity develops as “breathing room.”

When technologies serve surveillance functions, that is, when they encroach on that breathing room, they shape how people make sense of the world and themselves. When this surveillance is distributed across political and commercial actors, people lose the ability to pursue meaningful agendas toward human flourishing. Cohen calls this “modulation,” a form of surveillance that derives power from its ordinariness. Modulation threatens privacy because it subtly moves people to act in ways that serve institutional interests rather than social well-being (Cohen, 2013). Here, we see clear parallels between Zuboff and Cohen. But where Zuboff bemoans surveillance capitalism’s exploitation of human nature, Cohen warns that modulation alters people’s subjectivity:

Modulation is a mode of privacy invasion, but it is also a mode of knowledge production designed to produce a particular way of knowing and a mode of governance designed to produce a particular kind of subject. Its purpose is to produce tractable, predictable citizen-consumers whose preferred modes of self determination play out along predictable and profit-generating trajectories (Cohen, 2013, p. 1917).

Why do these differences matter? Zuboff believes surveillance capitalism threatens human autonomy, and her reading leaves people powerless to fight its incursion. Cohen believes modulation constructs people differently, leaving room for people to push back and resist such framings. Data and privacy literacy research and praxis offer avenues to enact such resistance. The next section explains how privacy has been conceptualized in data literacy.

Locating privacy literacy within data literacy

Several literature reviews have identified privacy as a key component of data literacy (Bhargava *et al.*, 2015; Crusoe, 2016; Gebre, 2022; Koltay, 2015; Matthews, 2016; Wolff *et al.*, 2016). In their illustration of modern literacies, Bhargava *et al.* (2015) include privacy management at the nexus of digital literacy, media literacy and data literacy. A different illustration of data literacy activities includes privacy, consent, anonymization and security and access controls as ethical considerations (Matthews, 2016). The ethical use of data often appears in definitions of data literacy (e.g. D'Ignazio and Bhargava, 2015; Prado and Marzal, 2013; Wolff *et al.*, 2016), and some argue “that data literacy is essentially an *ethical imperative*” (Bhargava *et al.*, 2015, p. 17, emphasis in original), since “data collection and retention has privacy implications” (Hautea *et al.*, 2017, p. 920). Being data literate thus involves knowing not only how to analyze datasets but also what effects such analysis has. From this perspective, data literacy entails recognizing whether “the data used has been collected without the subjects’ informed consent [...] or [is] used to discriminate against people (Bhargava *et al.*, 2015, pp. 15–16), since “no one wants to inadvertently breach the privacy of others” (Frank *et al.*, 2016, p. 6).

Some data literacy approaches center privacy by focusing on raising people’s awareness of personal data collection and use (Gebre, 2022; Pangrazio and Selwyn, 2019), while others emphasize the importance of adopting “strategies and tactics to manage and protect privacy and resist being profiled and tracked” (Pangrazio and Sefton-Green, 2020, p. 214). Privacy is also a topic of classroom-focused data literacy efforts (Matthews, 2016; Pangrazio and Cardozo-Gaibisso, 2021). Crusoe (2016) deepens the connection by defining data literacy as:

[...] the knowledge of what data are, how they are collected, analyzed, visualized and shared, and is the understanding of how data are applied for benefit or detriment, *within the cultural context of security and privacy* (p. 38, emphasis added).

Here, security and privacy are the encompassing conditions in which data literacy occurs. Below, I illustrate how privacy permeates each element of this definition.

Knowledge of what data is includes recognizing that data points are often stored or linked with identifiers like name, birthday or identification numbers (Crusoe, 2016). The privacy issue here is that such aggregation can reveal facts about people. For instance, analysis of Facebook likes can yield information about people’s political beliefs, sexual orientation and drug use (Halliday, 2013). Knowledge of how data is collected includes recognizing that data-driven technologies, including smartphones, fitness trackers, web trackers, traffic systems, payment systems, internet providers and government systems, gather data (Crusoe, 2016). Most American adults acknowledge the widespread nature of data collection and believe this poses privacy concerns related to data use and security (Auxier *et al.*, 2019).

Knowledge of how data is analyzed involves understanding that data is used to detect patterns and tell stories (Crusoe, 2016). Yet the outcomes of such analysis can be invasive, for instance, when a retail company analyzes purchase records to identify which customers are pregnant (Duhigg, 2012; Richards, 2022). Knowledge of how data is visualized involves understanding processes of converting data into visual representations that make stories and patterns easier to observe (Crusoe, 2016). This can reveal sensitive information, such as when a

fitness app's map of user activity indicated the location of US military bases (Pérez-Peña and Rosenberg, 2018). Knowledge of how data is shared involves understanding that given the value of data, it often flows from one entity to another (Crusoe, 2016). Though common, such data flows raise privacy concerns, as when the data analytics firm Cambridge Analytica harvested data from more than 50 million Facebook users and used it to target political advertising and influence elections (Rosenberg *et al.*, 2018). Understanding the benefits and costs of data use involves recognizing that data "can tell a story about us that we may not agree with, or which may paint an inaccurate picture of ourself" (Crusoe, 2016, p. 40). Such inaccuracies can have dire consequences, as when one woman's credit history was ruined by inaccurate claims that she intended to create and sell methamphetamines (Mui, 2011).

Indeed, Crusoe (2016) takes the links between data literacy and privacy as a given, explaining that:

The security and privacy of one's data is paramount[,] and one must live with the expectation that, at some point, data will be compromised. Thus, knowing which additional steps to take is simply a part of current life experience (pp. 34-35).

However, the privacy issues mentioned above cannot be rectified through individual steps. Although people can limit some data collection and sharing by adjusting privacy settings and using tracker blockers, most data collection and use lies beyond people's individual control. Meaningful privacy protection requires changes in corporate business models, legal regulation and technology design (Cohen, 2019; Hartzog, 2018; Maréchal *et al.*, 2020). I argue that privacy literacy research and praxis can play an important role in mobilizing people toward advocating for such social changes. In the following section, I explain how existing work has conceptualized privacy literacy and offer a shared purpose to guide future work.

Orienting privacy literacy as knowledge, process and practice toward social change

Scholars and practitioners have conceptualized privacy literacy in different ways, characterizing it as (1) knowledge about information flows and how to limit them, (2) a process of critical thinking about information flows and (3) a practice of enacting appropriate information flows (Kumar *et al.*, 2020). This section explains each conceptualization, defining their goals and noting the extent to which each has centered individual versus social dimensions of privacy. It concludes by proposing a shared purpose to animate privacy literacy research and praxis toward social change.

Privacy literacy as a form of knowledge

The knowledge-based conceptualization is prevalent in privacy literacy research and praxis. Here, a privacy-literate person is someone who knows *what* happens to information disclosed online and *how* to limit the spread of information (Park, 2013; Trepte *et al.*, 2015). Trepte *et al.* (2015), who developed an influential privacy literacy scale, differentiated these two components as factual/declarative knowledge and procedural knowledge, while Park (2013; Park and Jang, 2014) labeled them knowledge/awareness and behavior/skill, respectively. Both recognize that effectively managing information requires knowledge of technical features, institutional practices (i.e. of organizations collecting data as well as digital service providers), and relevant policy, law and regulation. This awareness-and-skill conceptualization of privacy literacy underpins several studies (Bartsch and Dienlin, 2016; Desimpelaere *et al.*, 2020; Epstein and Quinn, 2020; Harborth and Pape, 2020; Prince *et al.*, 2022; Sindermann *et al.*, 2021), though some focus more on the knowledge/awareness side (e.g. Morrison, 2013) and others on the skills/behavior side (e.g. Choi, 2023; Liu *et al.*, 2017).

