Title

Bringing Design to the Privacy Table: Broadening "Design" in "Privacy by Design" Through the Lens of HCI

Authors

Wong, Richmond Y
Mulligan, Deirdre K

Publication Date

2019-05-04

Peer reviewed

Bringing Design to the Privacy Table

Broadening "Design" in "Privacy by Design" Through the Lens of HCI

Richmond Y. Wong
University of California, Berkeley
Berkeley, California
richmond@ischool.berkeley.edu

Deirdre K. Mulligan
University of California, Berkeley
Berkeley, California
dkm@ischool.berkeley.edu

ABSTRACT

In calls for privacy by design (PBD), regulators and privacy scholars have investigated the richness of the concept of "privacy." In contrast, "design" in HCI is comprised of rich and complex concepts and practices, but has received much less attention in the PBD context. Conducting a literature review of HCI publications discussing privacy and design, this paper articulates a set of dimensions along which design relates to privacy, including: the purpose of design, which actors do design work in these settings, and the envisioned beneficiaries of design work. We suggest new roles for HCI and design in PBD research and practice: utilizing values- and critically-oriented design approaches to foreground social values and help define privacy problem spaces. We argue such approaches, in addition to current "design to solve privacy problems" efforts, are essential to the full realization of PBD, while noting the politics involved when choosing design to address privacy.

CCS CONCEPTS

• **Security and privacy** → **Human and societal aspects of security and privacy**; • **Social and professional topics** → **Computing / technology policy**; • **Human-centered computing** → *HCI design and evaluation methods.*

KEYWORDS

privacy by design, design approaches, design research

ACM Reference Format:
Richmond Y. Wong and Deirdre K. Mulligan. 2019. Bringing Design to the Privacy Table: Broadening "Design" in "Privacy by Design" Through the Lens of HCI. In *CHI Conference on Human Factors in Computing Systems Proceedings (CHI 2019), May 4–9, 2019, Glasgow, Scotland UK*. ACM, New York, NY, USA, 17 pages. https://doi.org/10.1145/3290605.3300492

CHI 2019, May 4–9, 2019, Glasgow, Scotland UK

ACM ISBN 978-1-4503-5970-2/19/05…$15.00
https://doi.org/10.1145/3290605.3300492

1 INTRODUCTION

The concept of *privacy by design* (PBD)—embedding privacy protections into products during the initial design phase, rather than retroactively—uses the word design to enlist technical artifacts in implementing policy choices. Traditional legal and regulatory levers generally forbid or demand behaviors that invade or protect privacy, respectively, but rely on after-the-fact penalties to enforce privacy protections. PBD in contrast suggests a proactive approach, to make occurrences of privacy harms impractical in the first place. It demands that privacy be "built in" during the design process. PBD is gaining traction in part due to its inclusion in the E.U.'s General Data Protection Regulation, policy recommendations by the U.S. Federal Trade Commission, and guidance from privacy advisory and regulatory bodies around the globe. While championing PBD, these regulatory discussions offer little in the way of concrete guidance of what "privacy by design" means in technical and design practice. While privacy and legal scholarship have developed a rich set of conceptualizations and approaches for thinking about privacy (e.g., [83, 88, 107, 108]), and engineering communities have begun developing engineering privacy solutions [12, 42, 44, 51, 109], the term "design" and the roles it might play in protecting privacy remain under explored.

At the same time, the privacy community has identified challenges beyond privacy engineering that HCI design methods and approaches are uniquely equipped to address. Privacy professionals have expressed a desire for tools and approaches to help "look around corners" [6, 7] to anticipate possible privacy concerns with emerging systems and technologies, rather than assuming that current conceptualizations of privacy are the correct ones to design into technological systems. Engineering approaches that dominate PBD today assume that privacy is pre-defined (often as control over personal data through notice and choice); it is exogenous to the design process. In contrast, HCI design approaches that position the work of identifying relevant concepts of

privacy and other values within design processes are largely absent from policy and implementation efforts around PBD. To map this space of design practices, we conduct a literature review of HCI publications that discuss privacy and design, curated to articulate the breadth of ways HCI researchers have positioned design in relation to privacy.

This paper makes two main contributions. First, we aim to broaden perspectives on the potential role for design within the HCI Privacy By Design research and practitioner community; Privacy By Design should engage with the *rich variety of purposes for which design can be enrolled for privacy*. Towards this end, we articulate a set of dimensions to describe design as it relates to privacy: the purpose of design, which actors do design work, and the beneficiaries of design work. These dimensions map out political and intellectual commitments that different design approaches make towards privacy. These dimensions are a tool for reflection, allowing the HCI PBD community to critically assess the predominant ways in which it has deployed design to address privacy. Second, we argue that collaborations and research exchanges among the HCI design and privacy research communities can broaden the understanding of design within the PBD community. In particular, we identify design approaches that foreground social values and use design to explore and define a problem (or solution) space, including values- and critically-oriented design. We argue that these design approaches are a missing piece of the PBD puzzle and are essential to the protection of a fuller range of privacy concepts and the full realization of PBD. Bridging PBD with HCI's design and privacy research can help encourage more holistic discussions, drawing connections among privacy's social, legal, and technical aspects.

