10

Designing for the Privacy Commons

Darakhshan J. Mir

10.1 INTRODUCTION

This chapter frames privacy enforcement processes through the lens of governance and situated design of sociotechnical systems. It considers the challenges in formulating and designing privacy as commons (as per the Governing Knowledge Commons framework (Sanfilippo, Frischmann, and Strandburg 2018)) when privacy ultimately gets enacted (or not) in complex sociotechnical systems.

Privacy has traditionally (in computing, legal, economic, and other scholarly communities) been conceptualized in an individualistic framing, often as a private good that is traded off against other goods. In this framing, meaningful decision-making processes about one's data are available to oneself, and any resulting decisions are assumed to impact only one's own self. While social scientists have articulated and studied social conceptualizations of privacy (Petronio and Altman 2002; Altman 1975), the dominant public and scholarly discourse on privacy has been that of individualized control, with characterizations such as informed consent, and "notice and choice" being particularly prominent.

An important conceptualization of the social nature of privacy that has found expression in policy and technical practices is due to Helen Nissenbaum, whose articulation of privacy as *Contextual Integrity* (Nissenbaum 2009) rests on the notion of information flows between social actors within a specific social context. The Contextual Integrity (CI) framework states that privacy is preserved when any arising information flows comply with *contextual informational norms* and, conversely, privacy is violated when contextual norms are breached. In other words, flows are appropriate when they comply with (privacy) norms and (prima facie) inappropriate when these norms are disrupted. While CI is a powerful framework that foregrounds social conceptualizations of privacy, the contextual norms themselves are exogenous to it. Yet, the fundamentally political question of who has the power and authority to decide what is appropriate is inextricably linked to high-level moral and political values of a society, and the contextual functions, purposes, and values that practices, as per CI, must serve. In order to directly engage with these questions, the Governing

https://doi.org/10.1017/9781108749978.011 Published online by Cambridge University Press

Knowledge Commons (GKC) framework considers privacy as the governance of these informational norms (Sanfilippo, Frischmann, and Strandburg 2018). It draws attention to the political and procedural aspects of governing these rules (or norms) of appropriateness.

Scholarly commitments to the characterization of privacy as governance and constitution of appropriate informational norms raise several theoretical, conceptual, empirical, and technical questions. This chapter explores questions that such orientations generate in the conceptualization, design, implementation, and production of technical artifacts and surrounding sociotechnical systems that enable these information flows. If attention to considerations of governance of informational norms is important, then it must find an expression in the design and conceptualization of sociotechnical systems, where information flows occur. These emergent questions reside at a rich interface between different disciplines such as communication theory, sociology, law, and computer science – including the sub-discipline of human–computer interaction (HCI).

As a computer scientist, my objective of mapping these research directions is twofold: one, to frame richer, more politically and normatively grounded questions for computer scientists to engage with. Even as CI has found expression in privacy scholarship within the discipline of computer science, including HCI and software engineering, existing literature review shows (Benthall, Gürses, and Nissenbaum 2017; Badillo-Urquiola, Page, and Wisniewski 2018) that computer scientists have largely not engaged with the normative aspects of CI. Benthall et al. (Benthall, Gürses, and Nissenbaum 2017) and Badillo-Urquiloa et al. (Badillo-Urquiola, Page, and Wisniewski 2018), with the latter being focused on HCI researchers, call upon computer scientists to engage with the normative elements of CI. In this chapter, I reinforce this calling by highlighting the normative valence of the governance of informational norms, and outline a set of research directions that such orientations open up for privacy researchers who locate themselves in computer science. Second, by examining conceptualizations and practices in computer science, the GKC framework has an opportunity to make connections to existing literature in computer science, particularly one that conceptually aligns with the philosophy of the commons approach, yet might not have a similar theoretical and conceptual articulation. This is especially pertinent as the commons approach seeks to "systematize descriptive empirical case studies of real-world contexts." Finding points of injection into the design and architecture of sociotechnical systems both expands the purview of the GKC approach as well as provides opportunities to construct additional empirical case studies.

Consequently, I identify six distinct research directions pertinent to the governance and formulation of privacy norms, spanning an examination of how tools of design could be used to develop design strategies and approaches to formulate, design, and sustain a privacy commons, and how specific technical formulations and approaches to privacy can serve the governance of such a privacy commons.

https://doi.org/10.1017/9781108749978.011 Published online by Cambridge University Press

First, I examine if the tools and methodologies of design can be used to explore questions of governance and procedural legitimacy both to assess the appropriateness of entrenched norms or rules-in-use, and to handle previously unresolved, hidden, un-surfaced ethical disagreements. Second, I examine what opportunities one of these design methodologies, *Participatory Design* (Muller 2009), with its political and ideological commitments to democratic decision-making, presents in the formulation and governance of privacy norms by communities in specific contexts. This direction lays out participatory decision-making about privacy as a normative goal to achieve. Third, I explore questions that arise from the relationship between privacy literacy, civic learning, and models of participatory governance. Relatedly, fourth I propose the empirical study of relationships between privacy norms and individuals' privacy expectations and preferences, and how participation and effective modes of community engagement can shape the latter. Fifth, I identify questions related to the capacities of computational techniques to automatically extract informational norms from human sentences that consist of privacy policies formulated through a participatory process. Sixth, I examine how a technical conceptualization of privacy, differential privacy (Dwork 2006), that provides a mathematical guarantee of plausible deniability to an individual can operate within the larger normative framing of governance.

The rest of the chapter is organized as follows. The next section discusses social conceptualizations of privacy. Following this, I outline existing literature on the operationalization of social notions of privacy in the design and implementation of technical systems, finally leading to a section that elaborates on the six research directions identified previously.

10.2 SOCIAL CONCEPTUALIZATIONS OF PRIVACY

The dominant public and scholarly discourse on privacy has been that of individualized control, with characterizations such as informed consent, and "notice and choice" being particularly prominent. Two conceptual underpinnings of this individualistic framing, namely, access to meaningful decision-making and the largely localized impact of sharing one's data, are insufficient when considering the larger social contexts in which privacy is or is not enacted. Meaningful decisions to share (or not share) one's data are contingent upon the availability of informative disclosures about how such data will be shared and processed. In reality, we have little to no control or understanding over what information about ourselves we exude, where it travels, who has access to it, the processes through which other parties or individuals share this information, the ways in which it is made actionable, and how we should respond to these situations on an individual level besides by opting out of services and becoming a "digital recluse". Furthermore, even if informative disclosures are made, and understood as such by the affected population, any resulting decisions

https://doi.org/10.1017/9781108749978.011 Published online by Cambridge University Press

people make are largely superfluous since access to services is typically only available in exchange for information that individuals must provide about themselves.

Additionally, individuals' lives, and, therefore, data are interlinked with each other in underlying social contexts animated by the social, communal, professional, civic, and commercial links they have with other individuals, entities, and institutions. Consequently, our privacy (or the lack thereof) is inherently linked. This becomes amply clear when privacy is considered within the context of predictive analytic power of data, including their correlational analyses – inferences about aspects of individuals' lives from data on other individuals are precisely possible because of the underlying networked nature of our personal information. Locating its origin in the networked nature of our social relationships, Marwick and boyd capture aspects of this inherently social nature of privacy using the concept of "Networked Privacy" (Marwick and boyd 2014).