Research advancing the knowledge-based conceptualization employs statistical analysis to make empirical claims about factors that influence privacy literacy, links between privacy concerns and privacy literacy, demographic and personality differences in privacy literacy and outcomes of privacy literacy (Bartsch and Dienlin, 2016; Baruh *et al.*, 2017; Choi, 2023; Epstein and Quinn, 2020; Harborth and Pape, 2020; Liu *et al.*, 2017; Morrison, 2013; Park, 2013; Prince *et al.*, 2022; Sindermann *et al.*, 2021). Broadly speaking, the knowledge-based conceptualization strives toward behavior change. The goal of privacy literacy here is to increase people's awareness of information flows and how to manage them such that they adopt more privacy-protective behaviors. Earlier research in the knowledge-based conceptualization saw privacy literacy as a means of rectifying the privacy paradox – the idea that although people express privacy concerns, they do not take actions to manage information flows (Bartsch and Dienlin, 2016; Baruh *et al.*, 2017; Morrison, 2013; Trepte *et al.*, 2015). More recent work sees privacy literacy as a means to combat broader social concerns such as government and corporate surveillance, data tracking, consumer profiling (Desimpelaere *et al.*, 2020; Harborth and Pape, 2020; Liu *et al.*, 2017; Prince *et al.*, 2022; Sindermann *et al.*, 2021) and digital inequality (Choi, 2023; Epstein and Quinn, 2020; Park, 2013; Park and Jang, 2014), though it largely focuses on individual action.

Some researchers have discussed the need for action beyond the individual level, such as in policymaking, legal regulation and technology and interface design (Park, 2013; Park and Jang, 2014; Prince *et al.*, 2022; Sindermann *et al.*, 2021). But these calls still serve the aim of individual behavior change because they advocate the provision of clearer information about data flows so people can take the “right” steps. For instance, Park (2013) insightfully notes that a data protection policy premised on knowledge of information flows “may be fundamentally flawed” given how few users actually understand what happens to their information (p. 232). Yet instead of advocating for new policymaking regimes to govern data, they propose future research investigate individual psychological and circumstantial factors that may affect privacy literacy. Similarly, in their introduction to a consumer research journal's special issue on privacy literacy, Langenderfer and Miyazaki (2009) note that “Because federal lawmakers have adopted [...] a hands-off approach with respect to private data collection and exchange, it has become increasingly incumbent upon individuals to take an active role in the ways they safeguard their own personal information” (p. 383). Again, the response to ineffective regulatory practices is for individuals to pick up the slack.

This reflects what scholars call a self-management approach to privacy (Baruh and Popescu, 2017; Hagendorff, 2018; Matzner *et al.*, 2016; Solove, 2013). While laudable, this approach is ineffective because it overestimates the extent to which rationality informs people's actions, disregards the complexity of privacy and its social value, and overlooks the fact that the potential harms of aggregated data collection are impossible to assess at the initial point of data collection. In contrast, Epstein and Quinn (2020) note that “[f]uture-oriented thinking about privacy should acknowledge that different privacy dimensions may require distinct policy solutions, as will different groups within society” and advocate that privacy literacy “capacity-building efforts should expand on questions of structural inequality” (p. 10). Thus, even individual-focused privacy literacy efforts must acknowledge the social determinants that influence whether and how people can manage their privacy.

Privacy literacy as a process of critical thinking

While the knowledge-based conceptualization pervades research in the fields of media and communication, psychology and business, library and information studies (LIS) largely conceptualizes privacy literacy as a process of critical thinking. This is likely due to the field's longstanding connection to information literacy. In this conceptualization, a privacy-

literate person is one who reflects on how information is used and makes a conscious decision informed by their beliefs or values (Hartman-Caverly and Chisholm, 2021; Rotman, 2009; Wissinger, 2017). Rotman (2009) outlined privacy literacy as a five-step process of understanding how information fits in social context, recognizing where information goes, realizing the privacy implications of disclosure, evaluating potential threats, and deciding how and when to disclose information, which Wissinger (2017) established as a form of critical thinking. This goes beyond the knowledge-based conceptualization by recognizing that different situations may require different kinds of responses (Pingo and Narayan, 2019). Here, privacy literacy is “a cognitive experience or thought process that takes place as information is shared” (Wissinger, 2017, p. 380).

Where research advancing the knowledge-based conceptualization focuses on measuring privacy literacy, research advancing the process-based conceptualization employs qualitative methods to understand people’s perceptions and experiences surrounding privacy literacy (Bowler *et al.*, 2017, 2019; Chi *et al.*, 2018; Chisholm and Hartman-Caverly, 2023; Hartman-Caverly and Chisholm, 2020; Jones *et al.*, 2019; Jones, Asher, *et al.*, 2020; Jones and Hinchliffe, 2023; Kumar *et al.*, 2020; Pangrazio and Cardozo-Gaibisso, 2020; Pangrazio and Selwyn, 2018; Pingo and Narayan, 2019; Stoilova *et al.*, 2020; Vitak *et al.*, 2018) and to develop interventions like educational programs, workshops and games to help people engage in critical reflection about privacy and data flows (Chisholm and Hartman-Caverly, 2022; Hartman-Caverly *et al.*, 2023; Pangrazio and Cardozo-Gaibisso, 2021; Raynes-Goldie and Allen, 2014). Here, the goal of privacy literacy is to encourage people to consider the implications of their actions and make decisions that prioritize privacy. The process-based conceptualization sees privacy literacy as a response to increased data tracking and the consequent inequities it exacerbates (Bowler *et al.*, 2017; Hartman-Caverly and Chisholm, 2021; Pangrazio and Selwyn, 2018; Pingo and Narayan, 2019; Stoilova *et al.*, 2020), as well as issues of health and well-being (Chisholm and Hartman-Caverly, 2022). LIS experts and practitioners note that librarians, given their long-standing professional commitments to protect patron privacy and support literacy and learning, can play an important role in advancing privacy literacy (Givens, 2015; Jones, Asher, *et al.*, 2020; Lowe, 2016; Wharton, 2018; Wissinger, 2017).

Publications using the process-based conceptualization initially positioned privacy literacy as a largely individual duty, with one guide stating that “[u]ltimately, in this age of extensive data mining, marketing, and diminished privacy controls, users must take responsibility for ensuring their own private information” (Givens, 2015, p. 12). More recent work has acknowledged the limits of individual action in responding to societal concerns about data-driven technologies. For instance, Hartman-Caverly and Chisholm (2021) advocate that “[r]obust privacy literacy instruction should unveil the backend processes of personal data collection and manipulation, and subject them to critical examination—to the limited extent that this is possible” (p. 147). With this in mind, they designed a privacy literacy workshop that “seek[s] to empower students with actionable information in privacy literacy instruction while honestly acknowledging individual users’ limited ability to influence [data] collection” (Hartman-Caverly *et al.*, 2023, p. 243). They presented participants with “decision-making frameworks and tools for determining their own online persona priorities, articulating areas of risk, identifying compromised and defunct digital accounts, and shredding some of their digital baggage” and facilitated a series of activities to help participants reflect on their privacy priorities and develop plans to align their digital presence with those priorities (Hartman-Caverly *et al.*, 2023, p. 244). Similarly, Kumar and Byrne (2022) offered a set of learning objectives called the 5Ds of privacy literacy to help children strengthen their privacy decision-making skills.

However, focusing on individual decision-making perpetuates the insufficient self-management approach to privacy (Baruh and Popescu, 2017; Hagendorff, 2018; Matzner *et al.*, 2016; Solove, 2013). Furthermore, children do not only want to learn more about how to manage information flows; they also want companies to improve their privacy practices (Livingstone *et al.*, 2020). Approaches to privacy literacy that center individual actions (as in the knowledge-based conceptualization) or decisions (as in the process-based conceptualization) are limited in their ability to change the conditions that create privacy concerns.

Privacy literacy as a practice of enacting information flows

While the knowledge- and process-based conceptualizations treat privacy literacy as largely cognitive, the practice-based conceptualization treats it as experiential. Here, privacy literacy is something people do. A privacy literate person is someone who acts on information in a way that aligns with the social context(s) in which they are embedded (Kumar, 2022). This conceptualization acknowledges that people's actions are influenced by social, cultural, economic, political, historical and technological forces such that they may not be fully conscious of how or why they act in a particular way. It also recognizes that practice is relational, meaning that it is shared among individuals, groups and communities (The New London Group, 1996). Thus, privacy-related change, whether in behavior, thinking or both, cannot be conceptualized as solely, or even primarily, individual action. This turn toward practice mirrors shifts in social theory more broadly (Knorr-Cetina *et al.*, 2000) as well as in literacy (Gee, 2015) and privacy specifically (Dourish and Anderson, 2006).