2 BACKGROUND

This paper aims to suggest how HCI's perspectives on design in relation to privacy can contribute to ongoing discussions of PBD. "Design" writ large has been discussed in many ways, such as a set of practices [13, 71], as discourses, or as qualities and properties of objects [89] and has a lineage spanning fields including graphic design, product design, architecture, and planning. This paper focuses on design as process or practice, and seeks to understand how this practice is used for privacy work within HCI.

Privacy by Design: A Brief History

While attempting to decode the exact history and meaning of "privacy by design" is beyond the paper's scope, a brief overview helps situate the current conversation and suggests gaps and opportunities for HCI perspectives to address. In the late 1990s and early 2000s, law and policy scholars began to consider how technologies, not just legal mechanisms, could support or protect liberties and rights [19, 34, 73]. For instance, the Platform for Privacy Preferences was seen as a technical way to address the policy problem of privacy [23].

In one of the earliest mentions of PBD, the 2000 Computers, Freedom and Privacy Conference hosted a "Workshop on Freedom and Privacy by Design," calling for participation by lawyers, social scientists, privacy & technology writers, and participatory design & accessibility experts [20]. While not explicitly defining privacy by design, workshop chair Lenny Foner described its goal as "using technology to bring about strong protections of civil liberties that are guaranteed by the technology itself" [34:153]. In the early 2000s, legal and technical researchers utilized the term privacy by design to express hopes that technical design choices could enforce conceptions of privacy present in regulation and law, such as avoiding intrusion or anonymity [19, 69].

A prominent version of PBD is "Privacy by Design" as articulated in the early 2010s by Ann Cavoukian, former Information and Privacy Commissioner for Ontario, Canada. Cavoukian provides a set of 7 principles, writing that privacy "must be approached from ...[a] design-thinking perspective. Privacy must be incorporated into networked data systems and technologies, by default," describing design-thinking as "a way of viewing the world and overcoming constraints that is at once holistic, interdisciplinary, integrative, innovative, and inspiring" [15]. Subsequently there has been a growth in calls for forms of PBD. The E.U.'s General Data Protection Regulation enshrines this, stating that data controllers "shall implement appropriate technical and organizational measures" as part of "data protection by design and default" [39]. The U.S. Federal Trade Commission has recommended companies adopt "Privacy by Design" to "promote consumer privacy throughout their organizations and at every stage of the development of their products and services" [33].

Despite these calls for PBD by regulators, there are still gaps between PBD in principle and as implemented in practice, highlighted by a series of recent workshops [21, 22, 49]. These gaps may stem in part from PBD's focus on legal and engineering practice and research. Prior work has documented the growth of privacy engineering as both a subdiscipline in computer science and a set of engineering practices [42, 44, 109]. Often privacy engineering approaches attempt to translate high level principles into implementable engineering requirements. The Fair Information Practices (FIPs) are a common set of principles used to derive privacy engineering requirements [38]. The FIPs conceptualize privacy as individuals having control over personal data—a definition that may not apply in every situation.

For example, in 2008 the U.S. Department of Homeland Security and Transportation Security Agency (TSA) used a privacy impact assessment (PIA) to analyze the potential privacy impact of airport security whole body imaging systems. Using the FIPs, the PIA conceptualized privacy as control

over personal data. The assessment found that while the system captured naked-like images of persons' bodies, it was designed such that the images would be deleted and faces were blurred so that images were not personally identifiable [113]. Nevertheless, many citizens, policymakers, and organizations cited privacy concerns about increased visibility and exposure to the TSA. Simply put, the privacy invasion arose from TSA agents viewing images of naked bodies, not from identifying people in the images. The PIA's focus on privacy risks from data collection and identification did not match people's concerns of closed-booth ogling by TSA agents, leading to expensive redesigns. The system was eventually redesigned to show a generic outline of a person rather than an image of the specific person being scanned.

Gürses et al. have critiqued privacy engineering's uses of the FIPs and the UK's PIA approach to PBD as "checklist" approaches, arguing that "it is not possible to reduce the privacy by design principles to a checklist that can be completed without further ado," as these approaches do not capture the complexities of creating systems to address privacy, and could enshrine a concept of privacy that is not applicable in all cases [44]. Building on this work, our paper charts a richer set of HCI design approaches to explore and address privacy in ways beyond checklists.