One of the earlier and more comprehensive articulations of the social dimensions of privacy is due to Regan (1986, 2000). She comprehensively outlines three dimensions of the social nature of privacy: that *privacy is a common value*, with all individuals having an appreciation of privacy to some extent, and with cultures and communities having a shared perception of privacy; that *privacy is a public value* in that it is crucial in supporting democratic political processes, and in "the forming of a body politic or public" (P. M. Regan 2015); and that *privacy is a collective value* in that one person is unlikely to have privacy unless all people have a similar level of privacy echoing the conceptualization of "networked privacy" by Marwick and boyd (Marwick and boyd 2014). Other scholars have recognized the need to deemphasize the individualized narrative of privacy by arguing that privacy is a "public good" (Fairfield and Engel 2017; P. M. Regan 2015, 2016) – something that requires public coordination for its protection – and that legal and regulatory tools should be "redesigned to focus less on individual knowledge and empowerment and more on facilitating groups' collective protection of their privacy" (Fairfield and Engel 2017). In another powerful departure from individualistic framings, Cohen argues that "protecting privacy effectively requires willingness to depart more definitively from subject-centered frameworks in favor of condition-centered frameworks" (Cohen 2019).

In a seemingly orthogonal recognition (from the approaches summarized above) of the social nature of privacy, Nissenbaum's articulation of privacy as *Contextual Integrity* (Nissenbaum 2009) rests on the notion of information flows between social actors within a specific social context. As discussed in the previous section, CI rests on the notion of appropriate information flows that are regulated by contextual informational norms. A norm is conceptualized to be "well-formed" if it is composed of five parameters: sender, recipient, information subject, attribute (information type), and a transmission principle. For example, in the healthcare context, senders, recipients, and subjects are social actors within this sphere, such as physicians, nurses, patients, therapists, etc., and attributes could consist of elements such as

https://doi.org/10.1017/9781108749978.011 Published online by Cambridge University Press

diagnoses, prescriptions, and test results. Transmission principles are expressed as a condition under which the information flow can occur, such as *with permission of the subject*, *under confidentiality*, etc. According to CI, when information flows comply with entrenched informational norms, privacy is respected, and when flows violate norms, privacy is violated.

While it might seem on the surface that informational norms (whether in policy or in technical practice) merely act as tools that regulate the appropriateness of the flow of information concerning an individual, key to the CI framework is the recognition that "legitimate" contextual informational norms are not determined individually (even though the flows themselves might involve information about specific individuals); rather these are socially constructed by our shared understanding, as members of a society, of contextual goals, values, and ends. Information flows do not occur in a vacuum but purportedly to achieve specific contextual goals and outcomes in distinct social contexts. Privacy as CI rests on this notion of socially constructed informational norms that have achieved "settled accommodation" (Nissenbaum 2019) among a group, network, or community. It also provides a normative yardstick to evaluate the appropriateness of novel information flows that could reflect evolving societal norms, against high-level moral and political values, and the extent to which these novel or evolving information flows align with the values, end, and goals of the social context they occur in.

In all of these characterizations of privacy seen above, the social versus individual dimensions of privacy (or to what extent each characterization lies on the social vs. individual spectrum) is actuated by the underlying values inherent in these characterizations and the origins of these values. As we shall see later, and elsewhere in this chapter, the GKC framework aims to understand the sources and conflicts in values in addition to locating shared values.

Among social conceptualizations of privacy, Nissenbaum's CI framework is particularly prominent, because of its descriptive and evaluative power, and because by virtue of finding expression into the logics of software system design, it is actionable in the design of technical systems. See for example Barth et al.'s (2006) work on expressing information flows and their appropriateness using first order temporal logic.

The GKC framework draws attention to the political and procedural aspects of governing these rules (or norms) of appropriateness. By foregrounding the perspective of governance, the norms of information flow can no longer be deemed to be exogenous to a specific context, but demand an engagement with aspects of procedural legitimacy of these norms – how are the norms of appropriateness in specific contexts constituted, who has a say in the process, who is excluded, how are these norms governed, and if, how, and by whom is compliance with these norms enforced? The GKC approach positions actors as members of a community rather than individuals acting within a broad social sphere subject to norms and rules that are largely deemed to be exogenous to the context. Sanfilippo et al. state that the

https://doi.org/10.1017/9781108749978.011 Published online by Cambridge University Press

most important difference between the knowledge commons framework and the CI framework is that the latter "envisions actors as individual participants in a broadly defined social context, such as education, healthcare, or the commercial market, while the knowledge commons framework envisions actors as members of a 'community' involved in producing or managing a set of resources, and in producing (or at least co producing) the applicable rules-in-use within a broader context ordinarily accounted for as part of the background environment." Sanfilippo et al., argue that:

> this shifts the focus from questions of consistency with externally defined norms and rules to questions of community governance involving not only what background norms and rules are in forces in a specific action arena but also how and by whom those rules are determined. (Sanfilippo, Frischmann, and Strandburg 2018, 127)

The GKC framework fortifies CI by further directing attention away from individuals' perceptions or experiences about privacy to the consideration of these perceptions and experiences in the context of governance, placing privacy squarely in the political and normative realm. While individuals feel the impacts of information flows, the networked nature of these impacts, and their enactment in, often, contested social contexts, necessitates an approach that returns their consideration to the normative and political sphere.

10.3 ENGAGING WITH UNDERLYING TECHNICAL PROCESSES

In this section I review literature on the motivations and means to build privacy-preserving capacities in technical systems, particularly those that embrace social conceptualizations of privacy.

In his book "Code: And other Laws of Cyberspace," Lawrence Lessig (2000) argues that in addition to the law, social norms, and the market, the underlying architecture that enables digital environments, namely "code," regulates cyberspace, making an argument for citizens to demand that any resulting technology reflect values that they would like to see being upheld in a democratic society:

> But underlying everything in this book is a single normative plea: that all of us must learn at least enough to see that technology is plastic. It can be remade to do things differently. And that if there is a mistake that we who know too little about technology should make, it is the mistake of imagining technology to be too plastic, rather than not plastic enough. We should expect – and demand – that it can be made to reflect any set of values that we think important. The burden should be on the technologists to show us why that demand can't be met. (Lessig 2000, 32)

Gürses and van Hoboken (2018) argue that public attention on privacy concerns is mainly focused on the step when digital artifacts reach consumers, and that as a result any strategies that address these concerns are conceptualized for this

https://doi.org/10.1017/9781108749978.011 Published online by Cambridge University Press

interface of technology consumption. They propose exploring ways in which interventions can be injected prior to any potential consumption – at the stage of production of such technologies. Shining a spotlight on the stages of production of software – the backbone of any technical artifact – can help scholars "better engage with new configurations of power" that "have implications for fundamental rights and freedoms, including privacy." They articulate privacy governance as the "combination of technical, organizational and regulatory approaches" for the governance of privacy. They use the term "end-users" to underline the limited agency typically users of software services have in designing the privacy and other affordances of such systems, making the argument that in addition to paying more attention to the production stages of software, privacy scholarship should also focus on the functionality that the software offers and how it impacts end-users' activities.

The recognition of the importance of integrating and operationalizing conceptualizations of privacy in the design of technical products led to the development of the Privacy by Design (PBD) framework (Cavoukian and others 2009; Gürses, Troncoso, and Diaz 2011). PBD takes a proactive approach to privacy by ensuring that privacy-preserving capacities are upheld and privacy-harming ones are extenuated, during the design of a technical artifact. It relies on design of a product as a means of complying with privacy policies – which may be articulated through regulations or law – rather than a reactive system such as one that imposes penalties. The PBD paradigm foregrounds the technical design process to create an artifact that is protective of privacy from the "ground-up".