Within the library context, efforts like the Library Freedom Project (2023), the National Forum on Web Privacy and Web Analytics (Young *et al.*, 2019), the Licensing Privacy project (Hinchliffe, 2023) the Privacy and Ethics in Technology Working Group (Digital Library Federation, 2022), the Prioritizing Privacy project (Hinchliffe and Jones, 2019) and the Brooklyn Public Library's Data Privacy Project (2023), have convened groups, developed materials, and taken action to integrate privacy literacy into the practice of librarianship. These have included fostering communities of practice (Young *et al.*, 2019), leading educational workshops (Data Privacy Project, 2023; Library Freedom Project, 2023; Hinchliffe and Jones, 2019; Macrina and Glaser, 2014; Walker *et al.*, 2020), providing primers on specific privacy issues, such as the use of learning analytics in academic libraries (Jones, Briney, *et al.*, 2020), developing privacy-protective language for library contracts with vendors (Hinchliffe, 2023), and setting up the anonymizing Tor browser on library computers (Glaser and Macrina, 2015; Macrina, 2015; Macrina and Glaser, 2014). Beyond the library context, scholars have examined how children develop privacy literacy through participation in an online coding community (Hautea *et al.*, 2017) and co-designed privacy literacy programs with teens and organizations (Smith *et al.*, 2017) as well as with people in marginalized neighborhoods (Lewis *et al.*, 2018; Petty *et al.*, 2018). Though varied, these efforts approach privacy as something people develop while rooted in a particular community, whether professional (e.g. librarianship), hobby (e.g. coding in Scratch) or geographical (e.g. Detroit).

Overall, the practice-based conceptualization strives toward reflexive engagement. Here, the goal of privacy literacy is for communities of people to recognize the privacy issues most salient to them and to work toward addressing the issues. Like the other conceptualizations, this one responds to the rise of digital technologies that exacerbate surveillance (Macrina and Glaser, 2014; Smith *et al.*, 2017), generate vast amounts of data about people (Hautea *et al.*, 2017; Jones, Briney, *et al.*, 2020; Young *et al.*, 2020) and harm marginalized communities (Lewis *et al.*, 2018; Petty *et al.*, 2018). But it does so recognizing that datafication is not a universal experience – its

harms and gains are unevenly distributed and its privacy implications context-specific. Consequently, efforts to address datafication concerns are more likely to be successful if they are grounded in the conditions of a particular community. Of course, community-based work is immensely challenging, requiring patience, time, buy-in and money. Yet the alternative – focusing on individuals – is unlikely to result in the kind of social change needed to address the root causes of contemporary privacy concerns.

Orienting privacy literacy toward social change

The boundaries between these three conceptualizations are by no means fixed. For instance, bridging the knowledge- and process-based characterizations, [Desimpelaere et al. \(2020\)](#) explain that while their privacy literacy training for children largely focused on behavior change, such trainings should also inspire critical thinking and reflection. Melding the process- and practice-based conceptualizations, [Pangrazio and Selwyn \(2018\)](#) and [Kumar and Byrne \(2022\)](#) treat data-driven interactions as embedded in practices while advocating literacy frameworks grounded in critical thinking. [Baruh et al. \(2017\)](#) highlight the value of qualitative research on privacy decision-making and practice, noting that the often quantitative studies of privacy literacy as knowledge cannot explain why people make the privacy decisions they do and how their actions reflect their response to the contemporary information landscape. [Trepte et al. \(2015\)](#) acknowledge that people may resist privacy literacy efforts, perceiving them as paternalistic.

Indeed, critics warn that privacy literacy may unfairly turn the social responsibility of privacy protection into an individual burden that requires education, time, money at a level that few can access ([Hagendorff, 2018](#); [McDonald and Forte, 2021](#)). In that spirit, [Masur \(2020\)](#) proposes a privacy literacy model that aims to infuse a social dimension into the knowledge-based conceptualization. While efforts to integrate the three conceptualizations are valuable, unless they grapple with the fact that literacy is not an autonomous force for social good ([Graff, 2010](#); [Street, 2003](#)), they are not likely to create much change when it comes to advancing privacy in the face of datafication. Change happens when those working toward it establish a shared vision of what they strive to accomplish. In the same vein as those working in media, information and data literacy ([Jansen, 2021](#); [Livingstone et al., 2008](#)), those working in privacy literacy must ask, what is privacy literacy for?

To answer this question, I build on legal theorist Julie [Cohen's \(2013\)](#) articulation of what privacy is for and [The New London Group \(1996\)](#) agenda-setting manifesto calling for new forms of literacy in the face of social and technological change. As explained earlier, [Cohen \(2013\)](#) argued that privacy “shelters dynamic, emergent subjectivity from the efforts of commercial and government actors to render individuals and communities fixed, transparent, and predictable” (p. 1905). In short, privacy gives people the breathing room they need to become themselves ([Cohen, 2013](#)). Fights to defend privacy in the face of data extraction are declarations to protect space for human flourishing.

At the same time, [The New London Group \(1996\)](#) contends that institutions are co-opting the discourse of personal relationships (e.g. workplace as family) to advance their own, often commercial, ends, simultaneously weakening the community spaces dedicated to human flourishing. The challenge of literacy efforts is to preserve these spaces in ways that “recruit, rather than attempt to ignore and erase, the different *subjectivities*—interests, intentions, commitments, and purposes—students bring to learning” ([The New London Group, 1996](#), p. 72, emphasis in original). Where privacy provides the shelter for subjectivities to develop, literacy enables people to learn how and where to channel their subjectivities toward communal good rather than commercial gain. This requires those involved in literacy to “see themselves as active participants in social change, as learners and students who can be active designers—

makers—of social futures.” (The New London Group, 1996, p. 64). **Thus, I advocate that privacy literacy research and praxis aim to mobilize people toward changing the technological *and* social conditions that nudge subjects toward advancing institutional, rather than community, goals.**

To consider *how* privacy literacy can work toward this vision, the next section articulates connections with the commitments of critical literacy and offers suggestions about ways privacy literacy scholars and practitioners can integrate them into their research and praxis.

Aligning privacy literacy and critical literacy

Like privacy, literacy is an “essentially contested” concept whose meaning cannot be resolved into one “correct” characterization (Lankshear and Knobel, 2011). Historically, reading, writing and language development were studied as matters of psychology and linguistics (Bloome and Green, 2015; Gee, 2015; Lankshear and Knobel, 2011; Rowsell and Pahl, 2015), while the term “literacy” typically referred to nonformal education efforts meant to improve the lives of people in disadvantaged circumstances, such as unemployment, teenage pregnancy, substance abuse, mental illness or incarceration (Lankshear and Knobel, 2011). By the 1980s, scholars and practitioners were questioning this approach to literacy, both for its presumption of literacy as an autonomous force for social good and for its moralized prioritization of certain kinds of literacy practice (Graff, 2010; Street, 2003). They resisted these logics, explaining that literacy entails more than the functional skills of reading and writing text, and that developing such abilities does not inherently improve someone’s life conditions. This is because social contexts, institutional values, historical precedence and technological affordances shape what literacy is, how literacy is achieved and what literacy does in particular circumstances (Gee, 2015; Street, 2003; The New London Group, 1996). Thus, literacy is more than a cognitive process of understanding meaning; it is a dynamic, situated, social practice of shared meaning-making (Bloome and Green, 2015; Gee, 2015; Pangrazio and Sefton-Green, 2020; Rowsell and Pahl, 2015; Street, 2003).

As digital technologies have permeated contemporary society, and as scholarship has grown to acknowledge the visual, material and embodied dimensions of meaning-making, “literacy can be apprehended as an ensemble of communicative practices, and print literacies can be subsumed within a much broader meshwork of practices” (Rowsell and Pahl, 2015, p. 14). Literacy practices are embedded in “cultural frameworks and models that inform when, where, and how written language should be used” (Bloome and Green, 2015, p. 20).

Of course, such norms shift over time and space. Changing social conditions throughout the late 20th century, including transformation from modernist to postmodernist worldviews, industrial to information economies and localized to networked technologies (Coiro *et al.*, 2008; Cope and Kalantzis, 2009; Lankshear and Knobel, 2011; The New London Group, 1996), have reconfigured the boundaries between public and private realms of life (Cope and Kalantzis, 2009; The New London Group, 1996). Formerly “private” topics such as sex or trauma are more acceptable in public discourses. Furthermore, people engage with public discourse while embedded in many different communities, each with their own subcultures of meaning-making and norms around information sharing. As such, successful collaboration and sense-making requires (among other things) attending to responsibilities such as privacy (Coiro *et al.*, 2008; Mackey and Jacobson, 2011). Here, privacy signifies the ability to understand and navigate the norms and rules that implicitly and explicitly govern the appropriate flow of information (Nissenbaum, 2010; Richards, 2022). The increasingly digital mediation of so much human experience makes privacy even harder to manage. This is because the technical architecture (e.g. http vs https) and economic structures (e.g. targeted advertising business models) of many digital technologies make information available to others in a way that is often not obvious to

the people using them. Thus, achieving privacy can require conscious effort, which makes privacy an important component of literacy.