Design in Privacy Law Scholarship

PBD's approach to design has largely been informed by legal scholarship, which conceives of design as a tool for implementing objectives, or less frequently, a process to attend to preset objectives. Privacy and legal scholarship have developed a rich language to discuss privacy, including multiple conceptions of privacy [83, 107] and privacy harms [108], or the role of social context [88]. However, design has received less attention. Design in much legal scholarship is discussed as a set of properties of a completed system. Hartzog's book on design and privacy law focuses on whether a product's end design allows or prohibits behaviors in a way that aligns with privacy values expressed in law [48]. In the U.S., the Federal Trade Commission (FTC) can bring enforcement actions onto companies if it determines that properties of a product's design are "deceptive" or "unfair" with regard to privacy [53]. However, the FTC's guidance on PBD also discusses the need for systematic business practices and procedures [33], and as part of past enforcement actions has demanded certain companies put in place a "comprehensive privacy program" [32], suggesting that they view PBD as both about organizational process and particular properties of products.

A few legal scholars engage with design as a process. Hildebrandt writes that technologies are not neutral enforcement mechanisms of laws, but promote values and articulate legal norms [50]. Rubinstein and Good encourage a user experience design approach to PBD, although they discuss design as a deductive engineering process that starts with a set of usability engineering principles from which to derive design solutions [100]. This description does not make use of additional inductive and open-ended aspects of design often discussed in HCI. Mulligan and King move in that direction, discussing privacy protection as a process that requires iterative discovery and assessment of privacy risks and responses, potentially aligning well with design processes in HCI [82]. As researchers who do privacy work in HCI, design, and legal communities, we situate this paper in HCI to see how design research can align with and contribute to PBD.

Expansion of Design in HCI

While there is a strong tradition of usability and user centered design in HCI privacy research, we also note a growing range of design approaches within HCI that go beyond user centered design. HCI, an interdisciplinary field, traces its lineage from computer engineering, computer science, and psychology. Addressing human factors, usability, and efficiency were often the focus of early HCI design with the goal of aligning a system's design with a user's mental model [14, 89], epitomized by user-centered design practices. HCI's focus expanded in the late 1990s and early 2000s, some using the term "third wave" HCI, as computers expanded from the workplace into other aspects of everyday life [47]. New questions about society, culture, and ethics were not well addressed by traditional experimental modes of HCI investigation. Thus HCI began broadening to include people, methods, and epistemologies with roots in social science, humanities, and art. Zimmerman et al. chart out some of the relationships among these varied actors, including interaction designers, engineers, behavioral scientists, anthropologists, and practitioners [128]. As such, the ways design practices were used in HCI expanded. Some new approaches included research through design practices, which use the process of design to ask questions about the social and political world [37, 93, 128]. As we will show, current privacy research often takes approaches consistent with user centered design, but less often adopts the more generative and exploratory uses of design reflected in other areas of HCI. Bringing in the breadth of HCI design perspectives into PBD could advance privacy research by surfacing grounded understandings of privacy, and moving beyond the solutionism perspective that dominates legal and engineering discussions of PBD.

3 METHODS

We conducted a literature review, curated to explore the richness of design and privacy work. We began by collecting research publications from HCI-related conferences. Using the ACM Digital Library (ACM-DL) web interface in January 2018, we searched the Full-Text collection with the "sponsor: SIGCHI" filter, sorted by the built-in relevance feature. As we

were searching for breath and richness of design approaches, we included demos, posters, workshops, and colloquia in our search results (as well as full papers), as design research contributions are often published in non-full paper tracks. The first author manually checked that each returned paper used the word "design" in reference to a practice or process, and used the word "privacy" at least once each. Papers that did both were included; those that did not were excluded.

We used the exact search term ["privacy by design"], returning 11 results with 6 meeting our inclusion criteria. We then used the search terms [privacy by design] and [privacy design], which each returned over 1000 results. Sorted by relevance, the first author skimmed the top 50 results from each search to see if they met our inclusion criteria, resulting in an additional 48 papers. Author 1 read and coded all the papers in the corpus (n=54). Papers were openly coded for: what is designed; when is design done; who does design; who is design done for; how design relates to privacy; and how privacy is conceptualized. We thought that these categories would help highlight differences among design practices. The first author used affinity diagrams on the open codes, which both authors discussed and refined into 3 categories, which the first author used to re-code the corpus. These categories are briefly shown below and discussed more in Section 4:

- Why design? To solve a privacy problem; To support or inform privacy; To explore people and situations; To critique, speculate, or present critical alternatives.
- Design by who? Design authorities; stakeholders
- Design for whom? Design authorities; stakeholders

After this initial analysis, while our corpus included some papers on usable privacy, we decided to look at a subset of papers from the Symposium on Usable Privacy and Security (SOUPS) as a way to spot check our categories' breadth and richness, to see if there were additional categories we left out. We did not seek to capture an exhaustive or representative sample of SOUPS papers.