Gürses et al. (Gürses, Troncoso, and Diaz 2011) point out that while a commitment to principles of PBD is finding growing traction in regulatory settings, there is little common, concrete understanding of how these principles translate to technical and design practice. They argue that an interpretation of these principles "requires specific engineering expertise, contextual analysis, and a balancing of multilateral security and privacy interests." Systematically locating these principles and their translation in the practice of engineering sociotechnical systems has led to the expression of PBD in the emerging field of privacy engineering (Gürses and Alamo 2016).

However, the operationalization of social conceptualizations of privacy in the privacy engineering process remains an underexplored area. Gürses and Alamo (Gürses and Alamo 2016) assert that a future important direction for privacy engineering would be to conduct empirical studies that are cognizant of different *contextual* challenges when the tools, techniques, and methodologies of privacy engineering are used. In 2015, the Computing Community Consortium undertook a PBD initiative to identify appropriate conceptualizations of privacy and to operationalize these conceptualizations effectively in the engineering process, with contextual integrity merging as a prominent concept.

Even as CI has been used by computer scientists (in contexts within and outside privacy engineering), a recent literature review finds that they have largely not

https://doi.org/10.1017/9781108749978.011 Published online by Cambridge University Press

engaged with the normative elements of CI (Benthall, Gürses, and Nissenbaum 2017). This finding holds true even for HCI researchers (Badillo-Urquiola, Page, and Wisniewski 2018). Even as HCI engages more deeply with questions of technology embedded in social and cultural contexts, Badillo-Urquiloa et al. find that HCI researchers too have not engaged deeply with the critical and normative aspects of CI, and HCI researchers must engage more deeply with the normative aspects of CI to "inform their research design, design new sociotechnical systems, and evaluate whether CI can be used as an actionable framework for translating users' privacy norms into usable systems." Many of the research directions identified in this chapter, directly speak to these recommendations.

10.4 RESEARCH DIRECTIONS

In this section, I map six research directions pertinent to the design of sociotechnical systems when considering the GKC framework. First, I examine if the tools and methodologies of design can be used to explore questions of governance and procedural legitimacy both to assess the appropriateness of entrenched norms or rules-in-use and to handle previously unresolved, hidden, un-surfaced ethical disagreements. Second, I examine what opportunities one of these design methodologies, Participatory Design, with its political and ideological commitments to democratic decision-making, presents in the formulation and governance of privacy norms by a community in a specific context. This direction lays out participatory decision-making about privacy as a normative goal to achieve. Third, I explore questions that arise from the relationship between privacy literacy, civic learning, and models of participatory governance. Relatedly, fourth I propose the empirical study of relationships between privacy norms and individuals' privacy expectations and preferences, and how participation and effective modes of community engagement can shape the latter. Fifth, I identify questions related to the capacities of computational techniques to automatically extract informational norms from human sentences that consist of privacy policies formulated through a participatory process. Sixth, I examine how a technical conceptualization of privacy, differential privacy, that provides a mathematical guarantee of plausible deniability to an individual can operate within the larger normative framing of governance. In the following subsections, I expand on these six research directions.

10.4.1 *Design Paradigms to Examine the Legitimacy of Privacy Rules-in-Use*

As discussed in the previous section, the alignment of PBD with privacy engineering could make the former an important enactor of privacy-preserving capabilities of a sociotechnical system. Wong and Mulligan (Wong and Mulligan 2019) outline the important place PBD has come to occupy in the privacy policy sphere, owing to its inclusion in the EU's General Data Protection Regulation, the United States

https://doi.org/10.1017/9781108749978.011 Published online by Cambridge University Press

Federal Trade Commission's privacy policy recommendations, and other privacy advisory and regulatory institutions. They argue that PBD is currently, largely, dominated by engineering approaches that assume that privacy is pre-defined and exogenous to the design process, whereas HCI has a rich collection of design methodologies and tools that are capable of identifying relevant conceptualizations of privacy and related values *within* the design process. Such approaches, they further argue, are largely absent from policy-making and practice of PBD. Furthermore, even within HCI, they find that most PBD approaches use design and associated principles "to solve a privacy problem" or "to support or inform privacy decision making", and that "design to explore people and situations and to critique, speculate, or present critical alternatives" – design approaches available from the field of HCI – are largely absent from both the policy-making and the practice dimensions of PBD. They argue that the latter are particularly pertinent when the "conception of privacy that ought to guide design is unknown or contested" (Wong and Mulligan 2019). This resonates with the GKC framework:

> The commons governance perspective encourages us to look behind the curtain to investigate the *origins* and dynamic characters of both nominal rules and rules-in-use and to interrogate the potentially contested legitimacy of the formal and informal processes that produce them. We believe that issues of procedural legitimacy and distinctions between nominal rules and rules-in-use are central both to descriptive understanding of privacy and to normative evaluation and policy making. Governance and legitimacy may be particularly important for the most perplexing privacy issues, which often involve overlapping ethical contexts or contested values. (Sanfilippo, Frischmann, and Strandburg 2018, 118–119)

Both approaches emphasize the contested nature of privacy and the procedural aspects of exploring and uncovering these contestations. An important question that a synthesis of this shared emphasis raises is: what kinds of design paradigms in computer science, generally, but HCI and adjoining disciplines, specifically, provide a way for questions of governance and procedural legitimacy to enter into the design and implementation of technology that mediates or enables information flows? How can the tools and methodologies of design be employed to explore questions of governance and procedural legitimacy both to assess the appropriateness of entrenched norms or rules-in-use, and to handle previously unresolved, hidden, un-surfaced ethical disagreements?

Gurses and van Hoboken argue that contextual integrity while not tied down to concepts of time and location requires "looking back in time" to identify entrenched social norms that govern the "appropriate" information flows, in order to enable an informed and reflective design of novel socio-technical systems. Utilizing such a lens on norms, and considering the GKC framework, what can the tools and methodologies of design reveal about the procedural legitimacy of entrenched privacy norms and values?

https://doi.org/10.1017/9781108749978.011 Published online by Cambridge University Press

One way forward toward exploring this question further is contained in the approaches outlined by Wong and Mulligan (2019), who map out the purposes for which design is employed in relation to privacy in the existing HCI literature. On examining 64 scholarly publications in HCI venues that use design in relation to privacy, they find that 56 percent use design "to solve a privacy problem," where "privacy is a problem that has already been well-defined outside of the design process," and 52 percent use design "to inform and support decision-making," which foregrounds the individualized framing of privacy by focusing on providing information to users to enable them to make privacy-preserving decisions, or on the creation of tools and processes so that designers can incorporate privacy more easily in their practice. Only 22 percent used design "to explore people and situations" where design and other methodologies are used to explore what conceptualizations of privacy in varying social and cultural contexts are "at play" – an approach that has "implications for design". Finally, only 11 percent use design to "to critique, speculate or present critical alternatives," where questions such as "what should be considered as privacy?," "privacy for whom?," and "how does privacy emerge from technical, social, and legal entanglements" are considered. The latter two orientations are particularly well suited to the surfacing of privacy conceptualizations in relation to surrounding social, cultural, and political factors, yet are under-explored in the literature. These design approaches have the potential to provide tools to bring procedural legitimacy "into play in assessing whether the rules-in-use for personal information are normatively appropriate" (Sanfilippo, Frischmann, and Strandburg 2018). Furthermore, these approaches directly relate to the three distinct ways identified by Sanfilippo et al. in which procedural legitimacy is in play the GKC framework: first, whether the procedures that construct the rules-in-use are deemed to be legitimate by diverse community members, and aid them in achieving their objectives; second, whether the governance practices account for the interests and needs of "impacted outsiders"; and third, whether the "exogenous rules and norms" to which a community is subject are responsive to member needs and interests.