This vision of orienting privacy literacy research and praxis toward changing technological and social conditions aligns with the commitments of critical literacy, which recognizes that issues of information access and meaning-making are also issues of power (Janks, 2010). As a field of inquiry as well as a praxis, critical literacy aims to “analyze, critique, and transform the norms, rule systems, and practices governing the social fields of everyday life,” and is particularly oriented toward striving toward “social justice in marginalized and disenfranchised communities” (Luke, 2012, p. 5).

Several existing data and privacy literacy efforts ground themselves in critical literacy (e.g. Lewis *et al.*, 2018; Markham, 2019; Pangrazio and Cardozo-Gaibisso, 2021; Pangrazio and Selwyn, 2019, 2021; Petty *et al.*, 2018). For instance, drawing inspiration from the work of James Gee, Brian Street and Allan Luke, Pangrazio and Selwyn (2019) explain that “[p]ersonal data literacies should aim to build awareness of the social, political, economic and cultural implications of data, as well as cultivating the metaphorical ‘space’ to reflect critically on these processes” (p. 425). They offer a framework that “aims to support the capacity of individuals to identify and analyze [the] processes [of datafication] and then devise uses and tactics in response.” (p. 428). Markham (2019), drawing on the critical pedagogy of Paulo Freire, has developed a method of digital autoethnography through which young adults develop critical consciousness of datafication and learn how to analyze the implications of data practices in the lives of themselves and those around them. These frameworks and techniques have much to offer privacy literacy. However, they focus more on the analysis and critique dimensions of critical literacy, leaving its transformational dimension underdeveloped.

Transforming the technological and social conditions that create privacy concerns

Critically oriented privacy and data literacy efforts often presume that knowledge will empower people into action (Pangrazio and Sefton-Green, 2020), yet empirical work suggests otherwise. Privacy and data literacy projects with youth have found that while participants value the knowledge they gain and express concerns about datafication, they do not typically change their own practices or push for social or structural change (Bowler *et al.*, 2017; Pangrazio and Cardozo-Gaibisso, 2021; Pangrazio and Selwyn, 2018, 2021; Selwyn and Pangrazio, 2018). To better equip people to help transform the conditions that create privacy concerns, privacy literacy projects should explicitly link their work with specific avenues of change, for instance, via law, design, organizational policy or advocacy. These examples are illustrative, not exhaustive, as the most persuasive pathway for change will depend on each project’s context:

- *Legal changes:* As digital privacy issues have captured lawmakers’ attention, privacy literacy scholars and practitioners can explain how people can get involved in such efforts. For instance, young adults in the USA have mobilized around digital privacy and online safety issues and are lobbying federal and state lawmakers regarding specific proposed bills (Lima, 2023). Privacy literacy projects that connect with such lobbying efforts could send a powerful signal to their participants about how youth can make a difference in regulation and policymaking.
- *Design changes:* Privacy literacy scholars and practitioners can push technology design practices that center the privacy interests of those most affected by technologies. For instance, Kumar *et al.* (2023) offer guidance on how technology developers can engage with privacy theory to grapple with design tensions and use

child- and community-centered design processes to integrate privacy protections directly into technologies. Privacy literacy projects that connect with design efforts can help transform practice at the level of industry.

- *Organizational changes:* Privacy literacy scholars and practitioners can work to change organizational policies and practices to better protect the privacy of the communities they serve. For instance, the Licensing Privacy Project ([Hinchliffe, 2023](#)) has identified how data collection through library systems can harm patrons and developed a rubric that librarians can use to evaluate privacy in vendor contracts. Ultimately, the project aims to provide librarians with privacy-protective language they can incorporate into vendor contracts, transforming practice at the level of organizational relations.
- *Advocacy:* Privacy literacy scholars and practitioners can partner with digital rights organizations like the Electronic Frontier Foundation, Fight for the Future, Access Now, Privacy International, the Panoptikon Foundation, Tactical Tech, Engage Media, the Manushya Foundation, the African Digital Rights Network, Tedic, Ipanetec, and many others around the world who engage in research, activism and community-building on digital privacy issues. Such partnerships could help ground privacy literacy research and praxis in the goals of specific communities already working toward making change.

Advancing community, not institutional, goals

Since privacy and literacy are each multi-faceted concepts, scholars and practitioners must determine how privacy literacy research and praxis fit into their specific contexts. Returning to critical literacy's goal of advancing social justice for disadvantaged communities can help orient them toward community, rather than institutional, goals. For instance, the Our Data Bodies project examines how datafication affects people's ability to access public benefits and what strategies people use to protect their privacy in its wake ([Petty et al., 2018](#)). They ground their work in marginalized neighborhoods in Charlotte, North Carolina, Detroit, Michigan and Los Angeles, California, synthesizing their findings into a workbook that other community organizations can use while also providing information on local organizations pushing for change ([Lewis et al., 2018](#)). They describe their work as a combination of academic research, capacity-building and community organizing ([Petty et al., 2018](#)), integrating research and praxis to emphasize not only how datafication harms specific people, but also how those people exercise agency to resist datafication.

While the Our Data Bodies project draws on digital justice principles and the perspectives of its community members to clarify its goals ([Lewis et al., 2018](#)), privacy literacy projects can also turn to other community sources for inspiration. For instance, many library-focused projects cite the privacy commitments embedded in the American Library Association's Bill of Rights as well as guiding documents from specialized organizations like the Association of College and Research Libraries (e.g. [Hartman-Caverly and Chisholm, 2021](#)) as motivations for their work. However, privacy literacy scholars and practitioners should also be on the lookout for ways that institutional rhetoric can co-opt community goals. For instance, laws that seek to protect children's privacy can further marginalize LGBTQ or other minoritized youth ([Grace et al., 2023](#); [Lima, 2023](#)); design standards that seek to protect privacy can sidestep the core issues of datafication ([Steeves, 2022](#)); and educational institutions often perpetuate the harms of datafication ([Hillman, 2022](#); [Jones, Briney, et al., 2020](#); [Jones, Asher, et al., 2020](#); [Jones et al., 2019](#); [Jones and Hinchliffe, 2023](#)). While no privacy literacy project can mitigate all of these tensions, aligning with

specific communities can help scholars and practitioners identify and work toward concrete efforts for change.

Conclusion

As the forces of datafication intensify, this article demonstrates that privacy can be a valuable rallying point for resisting the harms of datafication. It describes how privacy literacy aligns with data literacy and identifies three ways that current research and praxis have conceptualized privacy literacy – as a form of knowledge, as a process of critical thinking and as a practice of enacting information flows. To help scholars and practitioners working within each of these conceptualizations orient their work toward the social, rather than individual, dimensions of privacy, this article has advocated that privacy literacy research and praxis aim to mobilize people toward changing the technological and social conditions that nudge subjects toward advancing institutional, rather than community, goals, and explained how the commitments of critical literacy can help privacy literacy scholars and practitioners work toward this vision.

In sum, to transform the conditions that create privacy concerns, privacy literacy research and praxis need to do more than simply illustrate or explain what the harms are. They should help people “unpack complex racial and social justice issues, [...] [and] provide pathways forward for dismantling power structures that perpetuate injustices” (Jansen, 2021, p. 9). This is a political process (Janks, 2010; Jansen, 2021; MacKinnon, 2013; Pangrazio and Sefton-Green, 2020), which may unsettle some privacy literacy scholars and practitioners. But creating a world that respects the social value of privacy requires changing the circumstances that currently undermine privacy. And change does not simply happen; it must be pushed for. As abolitionist leader Frederick Douglass (1857) noted, “[p]ower concedes nothing without a demand” (p. 22). By defining the purpose of privacy literacy, this article aims to declare what we as privacy literacy scholars and practitioners are working toward – to declare what we are standing for.