In particular, three design methodologies are well positioned to explore these orientations: (a) speculative design, where design is undertaken to present critical alternatives (Wong and Khovanskaya 2018; Auger 2013; DiSalvo, Jenkins, and Lodato 2016); (b) value centered design, where design is used to achieve certain human values (Friedman 1997; Shilton 2018); and (c) participatory design (Muller 2009), where design is undertaken not only for, but by impacted stakeholders.

In this section, I outline one possible direction that directly opens up points of engagement between privacy as governance of privacy rules and speculative design methodologies. DiSalvo et al. (2016) use speculative design in the context of "civic tech" as "a way to explore potential, alternative, and future conditions by articulating their existence in generative forms, with a particular focus on the complications of governance and politics disposed by computational technologies." The tools of

https://doi.org/10.1017/9781108749978.011 Published online by Cambridge University Press

speculative design can speak directly to aspects of governance that the commons approach focuses on.

To summarize, design paradigms in HCI provide potent tools to explore questions of procedural legitimacy of rules-in-use in the commons governance framework. In addition to achieving, what Wong and Mulligan (2019) consider important, namely, broadening the notion of design in PBD, these orientations could build important bridges between the PBD framework and the GKC framework.

10.4.2 *Formulation and Governance of Privacy Norms via Participatory Design*

In this subsection, I explore the framework of Participatory Design (PD) in detail to consider the opportunities it presents for democratic governance of privacy norms. PD as a design methodology has historically had clear political commitments to democratic ideals. Pilemalm (2018) notes that PD developed in the late 60s and early 70s (as cooperative design) with the intention of involving citizens in urban areas in Scandinavia in the planning and design of their living environments. Soon, PD entered workplaces in Scandinavia with the intention of making workplaces more democratic, and empowering workers to participate in and influence their working conditions and workplace technology through the use of collaborative design processes between the workers and the designers (Bjerknes et al. 1987; Ehn 1988; Simonsen and Robertson 2012). Often, this occurred by assisting workplace unions in devising technological "control activities and policies" (Asaro 2000). Subsequent "generations" of PD, particularly its variants in the United Kingdom and North America were more focused on involving users and other stakeholders in the process of design of technologies to create better systems, an adoption that largely found resonance in HCI (Muller 2009). Several studies since then have argued to actively re-introduce the political and ideological dimensions of PD, highlighting the importance of democracy as a core political ideal to PD (Beck 2002; Kanstrup 2003).

Regan's argument (Regan 1986; 2015) that privacy is both a collective and a democratic value lends credence to the idea of using democratic processes to determine which norms or rules regarding privacy should be in use, how they should be governed, how the appropriateness of specific privacy rules should be evaluated, and by whom. As Sanfilippo et al. articulate:

> Like substantive appropriateness, procedural legitimacy is contextual. Legitimacy, as consensus about social good or appropriateness as reached through participatory decision-making of all potentially impacted, is itself a normative goal that may be addressed through commons institutions. (Sanfilippo, Frischmann, and Strandburg 2018, 127)

Scholarly and political commitments to democratic decision-making in the governance of privacy takes us down the route of exploring connections to PD, and its democratic and political ideals, in particular. Some preliminary attempts in this

https://doi.org/10.1017/9781108749978.011 Published online by Cambridge University Press

direction are due to Mir et al. (2018) and Shilton et al. (2008). Yet, at the time of writing this chapter, there is almost no work on operationalizing PD to conceptualize privacy. There is much important work to be done in this direction, such as determining which privacy rules-in-use in specific contexts are normatively appropriate, what the characteristics of the community are that determine these rules-in-use, how communities and other stakeholders, particularly dynamic ones, can negotiate around conflicting values such as privacy. In this section, I examine the affordances of PD to speak to such concerns.

While PD processes have largely been absent both in the shaping of privacy policy and in exploring contested aspects of privacy, privacy scholarship can learn and adapt from the vast body of literature that *does* envision using participatory, democratic processes in shaping and determining aspects of public policy. Such adaptations are especially pertinent in cases where technology (including potentially privacy-invasive technology) is employed within contexts that are democratic by their very nature, such as several decision-making processes employed by states, cities, municipalities, and public services, a context that is often dubbed as "civic tech." In such contexts, participants' relationship to the technology in question is more appropriately framed as that of a citizen rather than a consumer. For example, Pilemalm (2018) studies the role of PD in public sector contexts, including civic engagement and "we-government" initiatives. He presents case studies showing that after addressing the challenges and practical difficulties of involving civil citizens, PD can be employed in the design of technologies in the public sector and lead to empowerment of citizens involved by both including them in designing the products that impact them and enhancing their understanding and skills.

In particular, the democratic framing of PD harkening back to its historical roots had led several PD researchers and practitioners to view PD as a process that interrogates issues of power and politics with the ultimate aim of enhancing democratic ideals, mutual learning and empowerment of the participants (Ehn 1988). While PD flourished as a practice and value-based design system (Shilton 2018) in the context of unionized workers in the Scandinavian workplace, the changing nature of work organizations and the adoption of PD outside Scandinavia led to the adoption of PD beyond the workplace. In particular Teli et al. (2018) remark that the adoption of PD in the early 2000s extended beyond the "renewed workplace" – workplaces they term as arising out of "transformations in the mode of production toward post-Fordism" – to domains considered to be constituting the "public realm" (Huybrechts, Benesch, and Geib 2017). This expression continues in what DiSalvo et al. (2012) call community-based PD, where the participants are not workers, but rather citizens interested in community-related issues, and the context involves negotiations among multiple parties with heterogeneous, and often conflicting values (Grönvall, Malmborg, and Messeter 2016). As Grönvall and coauthors remark, in such settings:

https://doi.org/10.1017/9781108749978.011 Published online by Cambridge University Press

> Infrastructure is not viewed as a substrate that other actions are based upon, but rather as an on-going appropriation between different contexts with many different stakeholders and practices with negotiation of potentially conflicting agendas and motivations for participation. In community-based PD settings, contrasting and conflicting values are unavoidable and do not only need to be explicitly addressed in the PD process, but can act as drivers for PD negotiation processes. (Grönvall, Malmborg, and Messeter 2016)

Grönvall et al. present three case studies to demonstrate how design interventions enable the participants to become aware of other participant's attitudes toward the collaboration at hand as well as their values. The case studies illustrate how even as PD as a process can enable a consensus and an understanding, the dynamic nature of the participant population leads to a continuously changing landscape of values as each participant brings in their own roles, stances, and values into these collaborations. They remark that:

> the driving force in design is rarely a shared vision among stakeholders of a future made possible through design activities. Rather the driving force in our cases has been the plurality of dynamic values, and a continuous negotiation of values in agonistic spaces; not to reconcile value differences, but to reshape and achieve a productive co-existence between them, allowing new practices among project participants to form. (Grönvall, Malmborg, and Messeter 2016)

Lodato and DiSalvo (2018) consider PD in the context of institutions operating in the public realm, examining the constraints produced through employing PD in working with or through these institutions – what they call "institutional constraints," and are ultimately interested in understanding such institutions through the lens of PD.