References

- Abokhodair, N. and Vieweg, S. (2016), “Privacy and social media in the context of the Arab Gulf”, *Proceedings of the 2016 ACM Conference on Designing Interactive Systems, presented at the DIS '16: Designing Interactive Systems Conference 2016*, ACM, Brisbane QLD Australia, pp. 672-683, doi: [10.1145/2901790.2901873](https://doi.org/10.1145/2901790.2901873).
- Arora, P. (2019), “Decolonizing privacy studies”, *Television and New Media*, Vol. 20 No. 4, pp. 366-378, doi: [10.1177/1527476418806092](https://doi.org/10.1177/1527476418806092).
- Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M. and Turner, E. (2019), *Americans and Privacy: Concerned, Confused and Feeling Lack of Control over Their Personal Information*, Pew Research Center, Washington, DC.
- Bartsch, M. and Dienlin, T. (2016), “Control your Facebook: an analysis of online privacy literacy”, *Computers in Human Behavior*, Vol. 56, pp. 147-154, doi: [10.1016/j.chb.2015.11.022](https://doi.org/10.1016/j.chb.2015.11.022).
- Baruh, L. and Popescu, M. (2017), “Big data analytics and the limits of privacy self-management”, *New Media and Society*, Vol. 19 No. 4, pp. 579-596, doi: [10.1177/1461444815614001](https://doi.org/10.1177/1461444815614001).
- Baruh, L., Secinti, E. and Cemalcilar, Z. (2017), “Online privacy concerns and privacy management: a meta-analytical review”, *Journal of Communication*, Vol. 67 No. 1, pp. 26-53, doi: [10.1111/jcom.12276](https://doi.org/10.1111/jcom.12276).
- Benjamin, R. (2019), *Race after Technology: Abolitionist Tools for the New Jim Code*, Polity, Medford, MA.

-
- Bhargava, R., Deahl, E., Letouzé, E., Noonan, A., Sangokoya, D. and Shoup, N. (2015), *Beyond Data Literacy: Reinventing Community Engagement and Empowerment in the Age of Data*, Data Pop Alliance.
- Bloome, D. and Green, J. (2015), "The social and linguistic turns in studying language and literacy", in Rowsell, J. and Pahl, K. (Eds), *The Routledge Handbook of Literacy Studies*, Routledge, London New York, NY, pp. 19-34.
- Bowler, L., Acker, A. and Chi, Y. (2019), "Perspectives on youth data literacy at the public library: teen services staff speak out", *The Journal of Research on Libraries and Young Adults*, Vol. 10 No. 2, pp. 1-21.
- Bowler, L., Acker, A., Jeng, W. and Chi, Y. (2017), "It lives all around us: aspects of data literacy in teen's lives", *Proceedings of the Association for Information Science and Technology*, Vol. 54 No. 1, pp. 27-35, doi: [10.1002/pra2.2017.14505401004](https://doi.org/10.1002/pra2.2017.14505401004).
- Browne, S. (2015), *Dark Matters: On the Surveillance of Blackness*, Duke University Press, Durham.
- Chi, Y., Jeng, W., Acker, A. and Bowler, L. (2018), "Affective, behavioral, and cognitive aspects of teen perspectives on personal data in social media: a model of youth data literacy", in Chowdhury, G., McLeod, J., Gillet, V. and Willett, P. (Eds), *Transforming Digital Worlds*, Springer International Publishing, Cham, Vol. 10766 pp. 442-452, doi: [10.1007/978-3-319-78105-1_49](https://doi.org/10.1007/978-3-319-78105-1_49).
- Chisholm, A. and Hartman-Caverly, S. (2022), "Privacy literacy: from doomscrolling to digital wellness", *Portal: Libraries and the Academy*, Vol. 22 No. 1, pp. 53-79, doi: [10.1353/pla.2022.0009](https://doi.org/10.1353/pla.2022.0009).
- Chisholm, A. and Hartman-Caverly, S. (2023), "Emergent privacy literacy work among teaching librarians: a qualitative study", *Proceedings of ARCL'23, presented at the ACRL 2023 Conference*, ACRL, Pittsburgh, PA, pp. 377-385, doi: [10.26207/WVMZ-A698](https://doi.org/10.26207/WVMZ-A698).
- Choi, S. (2023), "Privacy literacy on social media: its predictors and outcomes", *International Journal of Human-Computer Interaction*, Vol. 39 No. 1, pp. 217-232.
- Cohen, J.E. (2013), "What privacy is for", *Harvard Law Review*, Vol. 126, pp. 1904-1933.
- Cohen, J.E. (2019), *Between Truth and Power: The Legal Constructions of Informational Capitalism*, Oxford University Press, New York, NY.
- Coiro, J., Knobel, M., Lankshear, C. and Leu, D.J. (2008), "Central issues in new literacies and new literacies research", in Coiro, J., Knobel, M., Lankshear, C. and Leu, D.J. (Eds), *Handbook of Research on New Literacies*, Routledge Handbooks Online, London, pp. 1-21, doi: [10.4324/9781410618894.ch1](https://doi.org/10.4324/9781410618894.ch1).
- Cope, B. and Kalantzis, M. (2009), "Multiliteracies: new literacies, new learning", *Pedagogies: An International Journal*, Vol. 4 No. 3, pp. 164-195, doi: [10.1080/15544800903076044](https://doi.org/10.1080/15544800903076044).
- Crawford, K. (2021), *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*, Yale University Press, New Haven London.
- Crusoe, D. (2016), "Data literacy defined pro Populo: to read this article, please provide a little information", *The Journal of Community Informatics*, Vol. 12 No. 3, doi: [10.15353/joci.v12i3.3276](https://doi.org/10.15353/joci.v12i3.3276).
- D'Ignazio, C. and Bhargava, R. (2015), "Approaches to building big data literacy", *presented at the Bloomberg Data for Good Exchange*, New York, NY, pp. 1-6.
- Data Privacy Project (2023), "Data privacy project", available at: <https://dataprivacyproject.org/curriculum/> (accessed 9 June 2023).
- Desimpelaere, L., Hudders, L. and Van de Sompel, D. (2020), "Knowledge as a strategy for privacy protection: how a privacy literacy training affects children's online disclosure behavior", *Computers in Human Behavior*, Vol. 110, pp. 1-12, doi: [10.1016/j.chb.2020.106382](https://doi.org/10.1016/j.chb.2020.106382).
- Digital Library Federation (2022), "Privacy and ethics in technology", *DLF Wiki*, 12 January, available at: https://wiki.diglib.org/Privacy_and_Ethics_in_Technology (accessed 9 June 2023).
- Douglass, F. (1857), *Two Speeches by Frederick Douglass; One on West India Emancipation, Delivered at Canandaigua, Aug. 4th, and the Other on the Dred Scott Decision, Delivered in New York, NY, C. P. Dewey, Rochester, New York, NY.*

- Dourish, P. and Anderson, K. (2006), "Collective information practice: exploring privacy and security as social and cultural phenomena", *Human-Computer Interaction*, Vol. 21 No. 3, pp. 319-342, doi: [10.1207/s15327051hci2103_2](https://doi.org/10.1207/s15327051hci2103_2).
- Duhigg, C. (2012), "How companies learn your secrets", *The New York Times*, 16 February.
- Epstein, D. and Quinn, K. (2020), "Markers of online privacy marginalization: empirical examination of socioeconomic disparities in social media privacy attitudes, literacy, and behavior", *Social Media + Society*, Vol. 6 No. 2, pp. 1-13, doi: [10.1177/2056305120916853](https://doi.org/10.1177/2056305120916853).
- Eubanks, V. (2017), *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*, 1st ed., St. Martin's Press, New York, NY.
- Frank, M., Walker, J., Attard, J. and Tygel, A. (2016), "Data literacy – What is it and how can we make it happen?", *The Journal of Community Informatics*, Vol. 12 No. 3, doi: [10.15353/joci.v12i3.3274](https://doi.org/10.15353/joci.v12i3.3274).
- Gebre, E. (2022), "Conceptions and perspectives of data literacy in secondary education", *British Journal of Educational Technology*, Vol. 53 No. 5, pp. 1080-1095, doi: [10.1111/bjet.13246](https://doi.org/10.1111/bjet.13246).
- Gee, J.P. (2015), *The New Literacy Studies*, Routledge Handbooks Online, London, doi: [10.4324/9781315717647.ch2](https://doi.org/10.4324/9781315717647.ch2).
- Gerlitz, C. and Helmond, A. (2013), "The like economy: social buttons and the data-intensive web", *New Media and Society*, Vol. 15 No. 8, pp. 1348-1365, doi: [10.1177/1461444812472322](https://doi.org/10.1177/1461444812472322).
- Givens, C.L. (2015), *Information Privacy Fundamentals for Librarians and Information Professionals*, Rowman and Littlefield, Lanham, MD.
- Glaser, A. and Macrina, A. (2015), "How a small New Hampshire library fought government fearmongering", *Slate*, 16 September.
- Grace, T.D., Abel, C. and Salen, K. (2023), "Child-centered design in the digital world: investigating the implications of the Age-Appropriate design code for interactive digital media", *Proceedings of the 22nd Annual ACM Interaction Design and Children Conference, presented at the IDC '23: Interaction Design and Children*, ACM, Chicago IL USA, pp. 289-297, doi: [10.1145/3585088.3589370](https://doi.org/10.1145/3585088.3589370).
- Graff, H.J. (2010), "The literacy myth at thirty", *Journal of Social History*, Vol. 43 No. 3, pp. 635-661.
- Hagendorff, T. (2018), "Privacy literacy and its problems", *Journal of Information Ethics*, Vol. 27 No. 2, pp. 127-145.
- Halliday, J. (2013), "Facebook users unwittingly revealing intimate secrets, study finds", *The Guardian*, 11 March.
- Harborth, D. and Pape, S. (2020), "How privacy concerns, trust and risk beliefs, and privacy literacy influence users' intentions to use privacy-enhancing technologies: the case of Tor", *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, Vol. 51 No. 1, pp. 51-69, doi: [10.1145/3380799.3380805](https://doi.org/10.1145/3380799.3380805).
- Hartman-Caverly, S. and Chisholm, A. (2020), "Privacy literacy instruction practices in academic libraries: past, present, and possibilities", *IFLA Journal*, Vol. 46 No. 4, pp. 305-327, doi: [10.1177/0340035220956804](https://doi.org/10.1177/0340035220956804).
- Hartman-Caverly, S. and Chisholm, A. (2021), "Transforming privacy literacy instruction: from surveillance theory to teaching practice", proceedings of LOEX'21, presented at the 49th Annual LOEX Conference, LOEX, pp. 145-151.
- Hartman-Caverly, S., Chisholm, A. and Glenn, A. (2023), "Digital shred: case study of a remote privacy literacy collaboration", *College and Research Libraries*, Vol. 84 No. 2, doi: [10.5860/crl.84.2.238](https://doi.org/10.5860/crl.84.2.238).
- Hartzog, W. (2018), *Privacy's Blueprint: The Battle to Control the Design of New Technologies*, Harvard University Press, Cambridge, MA.
- Hautea, S., Dasgupta, S. and Hill, B.M. (2017), "Youth perspectives on critical data literacies", *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, ACM, New York, NY, pp. 919-930, doi: [10.1145/3025453.3025823](https://doi.org/10.1145/3025453.3025823).
- Hill, K. and Mehrotra, D. (2019), "Goodbye big Five", *Gizmodo*, February.

-
- Hillman, V. (2022), "Data privacy literacy as a subversive instrument to datafication", *International Journal of Communication*, Vol. 16, pp. 767-788.
- Hinchliffe, L.J. (2023), "Licensing privacy", available at: <https://publish.illinois.edu/licensingprivacy/> (accessed 11 September 2023).
- Hinchliffe, L.J. and Jones, K.M.L. (2019), "Prioritizing privacy: curriculum", *Prioritizing Privacy*, 3 October, available at: <https://prioritizingprivacy.org/curriculum/> (accessed 11 September 2023).
- Janks, H. (2010), *Literacy and Power*, Routledge, New York, NY.
- Jansen, F. (2021), "Critical is not political: the need to (re)politicize data literacy", *Seminar.net*, Vol. 17 No. 2, doi: [10.7577/seminar.4280](https://doi.org/10.7577/seminar.4280).
- John, N.A. and Peters, B. (2017), "Why privacy keeps dying: the trouble with talk about the end of privacy", *Information, Communication and Society*, Vol. 20 No. 2, pp. 284-298, doi: [10.1080/1369118X.2016.1167229](https://doi.org/10.1080/1369118X.2016.1167229).
- Jones, K., Briney, K., Goben, A., Salo, D., Asher, A. and Perry, M. (2020), "A comprehensive primer to library learning analytics practices, initiatives, and privacy issues", *College and Research Libraries*, Vol. 81 No. 3, doi: [10.5860/crl.81.3.570](https://doi.org/10.5860/crl.81.3.570).
- Jones, K.M.L. and Hinchliffe, L.J. (2023), "Ethical issues and learning analytics: are academic library practitioners prepared?", *The Journal of Academic Librarianship*, Vol. 49 No. 1, p. 102621, doi: [10.1016/j.acalib.2022.102621](https://doi.org/10.1016/j.acalib.2022.102621).
- Jones, K.M.L., Asher, A., Goben, A., Perry, M.R., Salo, D., Briney, K.A. and Robertshaw, M.B. (2020), "We're being tracked at all times': student perspectives of their privacy in relation to learning analytics in higher education", *Journal of the Association for Information Science and Technology*, Vol. 71 No. 9, pp. 1044-1059, doi: [10.1002/asi.24358](https://doi.org/10.1002/asi.24358).
- Jones, K.M.L., Perry, M.R., Goben, A., Asher, A., Briney, K.A., Robertshaw, M.B. and Salo, D. (2019), "'In their own words: student perspectives on privacy and library participation in learning analytics initiatives", *Recasting the Narrative: The Proceedings of the ACRL 2019 Conference, presented at the ACRL 2019*, ALA, pp. 1-13.
- Knorr-Cetina, K., Schatzki, T.R. and von Savigny, E. (Eds) (2000), *The Practice Turn in Contemporary Theory*, Routledge, New York, NY.
- Koltay, T. (2015), "Data literacy: in search of a name and identity", *Journal of Documentation*, Vol. 71 No. 2, pp. 401-415, doi: [10.1108/JD-02-2014-0026](https://doi.org/10.1108/JD-02-2014-0026).
- Kumar, P. (2016), "Privacy policies and their lack of clear disclosure regarding the life cycle of user information", *AAAI Fall Symposium Series, presented at the 2016 AAAI Fall Symposium Series*, AAAI, pp. 249-256.
- Kumar, P.C. (2022), "Toward a practice-based approach to privacy literacy", in Smits, M. (Ed.), *Information for a Better World: Shaping the Global Future*, Springer International Publishing, Cham, Vol. 13192, pp. 135-142, doi: [10.1007/978-3-030-96957-8_13](https://doi.org/10.1007/978-3-030-96957-8_13).
- Kumar, P.C. and Byrne, V.L. (2022), "The 5Ds of privacy literacy: a framework for privacy education", *Information and Learning Sciences*, Vol. 123 Nos 7/8, pp. 445-461, doi: [10.1108/ILS-02-2022-0022](https://doi.org/10.1108/ILS-02-2022-0022).
- Kumar, P.C., Subramaniam, M., Vitak, J., Clegg, T.L. and Chetty, M. (2020), "Strengthening children's privacy literacy through contextual integrity", *Media and Communication*, Vol. 8 No. 4, pp. 175-184, doi: [10.17645/mac.v8i4.3236](https://doi.org/10.17645/mac.v8i4.3236).
- Kumar, P.C., O'Connell, F., Li, L., Byrne, V.L., Chetty, M., Clegg, T.L. and Vitak, J. (2023), "Understanding research related to designing for children's privacy and security: a document analysis", *Proceedings of the 22nd Annual ACM Interaction Design and Children Conference, presented at the IDC '23: Interaction Design and Children*, ACM, Chicago IL USA, pp. 335-354, doi: [10.1145/3585088.3589375](https://doi.org/10.1145/3585088.3589375).
- Langenderfer, J. and Miyazaki, A.D. (2009), "Privacy in the information economy", *Journal of Consumer Affairs*, Vol. 43 No. 3, pp. 380-388, doi: [10.1111/j.1745-6606.2009.01152.x](https://doi.org/10.1111/j.1745-6606.2009.01152.x).
-