PD, when employed in the so-called public realm, raises questions about who the participants are, who is considered to be part of the community, how those boundaries are drawn, and who is left out of the "participation." For example, Lodato and DiSalvo claim that:

> A central concern of PD is the distribution of power – authority, control, decision-making, etc. – to underrepresented bodies, populations, and people in the design, use, and deployment of products, services, and systems in work and public life. (Lodato and DiSalvo 2018)

Since PD aims to enhance democratic decision-making, mutual learning between designers and participants, and empowerment of participants, Bossen et al. (2016) consider the question of evaluating whether PD processes indeed achieve these goals. They present a framework to systematically evaluate PD projects for these goals paying attention to the purpose of the evaluation, who conducts and leads the evaluation, who participates, the methods used, and the audience for the evaluation. These criteria help understand questions of participation, legitimacy, and empowerment in PD.

https://doi.org/10.1017/9781108749978.011 Published online by Cambridge University Press

There is some literature on the commonalities between Commons Design and Participatory Design; here I briefly review that literature to explore ideas pertinent to the design of a privacy commons. Marttila et al. (2014) examine the connections between the literature on commons (for example, using Ostrom's framework (Ostrom 1990)) and PD, with the aim of developing design strategies and approaches to designing the commons. They argue that both PD and the commons literatures "build upon stakeholders and communities' capabilities and right to act and decide upon their future." They point out how while Ostrom's "design principles"(Ostrom 1990) for long-enduring commons were not intended to provide a framework to design a commons, nevertheless, they can be integrated in the PD process "to develop a nuanced understanding of design agency and its interplay with multiple mechanisms of collective action" (Marttila, Botero, and Saad-Sulonen 2014).

Such orientations are also available (and arguably, direly needed) for the conceptualizations and implementations of privacy. However, such engagements open up questions about efficiency of processes, and scalability of solutions, two framings that technologists are particularly attuned to.

In his book titled the "Smart Enough City" (Green 2019), Ben Green presents an example that instead works with an alternative concept: "meaningful inefficiencies" that he borrows from civic media scholars (Gordon and Walter 2016). Green cites work by Gordon and coauthors (Gordon and Baldwin-Philippi 2014) to create Community PlanIt (CPI),[1] an online, multiplayer game to promote engagement, deliberation, and decision-making within communities. The game is focused not on making the process of deliberation and engagement efficient, but rather to recognize that these are necessarily inefficient processes, and to design such platforms for "meaningful inefficiencies" that highlight aspects of community member engagement, coordination, and reflection:

> Instead of being gamified with a rigid structure that funnels users to predetermined ends, CPI embraces play to enable exploration and deliberation. Every user is tasked with responding to open-ended prompts, and in order to see the responses of others, one must first submit one's own answer. Such game mechanics lead to positive and reflective deliberation that one participant called "the back and forth that you don't get in a town hall meeting." Players also noted that the game encouraged them to reflect on their own opinions and appreciate alternative viewpoints. "I think it forced you to really think about what you wanted to say in order to see other people's opinions," said one participant. "Whenever I found out that I was like the minority . . . it just made me think of why do people think the other idea is better," added another. "I put my comment and someone disagreed with it," remarked another player, before adding, "I don't really know who's right, but I feel like it made me really think about what I thought prior." Through these interactions, players developed their capacities to reflect on their positions and emerged with deeper trust in the community. (Green 2019, 54)

[1] https://elab.emerson.edu/projects/community-planit

https://doi.org/10.1017/9781108749978.011 Published online by Cambridge University Press

Could community engagement platforms that are designed to enhance civic engagement and are embedded appropriately in the civic, social, and cultural contexts of communities, such as Community PlanIt, be deployed to develop models of participatory governance of information norms? This question is inextricably linked to the larger goals of PD – that of enhancing democratic ideals, mutual learning and empowerment of the participants. The next section will delve into some of the literature on "civic learning" and reflective decision-making that enables participants to negotiate around and make collective decisions about issues impacting them.

10.4.3 *Privacy Literacy, Civic Leaning, and Participatory Governance*

Questions of participation in mechanisms of governance lead to underlying questions about people's understanding of the information flow landscape, their perception of their roles in it, and what kinds of coordination and deliberation mechanisms enable people to engage meaningfully in such participatory frameworks. In relation to the GKC framework, "adequate" privacy literacy may be viewed as "attributes of the community members" (Strandburg, Frischmann, and Madison 2017). Community members can effectively govern the privacy commons only when they understand the underlying information flows and consequences of appropriate and inappropriate flows.

An important question that such considerations raise is: What kinds of (pedagogical) tools can be used to enhance people's understanding of the data ecosystem and its implications? As Regan outlines, "the goal here would be to make visible the privacy implications which to date have effectively remained invisible to those affected" (P. Regan 2016). Here, Kumar (2018) offers some preliminary research directions by outlining the possibility of using CI as an educational tool. This stems from an earlier study Kumar conducted with her co-authors (Kumar et al. 2017), where CI was used as an analytical tool to understand how children used digital devices and how they both understood and navigated privacy concerns online. The study provided evidence that children (especially over ten) largely understand how the parameters of CI affect norms of information flow, and in particular, they had an understanding of actors and attributes, even as they don't use the same terminology. Based on this, Kumar suggests exploring CI as a tool for privacy education (Kumar 2018). In related studies, Martin and Nissenbaum (2015) use survey-based methods to show that people typically understand the parameters of an informational norm, and frame their privacy expectations in view of the context in which the information flow occurs, as well as how the information is transmitted and used, and who the senders and receivers of this information are (Martin 2012).

While Kumar is largely interested in privacy literacy for children, with the objective of equipping children to make better decisions about their privacy, a larger additional question worth examining would be to understand whether and

https://doi.org/10.1017/9781108749978.011 Published online by Cambridge University Press

how CI can be used as an educational tool to equip adults (and, potentially, children) to better understand information flows within a larger governance context.

Much work in the privacy literacy space has focused on the understanding and empowerment of individual actors with respect to their privacy – another place where individualistic, subject-centered notions of privacy have gained traction. As Park notes:

> In the digital era, the idea encompasses critical understanding of data flow and its implicit rules for users to be able to act. Literacy may serve as a principle to support, encourage, and empower users to undertake informed control of their digital identities. In short, to exercise appropriate measures of resistance against the potential abuse of personal data, it may be that users should be able to understand data flow in cyberspace and its acceptable limits of exposure. (Park 2013, 217)

However, as Cohen (2019) argues, to consider effective responses to the erosion of privacy, scholarship and practice needs to shift from "subject-centered" to "condition-centered" frameworks. In this vein, literacy can also be broadly conceptualized as the building of capacity for an individual to act in a deliberative democratic system, a direction that remains under-explored in studies of privacy literacy. Gordon and Baldwin-Phillipi (2014) call this "civic learning". They present two case studies, in which the online game Community PlanIt (CPI) was deployed in a community to enhance civic-engagement with support from local community organizations. One was part of a district wide planning process in the Boston Public Schools and the second as part of a master planning process in Detroit, Michigan. On assessing the impact of CPI in both case studies, they concluded that the gaming platform allowed what they term as "civic learning" to occur. This has important implications for privacy governance and privacy literacy: what kinds of tools and systems can help build individuals' capacities as engaged, informed, and empowered citizens in the governance of privacy rules?

10.4.4 *Empirical Studies of Privacy Norms and Their Relation to Individuals' Expectations and Preferences*

A focus on procedural legitimacy of informational norms raises another related important question: how can community members' expectations and preferences of privacy be used to assess the legitimacy of contextual informational norms?

This calls for ways of empirically studying such expectations and preferences, not merely at an individual level, but at a group level. In prior work (Shvartzshnaider et al. 2016) survey-based methods were used to measure users' expectations and preferences of privacy to determine whether or not specific information flows are appropriate. However, as Benthall at al. outline:

https://doi.org/10.1017/9781108749978.011 Published online by Cambridge University Press

> In CI, appropriateness is a function of social norms, and these norms do codify social expectations and values. Certainly, in some cases user expectations will track social expectations. But though they are related, we caution researchers against conflating social norms with user expectations and preferences. This is because individual users are more prone to becoming unreflectively habituated to a new technology than society as a whole. Also, individual user preferences may at times be opposed to the interests of society. We have identified elaborating on the relationship between individual preferences and social norms as a way to improve CI. (Benthall, Gürses, and Nissenbaum 2017, 44)

Since the GKC approach seeks to further direct attention from the individual, an important research direction is to explore how individuals' understanding, expectations, and preferences regarding privacy change in a group setting, and how such changes reflect on the larger governance procedures, particularly when these processes are democratic and participatory in nature?

In her articulation of privacy as a Common Good (P. M. Regan 2002; 2015), Regan raises an important and nuanced point to differentiate between "groups" and "individuals in a group" as a unit of analysis. She also poses the question of probing how individuals in groups differ from individuals acting individually in regards to privacy, highlighting that focusing on individuals who act and are aware of their actions and experiences as members of a group rather than merely as individuals acting in isolated capacities will aid our understanding of privacy behaviors and consequent "privacy actions and inactions." A consequent key problem Regan identifies is to create avenues to help individuals realize that they are not merely individuals but members of a group both being impacted by the actions of others in the privacy dimension and affecting other people's privacy. This has close connections to the idea of civic learning explored in the previous section. She recommends drawing on the work of sociologists, social psychologists, and communication scholars who study individual behavior in groups. This line of investigation is also open and available to computer science researchers, particularly those in HCI.

10.4.5 *Calibrating Norm Evaluation and Enforcement Engines for Dynamic Sources of Norms*

Technical systems that implement CI usually express informational norms in formal systems, and operationalize these norms on information flows that act on specific data exchange between actors in a particular context. Such systems typically rely on norm evaluation and enforcement engines that check whether the information flows are consistent with the supplied norms (Barth et al. 2006; Chowdhury et al. 2013). An important research consideration that the governance perspective raises is related to the design and architecture of CI norm evaluation and enforcement engines (along with accompanying human–computer interfaces) that are more suited for dynamic

https://doi.org/10.1017/9781108749978.011 Published online by Cambridge University Press

deliberative sources of these norms rather than static sources such as laws and policies, as has been the case in prior work (Barth et al. 2006).

Shvartzshanider et al. (2018) provide important directions here – they use natural language processing techniques such as dependency parsing to automatically extract the parameters of CI from individual sentences. Their approach extracts the CI norm parameters based on the syntactic structure of a single sentence, and uses an accompanying reading comprehension model to incorporate a semantic understanding of the larger scope in order to incorporate it into the CI parameters. They apply their techniques on a corpus that contains website privacy policies in natural text alongside annotations by law students. By supplementing this process with crowdsourcing, they demonstrate that information flows can be automatically extracted from natural text and can be made more precise by appropriate crowdsourcing techniques. While they use a corpus of website privacy policies for this purpose, an open direction is to use natural language processing to infer the parameters of privacy norms from privacy policies generated in a more participatory setting.

10.4.6 *Normative Considerations in Differential Privacy*

Contextual Integrity could provide a normative framework to embed technical notions such as differential privacy within it (Dwork 2006). To the best of the author's knowledge, there is no existing work that considers the appropriateness (or not) of releasing specific functions of a database from the perspective of CI. The GKC framework could further engage with these questions of appropriateness by considering aspects of governance of these rules of appropriateness.

Differential privacy (DP) is primarily suitable for settings where there is interest in releasing an aggregate function of a dataset consisting of data from individuals. This could include simple functions such as averages or more complex machine learning predictors. As Dwork and Roth state:

> "Differential privacy" describes a promise, made by a data holder, or curator, to a data subject: "You will not be affected, adversely or otherwise, by allowing your data to be used in any study or analysis, no matter what other studies, data sets, or information sources, are available." (Dwork and Roth 2013, 5)

This is a more intuitive explanation of an underlying mathematical guarantee of plausible deniability, modulated by a privacy parameter, that has been called epsilon in the literature (Dwork 2006; Dwork and Roth 2013). For a detailed non-technical discussion of differential privacy consult Wood et al.'s (2018) primer.

Even though the DP guarantee targets individuals, functions that could be potentially publicly released or shared are computed over a dataset consisting of several individuals. Such a guarantee might, therefore, be meaningful to examine within the context of community governance and deliberation about sharing of data or functions of data more widely. For example, access to information that furthers

https://doi.org/10.1017/9781108749978.011 Published online by Cambridge University Press

understanding of medical ailments has a different normative valence than that of aggregation and prediction for commercial purposes such as online advertising and applications that might intentionally or unintentionally enact discrimination. Communities are likely to evaluate the appropriateness of sharing aggregate functions for these two purposes in different ways. For example, many polls indicate that the public views sharing of personal health data with researchers to be different from sharing such data with other more commercializing applications, indicating the need for context-specific attention to such details. On surveying personally controlled health records (PCHRs) users, Weitzman et al. found that 91 percent were willing to share medical information for health research with such willingness "conditioned by anonymity, research use, engagement with a trusted intermediary, transparency around PCHR access and use, and payment" (Weitzman, Kaci, and Mandl 2010). In survey-based research conducted at the Pew Center, Madden and Rainie (2015) found that only 76 percent of respondents say they are "not too confident" or "not at all confident" that data on their online activity held by the online advertisers who place ads on the websites they visit will remain private and secure.

If sharing data at an aggregate level for, say, medical research purposes is deemed to be appropriate, DP can be employed within a governance framework to achieve the guarantee of plausible deniability for individual community members, and to consider questions about what are appropriate aggregate functions that should be shared with people outside the community. By paying attention to the larger normative elements of the use, purpose, and politics of aggregation, DP can be a powerful and effective tool to disrupt what Cohen terms "semantic continuity" (Cohen 2019).

Several other research directions open up when we consider embedding DP within the larger normative elements of the commons framework: what kinds of interfaces will enable citizens (without a deep mathematical background) to understand the larger guarantees of DP, and make good governance decisions? Bullek et al.'s (2017) preliminary work on making the core guarantees of DP understandable and accessible to the larger public provides one step in this direction. Further research that examines groups as units of analysis, rather than only individuals, along with considering contextual dimensions of the settings in which communities might want to share aggregate data, is needed here.

10.5 CONCLUSION

To conclude, attention toward aspects of governance, particularly its participatory orientations, opens a host of research directions that are ripe to be explored by computer scientists. Designing sociotechnical systems for the privacy commons is important scholarly work, which demands interdisciplinary engagements

https://doi.org/10.1017/9781108749978.011 Published online by Cambridge University Press

as well as orienting computer scientists toward such considerations. It is my hope that this chapter will be helpful in charting out some of these research directions.