-
- Lankshear, C. and Knobel, M. (2011), *New Literacies: Everyday Practices and Social Learning*, 3rd ed., McGraw-Hill Open University Press, Maidenhead.
- Lewis, T., Gangadharan, S.P., Saba, M. and Petty, T. (2018), *Digital Defense Playbook: Community Power Tools for Reclaiming Data*, Our Data Bodies.
- Library Freedom Project (2023), available at: <https://libraryfreedom.org/crashcourse/> (accessed 9 June 2023).
- Lima, C. (2023), "The young activists shaking up the kids' online safety debate", Washington Post, 8 September.
- Liu, Q., Yao, M.Z., Yang, M. and Tu, C. (2017), "Predicting users' privacy boundary management strategies on Facebook", *Chinese Journal of Communication*, Vol. 10 No. 3, pp. 295-311, doi: [10.1080/17544750.2017.1279675](https://doi.org/10.1080/17544750.2017.1279675).
- Livingstone, S., Van Couvering, E. and Thumim, N. (2008), "Converging traditions of research on media and information literacies: disciplinary, critical, and methodological issues", in Coiro, J., Knobel, M., Lankshear, C. and Leu, D.J. (Eds), *Handbook of Research on New Literacies*, Routledge, London, pp. 103-132.
- Livingstone, S., Stoilova, M. and Nandagiri, R. (2020), "Data and privacy literacy: the role of the school in educating children in a datafied society", in Frau-Meigs, D., Kotilainen, S., Pathak-Shelat, M., Hoechsmann, M. and Poyntz, S.R. (Eds), *The Handbook of Media Education Research*, 1st ed., Wiley, pp. 413-425, doi: [10.1002/9781119166900.ch38](https://doi.org/10.1002/9781119166900.ch38).
- Lowe, M.W. (2016), "Information literacy and privacy/security", *Codex: The Journal of the Louisiana Chapter of the ACRL*, Vol. 4 No. 1, pp. 1-8.
- Luke, A. (2012), "Critical literacy: foundational notes", *Theory into Practice*, Vol. 51 No. 1, pp. 4-11, doi: [10.1080/00405841.2012.636324](https://doi.org/10.1080/00405841.2012.636324).
- McDonald, N. and Forte, A. (2021), "Powerful privacy norms in social network discourse", *Proceedings of the ACM on Human-Computer Interaction*, Vol. 5 No. CSCW2, pp. 1-27, doi: [10.1145/3479565](https://doi.org/10.1145/3479565).
- Mackey, T.P. and Jacobson, T.E. (2011), "Reframing information literacy as a metaliteracy", *College and Research Libraries*, Vol. 72 No. 1, pp. 62-78, doi: [10.5860/crl-76r1](https://doi.org/10.5860/crl-76r1).
- MacKinnon, R. (2013), *Consent of the Networked: The Worldwide Struggle for Internet Freedom*, Paperback edition Basic Books, New York, NY.
- Macrina, A. (2015), "Accidental technologist: the tor browser and intellectual freedom in the digital age", *Reference and User Services Quarterly*, Vol. 54 No. 4, pp. 17-20, doi: [10.5860/rusq.54n4.17](https://doi.org/10.5860/rusq.54n4.17).
- Macrina, A. and Glaser, A. (2014), "Radical librarianship: how ninja librarians are ensuring patrons' electronic privacy", Boing Boing, 13 September, available at: <https://boingboing.net/2014/09/13/radical-librarianship-how-nin.html> (accessed 9 June 2023).
- Maréchal, N., MacKinnon, R. and Dheere, J. (2020), *Getting to the Source of Infodemics: It's the Business Model*, Ranking Digital Rights, Washington, D.C, pp. 1-73.
- Markham, A.N. (2019), "Critical pedagogy as a response to datafication", *Qualitative Inquiry*, Vol. 25 No. 8, pp. 754-760, doi: [10.1177/1077800418809470](https://doi.org/10.1177/1077800418809470).
- Masur, P.K. (2020), "How online privacy literacy supports self-data protection and self-determination in the age of information", *Media and Communication*, Vol. 8 No. 2, pp. 258-269, doi: [10.17645/mac.v8i2.2855](https://doi.org/10.17645/mac.v8i2.2855).
- Matthews, P. (2016), "Data literacy conceptions, community capabilities", *The Journal of Community Informatics*, Vol. 12 No. 3, doi: [10.15353/joci.v12i3.3277](https://doi.org/10.15353/joci.v12i3.3277).
- Matzner, T., Masur, P.K., Ochs, C. and Von Pape, T. (2016), "Do-It-Yourself data protection—empowerment or burden?", in Gutwirth, S., Leenes, R. and De Hert, P. (Eds), *Data Protection on the Move*, Springer, Dordrecht, Vol. 24, pp. 277-305, doi: [10.1007/978-94-017-7376-8_11](https://doi.org/10.1007/978-94-017-7376-8_11).
- Morrison, B. (2013), "Do we know what we think we know? An exploration of online social network users' privacy literacy", *Workplace Review*, Atlantic Schools of Business, Nos 1/2, pp. 58-79.

-
- Mui, Y.Q. (2011), "Little-known firms tracking data used in credit scores", *Washington Post*, 16 July.
- Mulligan, D.K., Koopman, C. and Doty, N. (2016), "Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy", *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, Vol. 374 No. 2083, pp. 1-17, doi: [10.1098/rsta.2016.0118](https://doi.org/10.1098/rsta.2016.0118).
- Nissenbaum, H. (2010), *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press, Stanford, CA.
- Pangrazio, L. and Cardozo-Gaibisso, L. (2020), "Beyond cybersafety: the need to develop social media literacies in pre-teens", *Digital Education Review*, No. 37, pp. 49-63, doi: [10.1344/der.2020.37.49-63](https://doi.org/10.1344/der.2020.37.49-63).
- Pangrazio, L. and Cardozo-Gaibisso, L. (2021), "'Your data can go to anyone': the challenges of developing critical data literacies in children", *Critical Digital Literacies: Boundary-Crossing Practices*, Brill, pp. 35-51, doi: [10.1163/9789004467040_003](https://doi.org/10.1163/9789004467040_003).
- Pangrazio, L. and Sefton-Green, J. (2020), "The social utility of 'data literacy'", *Learning, Media and Technology*, Vol. 45 No. 2, pp. 208-220, doi: [10.1080/17439884.2020.1707223](https://doi.org/10.1080/17439884.2020.1707223).
- Pangrazio, L. and Selwyn, N. (2018), "It's not like it's life or death or whatever': young people's understandings of social media data", *Social Media + Society*, Vol. 4 No. 3, pp. 1-9, doi: [10.1177/2056305118787808](https://doi.org/10.1177/2056305118787808).
- Pangrazio, L. and Selwyn, N. (2019), "Personal data literacies': a critical literacies approach to enhancing understandings of personal digital data", *New Media and Society*, Vol. 21 No. 2, pp. 419-437, doi: [10.1177/1461444818799523](https://doi.org/10.1177/1461444818799523).
- Pangrazio, L. and Selwyn, N. (2021), "Towards a school-based 'critical data education'", *Pedagogy, Culture and Society*, Vol. 29 No. 3, pp. 431-448, doi: [10.1080/14681366.2020.1747527](https://doi.org/10.1080/14681366.2020.1747527).
- Park, Y.J. (2013), "Digital literacy and privacy behavior online", *Communication Research*, Vol. 40 No. 2, pp. 215-236, doi: [10.1177/0093650211418338](https://doi.org/10.1177/0093650211418338).
- Park, Y.J. and Jang, S.M. (2014), "Understanding privacy knowledge and skill in mobile communication", *Computers in Human Behavior*, Vol. 38, pp. 296-303, doi: [10.1016/j.chb.2014.05.041](https://doi.org/10.1016/j.chb.2014.05.041).
- Pérez-Peña, R. and Rosenberg, M. (2018), "Strava fitness app can reveal military sites, analysts say", *The New York Times*, 29 January.
- Petty, T., Saba, M., Lewis, T., Gangadharan, S.P. and Eubanks, V. (2018), *Reclaiming Our Data*, Our Data Bodies, Detroit, MI.
- Pingo, Z. and Narayan, B., *et al.* (2019), "Privacy literacy and the everyday use of social technologies", in Kurbanoglu, S., Špiranec, S., Ünal, Y., Boustany, J., Huotari, M.L., Grassian, E. and Mizrahi, D., (Eds), *Information Literacy in Everyday Life*, Springer International Publishing, Cham, Vol. 989, pp. 33-49, doi: [10.1007/978-3-030-13472-3_4](https://doi.org/10.1007/978-3-030-13472-3_4).
- Prado, J.C. and Marzal, M.Á. (2013), "Incorporating data literacy into information literacy programs: core competencies and contents", *Libri*, Vol. 63 No. 2, pp. 123-134, doi: [10.1515/libri-2013-0010](https://doi.org/10.1515/libri-2013-0010).
- Prince, C., Omrani, N., Maalaoui, A., Dabic, M. and Kraus, S. (2022), "Are we living in surveillance societies and is privacy an illusion? An empirical study on privacy literacy and privacy concerns", *IEEE Transactions on Engineering Management*, Vol. 70 No. 10, pp. 1-18, doi: [10.1109/TEM.2021.3092702](https://doi.org/10.1109/TEM.2021.3092702).
- Raynes-Goldie, K. and Allen, M. (2014), "Gaming privacy: a Canadian case study of a children's co-created privacy literacy game", *Surveillance & Society*, Vol. 12 No. 3, pp. 414-426.
- Regan, P.M. (1995), *Legislating Privacy: Technology, Social Values, and Public Policy*, University of NC Press, Chapel Hill.
- Richards, N. (2022), *Why Privacy Matters*, Oxford University Press, New York, NY.
- Rosenberg, M., Confessore, N. and Cadwalladr, C. (2018), "How Trump consultants exploited the facebook data of millions", *The New York Times*, 17 March.