REFERENCES

Altman, Irwin. 1975. "The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding." Brooks/Cole Publishing Company, Monterey California.

Auger, James. 2013. "Speculative Design: Crafting the Speculation." *Digital Creativity* 24 (1): 11–35. https://doi.org/10.1080/14626268.2013.767276.

Badillo-Urquiola, Karla, Xinru Page, and Pamela Wisniewski. 2018. "Literature Review: Examining Contextual Integrity within Human-Computer Interaction." *Available at SSRN 3309331*.

Barth, A., A. Datta, J. C. Mitchell, and H. Nissenbaum. 2006. "Privacy and Contextual Integrity: Framework and Applications." In *2006 IEEE Symposium on Security and Privacy (S&P'06)*, 15 pp. 184–198. Berkeley/Oakland, CA: IEEE. https://doi.org/10.1109/SP.2006.32.

Beck, Eevi. 2002. "P for Political: Participation Is Not Enough." *Scandinavian Journal of Information Systems* 14 (1). https://aisel.aisnet.org/sjis/vol14/iss1/1.

Benthall, Sebastian, Seda Gürses, and Helen Nissenbaum. 2017. "Contextual Integrity through the Lens of Computer Science." *Foundations and Trends in Privacy and Security* 2 (1): 1–69.

Bjerknes, Gro, Pelle Ehn, Morten Kyng, and Kristen Nygaard. 1987. *Computers and Democracy: A Scandinavian Challenge*. Gower Pub Co.

Bossen, Claus, Christian Dindler, and Ole Sejer Iversen. 2016. "Evaluation in Participatory Design: A Literature Survey." In *Proceedings of the 14th Participatory Design Conference: Full Papers – Volume 1*, 151–160. PDC '16. New York, NY, USA: ACM. https://doi.org/10.1145/2940299.2940303.

Bullek, Brooke, Stephanie Garboski, Darakhshan J. Mir, and Evan M. Peck. 2017. "Towards Understanding Differential Privacy: When Do People Trust Randomized Response Technique?" In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 3833–3837. CHI '17. New York, NY, USA: ACM. https://doi.org/10.1145/3025453.3025698.

Cavoukian, Ann and others. 2009. "Privacy by Design: The 7 Foundational Principles." *Information and Privacy Commissioner of Ontario, Canada* 5.

Chowdhury, Omar, Andreas Gampe, Jianwei Niu, Jeffery von Ronne, Jared Bennatt, Anupam Datta, Limin Jia, and William H Winsborough. 2013. "Privacy Promises That Can Be Kept: A Policy Analysis Method with Application to the HIPAA Privacy Rule." In *Proceedings of the 18th ACM Symposium on Access Control Models and Technologies*, 3–14. ACM.

Cohen, Julie E. 2019. "Turning Privacy Inside Out." *Theoretical Inquiries in Law* 20 (1). www7.tau.ac.il/ojs/index.php/til/article/view/1607.

DiSalvo, Carl, Andrew Clement, and Volkmar Pipek. 2012. "Communities: Participatory Design for, with and by Communities." In *Routledge International Handbook of Participatory Design*, 202–230. Routledge.

DiSalvo, Carl, Tom Jenkins, and Thomas Lodato. 2016. "Designing Speculative Civics." In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 4979–4990. CHI '16. New York, NY, USA: ACM. https://doi.org/10.1145/2858036.2858505.

https://doi.org/10.1017/9781108749978.011 Published online by Cambridge University Press

Dwork, Cynthia. 2006. “Differential Privacy.” In *Proceedings of the 33rd International Conference on Automata, Languages and Programming – Volume Part II*, 1–12. ICALP’06. Berlin, Heidelberg: Springer-Verlag. https://doi.org/10.1007/11787006_1.

Dwork, Cynthia and Aaron Roth. 2013. “The Algorithmic Foundations of Differential Privacy.” *Foundations and Trends® in Theoretical Computer Science* 9 (3–4): 211–407. https://doi.org/10.1561/0400000042.

Ehn, Pelle. 1988. “Work-Oriented Design of Computer Artifacts.” PhD Thesis, Arbetslivscentrum.

Fairfield, Joshua and Christoph Engel. 2017. “Privacy as a Public Good.” In *Privacy and Power*, edited by Russell A. Miller, 95–128. Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9781316658888.004.

Friedman, Batya, ed. 1997. *Human Values and the Design of Computer Technology*. Stanford, CA, USA: Center for the Study of Language and Information.

Gordon, Eric and Jessica Baldwin-Philippi. 2014. “Playful Civic Learning: Enabling Lateral Trust and Reflection in Game-Based Public Participation.” *International Journal of Communication* 8: 759–786.

Gordon, Eric and Stephen Walter. 2016. “16. Meaningful Inefficiencies: Resisting the Logic of Technological Efficiency in the Design of Civic Systems.” *The Playful Citizen*, 310.

Green, Ben. 2019. *The Smart Enough City: Putting Technology in Its Place to Reclaim Our Urban Future*. MIT Press.

Grönvall, Erik, Lone Malmborg, and Jörn Messeter. 2016. “Negotiation of Values As Driver in Community-Based PD.” In *Proceedings of the 14th Participatory Design Conference: Full Papers – Volume 1*, 41–50. PDC ’16. New York, NY, USA: ACM. https://doi.org/10.1145/2940299.2940308.

Gürses, S. and J. M. del Alamo. 2016. “Privacy Engineering: Shaping an Emerging Field of Research and Practice.” *IEEE Security Privacy* 14 (2): 40–46. https://doi.org/10.1109/MSP.2016.37.

Gürses, Seda and Joris van Hoboken. 2018. “Privacy after the Agile Turn.” The Cambridge Handbook of Consumer Privacy. April 2018. https://doi.org/10.1017/9781316831960.032.

Gürses, Seda, Carmela Troncoso, and Claudia Diaz. 2011. “Engineering Privacy by Design.” *Computers, Privacy & Data Protection* 14 (3): 25.

Huybrechts, Liesbeth, Henric Benesch, and Jon Geib. 2017. “Institutioning: Participatory Design, Co-Design and the Public Realm.” *CoDesign* 13 (3): 148–159.

Kanstrup, Anne Marie. 2003. “D for Democracy: On Political Ideals in Participatory Design.” *Scand. J. Inf. Syst.* 15 (1): 81–85.

Kumar, Priya. 2018. “Contextual Integrity as a Conceptual, Analytical, and Educational Tool for Research,” 5.

Kumar, Priya, Shalmali Milind Naik, Utkarsha Ramesh Devkar, Marshini Chetty, Tamara L. Clegg, and Jessica Vitak. 2017. “‘No Telling Passcodes Out Because They’Re Private’: Understanding Children’s Mental Models of Privacy and Security Online.” *Proc. ACM Hum.-Comput. Interact.* 1 (CSCW): 64: 1–64: 21. https://doi.org/10.1145/3134699.

Lessig, Lawrence. 2000. *Code and Other Laws of Cyberspace*. New York, NY, USA: Basic Books, Inc.

Lodato, Thomas and Carl DiSalvo. 2018. “Institutional Constraints: The Forms and Limits of Participatory Design in the Public Realm.” In *Proceedings of the 15th Participatory Design Conference: Full Papers – Volume 1*, 5: 1–5:12. PDC ’18. New York, NY, USA: ACM. https://doi.org/10.1145/3210586.3210595.

https://doi.org/10.1017/9781108749978.011 Published online by Cambridge University Press

Madden, Mary and Lee Rainie. 2015. "NUMBERS, FACTS AND TRENDS SHAPING THE WORLD." Pew Research Center. www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/.

Martin, Kirsten E. 2012. "Diminished or Just Different? A Factorial Vignette Study of Privacy as a Social Contract." *Journal of Business Ethics* 111 (4): 519–539. https://doi.org/10.1007/s10551-012–1215-8.

Martin, Kirsten E. and Helen Nissenbaum. 2015. "Measuring Privacy: An Empirical Test Using Context To Expose Confounding Variables." SSRN Scholarly Paper ID 2709584. Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=2709584.

Marttila, Sanna, Andrea Botero, and Joanna Saad-Sulonen. 2014. "Towards Commons Design in Participatory Design." In *Proceedings of the 13th Participatory Design Conference: Short Papers, Industry Cases, Workshop Descriptions, Doctoral Consortium Papers, and Keynote Abstracts – Volume 2*, 9–12. PDC '14. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/2662155.2662187.

Marwick, Alice E. and danah boyd. 2014. "Networked Privacy: How Teenagers Negotiate Context in Social Media." *New Media & Society* 16 (7): 1051–1067. https://doi.org/10.1177/1461444814543995.

Mir, Darakhshan J., Yan Shvartzshnaider, and Mark Latonero. 2018. "It Takes a Village: A Community Based Participatory Framework for Privacy Design." In *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 112–115. IEEE.

Muller, Michael J. 2009. "Participatory Design: The Third Space In HCI." Human-Computer Interaction. March 2, 2009. https://doi.org/10.1201/9781420088892–15.

Nissenbaum, Helen. 2009. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford University Press.

Nissenbaum, Helen. 2019. "Contextual Integrity Up and Down the Data Food Chain." *Theoretical Inquiries in Law* 20 (1): 221–56. https://doi.org/10.1515/til-2019–0008.

Ostrom, Elinor. 1990. *Governing the Commons: The Evolution of Institutions for Collective Action*. The Political Economy of Institutions and Decisions. Cambridge; New York: Cambridge University Press.

Park, Yong Jin. 2013. "Digital Literacy and Privacy Behavior Online." *Communication Research* 40 (2): 215–36. https://doi.org/10.1177/0093650211418338.

Petronio, Sandra and Irwin Altman. 2002. *Boundaries of Privacy: Dialectics of Disclosure*. Albany, UNITED STATES: State University of New York Press. http://ebookcentral.proquest.com/lib/bucknell/detail.action?docID=3408055.

Pilemalm, Sofie. 2018. "Participatory Design in Emerging Civic Engagement Initiatives in the New Public Sector: Applying PD Concepts in Resource-Scarce Organizations." *ACM Trans. Comput.-Hum. Interact.* 25 (1): 5:1–5: 26. https://doi.org/10.1145/3152420.

Regan, Priscilla. 2016. "Response to Privacy as a Public Good." *Duke Law Journal Online*, February, 51–65.

Regan, Priscilla M. 1986. "Privacy, Government Information, and Technology." *Public Administration Review* 46 (6): 629–34. https://doi.org/10.2307/976229.

Regan, Priscilla M. 2000. *Legislating Privacy: Technology, Social Values, and Public Policy*. University of North Carolina Press.

Regan, Priscilla M. 2002. "Privacy as a Common Good in the Digital World." *Information, Communication & Society* 5 (3): 382–405. https://doi.org/10.1080/13691180210159328.

Regan, Priscilla M. 2015. "Privacy and the Common Good: Revisited." In *Social Dimensions of Privacy: Interdisciplinary Perspectives*, edited by B. Roessler & D. Mokrosinska, 50–70, Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9781107280557.004.

Sanfilippo, Frischmann and Strandburg. 2018. “Privacy as Commons: Case Evaluation Through the Governing Knowledge Commons Framework.” *Journal of Information Policy* 8: 116. https://doi.org/10.5325/jinfopoli.8.2018.0116.

Shilton, Katie. 2018. “Values and Ethics in Human-Computer Interaction.” *Foundations and Trends® Human–Computer Interaction* 12 (2): 107–71. https://doi.org/10.1561/1100000073.

Shilton, Katie, Jeff Burke, Deborah Estrin, Mark Hansen, and Mani B Srivastava. 2008. “Participatory Privacy in Urban Sensing.” http://scholarworks.umass.edu/esence http://escholarship.org/uc/item/90j149pp.pdf.

Shvartzshanider, Yan, Ananth Balashankar, Thomas Wies, and Lakshminarayanan Subramanian. 2018. “RECIPE: Applying Open Domain Question Answering to Privacy Policies.” In *Proceedings of the Workshop on Machine Reading for Question Answering*, 71–77.

Shvartzshnaider, Yan, Schrasing Tong, Thomas Wies, Paula Kift, Helen Nissenbaum, Lakshminarayanan Subramanian, and Prateek Mittal. 2016. “Learning Privacy Expectations by Crowdsourcing Contextual Informational Norms.” In *Fourth AAAI Conference on Human Computation and Crowdsourcing*.

Simonsen, J., and T. Robertson. 2012. *Routledge International Handbook of Participatory Design*. Routledge International Handbooks. Taylor & Francis. https://books.google.com/books?id=l29JFCmqFikC.

Strandburg, Katherine J., Brett M. Frischmann, and Michael J. Madison. 2017. “The Knowledge Commons Framework.” In *Governing Medical Knowledge Commons*, edited by Katherine J. Strandburg, Brett M. Frischmann, and Michael J. Madison, 9–18. Cambridge Studies on Governing Knowledge Commons. Cambridge University Press. https://doi.org/10.1017/9781316544587.002.

Teli, Maurizio, Peter Lyle, and Mariacristina Sciannamblo. 2018. “Institutioning the Common: The Case of Commonfare.” In *Proceedings of the 15th Participatory Design Conference: Full Papers – Volume 1*, 6:1–6:11.PDC ’18. New York, NY, USA: ACM. https://doi.org/10.1145/3210586.3210590.

Weitzman, Elissa R., Liljana Kaci, and Kenneth D. Mandl. 2010. “Sharing Medical Data for Health Research: The Early Personal Health Record Experience.” *Journal of Medical Internet Research* 12 (2): e14. https://doi.org/10.2196/jmir.1356.

Wong, Richmond Y. and Vera Khovanskaya. 2018. “Speculative Design in HCI: From Corporate Imaginations to Critical Orientations.” In *New Directions in Third Wave Human-Computer Interaction: Volume 2 – Methodologies*, edited by Michael Filimowicz and Veronika Tzankova, 175–202. Human–Computer Interaction Series. Cham: Springer International Publishing. https://doi.org/10.1007/978–3-319–73374-6_10.

Wong, Richmond Y. and Deirdre K. Mulligan. 2019. “Bringing Design to the Privacy Table: Broadening ‘Design’ in ‘Privacy by Design’ Through the Lens of HCI.” In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 262:1–262: 17.CHI ’19. New York, NY, USA: ACM. https://doi.org/10.1145/3290605.3300492.

Wood, Alexandra, Micah Altman, Aaron Bembenek, Mark Bun, Marco Gaboardi, James Honaker, Kobbi Nissim, David R O’Brien, Thomas Steinke, and Salil Vadhan. 2018. “Differential Privacy: A Primer for a Non-Technical Audience.” *Vand. J. Ent. & Tech. L.* 21: 209.

https://doi.org/10.1017/9781108749978.011 Published online by Cambridge University Press