- Rotman, D. (2009), "Are you looking at me?—social media and privacy literacy", *Proceedings of the iConference 2009, presented at the iConference 2009*, iSchools, Chapel Hill, NC, pp. 1-3.
- Rowsell, J. and Pahl, K. (2015), "Introduction", in Rowsell, J. and Pahl, K. (Eds), *The Routledge Handbook of Literacy Studies*, Routledge, London New York, NY, pp. 1-16.
- Sambasivan, N., Checkley, G., Batool, A., Ahmed, N., Nemer, D., Gaytán-Lugo, L.S., Matthews, T., *et al.* (2018), "'Privacy is not for me, it's for those rich women': performative privacy practices on mobile phones by women in South Asia", *presented at the Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, pp. 127-142.
- Selwyn, N. and Pangrazio, L. (2018), "Doing data differently? Developing personal data tactics and strategies amongst young mobile media users", *Big Data and Society*, Vol. 5 No. 1, pp. 1-12, doi: [10.1177/2053951718765021](https://doi.org/10.1177/2053951718765021).
- Sindermann, C., Schmitt, H.S., Kargl, F., Herbert, C. and Montag, C. (2021), "Online privacy literacy and online privacy behavior – the role of crystallized intelligence and personality", *International Journal of Human-Computer Interaction*, Vol. 37 No. 15, pp. 1455-1466, doi: [10.1080/10447318.2021.1894799](https://doi.org/10.1080/10447318.2021.1894799).
- Smith, K.L., Shade, L.R. and Shepherd, T. (2017), "Open privacy badges for digital policy literacy", *International Journal of Communication*, Vol. 11, pp. 2784-2805.
- Solove, D. (2008), *Understanding Privacy*, Harvard University Press, Cambridge, MA.
- Solove, D.J. (2013), "Privacy self-management and the consent dilemma", *Harvard Law Review*, Vol. 126, pp. 1880-1903.
- Steeves, V. (2022), "Regulating children's privacy: the UK age appropriate design code and the pitfalls of the past", Parenting for a Digital Future, 22 June, available at: <https://blogs.lse.ac.uk/parenting4digitalfuture/2022/06/22/regulating-privacy/> (accessed 11 September 2023).
- Stoilova, M., Livingstone, S. and Nandagiri, R. (2020), "Digital by default: Children's capacity to understand and manage online data and privacy", *Media and Communication*, Vol. 8 No. 4, pp. 197-207, doi: [10.17645/mac.v8i4.3407](https://doi.org/10.17645/mac.v8i4.3407).
- Street, B. (2003), "What's 'new' in new literacy studies? Critical approaches to literacy in theory and practice", *Current Issues in Comparative Education*, Vol. 5 No. 2, pp. 77-91.
- The New London Group (1996), "A pedagogy of multiliteracies: designing social futures", *Harvard Educational Review*, Vol. 66 No. 1, pp. 60-93, doi: [10.17763/haer.66.1.17370n67v22j160u](https://doi.org/10.17763/haer.66.1.17370n67v22j160u).
- The Red Nation (Albuquerque, NM) (2021) (Ed.), *The Red Deal: Indigenous Action to save Our Earth*, Common Notions, Brooklyn, New York, NY.
- Trepte, S., Teutsch, D., Masur, P.K., Eicher, C., Fischer, M., Hennhöfer, A. and Lind, F. (2015), "Do people know about privacy and data protection strategies? Towards the 'online privacy literacy scale (OPLIS)", in Gutwirth, S., Leenes, R. and de Hert, P. (Eds), *Reforming European Data Protection Law*, Springer Netherlands, Dordrecht, Vol 20, pp. 333-365, doi: [10.1007/978-94-017-9385-8](https://doi.org/10.1007/978-94-017-9385-8).
- Vitak, J., Liao, Y., Kumar, P. and Subramaniam, M. (2018), "Librarians as information intermediaries: Navigating tensions between being helpful and being liable", in Chowdhury, G., McLeod, J., Gillet, V. and Willett, P. (Eds), *Transforming Digital Worlds, Presented at the iConference*, Springer International Publishing, Cham, pp. 693-702.
- Walker, P., Ferguson, J., Rowell, C.J., Shorish, Y., Bettinger, E. and Patterson, B. (2020), "Digital privacy instruction curriculum", Open Science Framework, 10 January, doi: [10.17605/OSF.IO/SEBHF](https://doi.org/10.17605/OSF.IO/SEBHF).
- Warren, S.D. and Brandeis, L.D. (1890), "The right to privacy", *Harvard Law Review*, Vol. 4 No. 5, pp. 193-220, doi: [10.2307/1321160](https://doi.org/10.2307/1321160).
- Wharton, L. (2018), "Ethical implications of digital tools and emerging roles for academic librarians", in Fernandez, P.D. and Tilton, K. (Eds), *Applying Library Values to Emerging Technology: Decision-Making in the Age of Open Access, Maker Spaces, and the Ever-Changing Library*, Association of College and Research Libraries, Chicago, IL, pp. 35-54.
- Wissinger, C.L. (2017), "Privacy literacy: from theory to practice", *Communications in Information Literacy*, Vol. 11 No. 2, pp. 378-389.

-
- Wolff, A., Cavero Montaner, J.J. and Kortuem, G. (2016), "Urban data in the primary classroom: bringing data literacy to the UK curriculum", *The Journal of Community Informatics*, Vol. 12 No. 3, doi: [10.15353/joci.v12i3.3278](https://doi.org/10.15353/joci.v12i3.3278).
- Young, S.W.H., Clark, J.A., Mannheimer, S. and Hinchliffe, L.J. (2019), *A National Forum on Web Privacy and Web Analytics: Action Handbook*, MT State University, doi: [10.15788/20190416.15446](https://doi.org/10.15788/20190416.15446).
- Young, S.W.H., Walker, P., Swauger, S., Gibeault, M.J., Mannheimer, S. and Clark, J.A. (2020), "Participatory approaches for designing and sustaining privacy-oriented library services", *Journal of Intellectual Freedom and Privacy*, Vol. 4 No. 4, pp. 3-18, doi: [10.5860/jifp.v4i4.7134](https://doi.org/10.5860/jifp.v4i4.7134).
- Zuboff, S. (2019), *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, 1st ed., PublicAffairs, New York, NY.
-

About the author

Priya C. Kumar, PhD, is an assistant professor at Pennsylvania State University's College of Information Sciences and Technology. She studies how we as society think, talk, study and learn about data privacy, especially in relation to children. She holds a PhD from the University of Maryland's College of Information Studies and an M.S. from the University of Michigan School of Information. She publishes across the fields of social computing, information studies and media and communication studies and regularly discusses her research with national media outlets. For more information, visit www.priyakumar.org. Priya C. Kumar can be contacted at: priya.kumar@psu.edu