In July 2018, we used the SOUPS USENIX proceedings web interface with the same search terms, ["privacy by design"], [privacy by design], and [privacy design], resulting in 119 unique papers. There was no "relevance" sort feature, so we used every fourth paper to generate a sample to examine. We applied the same inclusion and exclusion criteria, resulting in 9 papers. The first author skimmed the titles of additional SOUPS papers to see if they suggested additional design orientations, adding an additional paper on nudges (though this paper was eventually coded as "to support or inform privacy"). While this second search was not exhaustive, it was a tradeoff made given that our goal was to spot check our initial set of categories, as well as time and resource constraints. The first author coded the SOUPS papers (n=10) using the 3 refined coding categories listed above. The SOUPS papers all fit into existing coding categories.

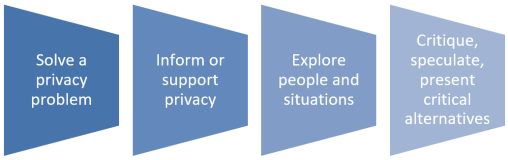

Figure 1: Design purposes that emerged from our corpus: To solve a privacy problem (56%); To inform or support privacy (52%); To explore people and situations (22%); and To critique, speculate, and present critical alternatives (11%).

The combined corpus (n=64) spans a range of HCI conferences, including CHI, Computer Supported Cooperative Work, Participatory Design Conference, Designing Interactive Systems, Computer-Human Interaction in Play, Ubiquitous Computing, and SOUPS. The range in conferences helps provide greater variety and diversity to the corpus as each conference focuses on different approaches to HCI. Some focus more on technical contributions, while others focus on design techniques and practices, or on social processes.

As with any map of a space, this analysis and corpus has some limitations. Most HCI research is published in conference proceedings, however research from journals, books, and HCI publications not published by ACM SIGCHI (except SOUPS) are not captured in the corpus. However, this analysis does not aim to provide a complete review of every paper that has discussed privacy and design. Rather it highlights the breadth and diversity of how design is considered in relation to privacy in HCI.

4 RESULTS: DIMENSIONS OF DESIGN PRACTICE

We highlight three dimensions that emerged from the analysis and coding: the purpose of design in relation to privacy; who does design work; and for whom is design done. While these are not the only way to think about design practices, they provide a useful framework to explore how design and privacy relate. We provide coding frequencies to describe how often these categories appeared in our corpus (each paper was allowed to have more than one code); however these are not necessarily representative of all privacy and design literature at large.

Purpose: How Privacy is Addressed by Design

Towards what ends is design used in relation to privacy? This section discusses four purposes of design which emerged from our coding process (Fig 1). In practice, these purposes overlap and are not mutually exclusive, but nevertheless have different enough foci to be discussed separately.

To Solve a Privacy Problem. (56%: 32 ACM, 4 USENIX papers) In our corpus, design is most commonly referred to as a way to solve a privacy problem. Some solutions take place at a system architecture level, including pseudonymous-based identity management [69], computational privacy agents to help make privacy decisions for users [75], limiting data retention [123], or encryption systems [5]. Others focus on solutions at the user interface and interaction level, such as using anti-spam tools to protect users from being intruded upon [86], or using wearable LEDs to design a private, intimate communication system [57]. Some researchers design non-technical systems to solve privacy problems. Considering personal drones, Yao et al. propose the design of a legal registration system as well as the technical design of the drone to provide privacy and enforcement [124]. In design *to solve a privacy problem*, privacy is a problem that has already been well-defined outside of the design process. A solution is then designed to address that defined problem.

To Inform or Support Privacy. (52%: 24 ACM, 9 USENIX papers) Second, design is seen used to inform or support actors who must make privacy-relevant choices, rather than solving a privacy problem outright. A system's design can help inform or support users' privacy-related actions during use. A large body of work focuses on improving the design of privacy notices [41, 63, 64, 102], ranging from their visual design, to textual content, to when they get presented. Other work considers the design of user privacy controls, their visual and interaction design, and their choice architecture [24, 59, 90, 101, 112]. The design of privacy nudges or cues [16, 94, 97] similarly supports users' decision making by encouraging users to engage in privacy-enhancing behaviors.

Design can also be deployed outside of a specific system to inform publics about privacy risks or raise awareness about protecting privacy. This includes designing educational materials or games for audiences to learn about privacy [111, 116, 126]. Others create third-party systems to support end user decision making, such as browser plugins and apps to highlight websites' and mobile apps' data practices [18, 106], or icons to help compare multiple websites' privacy behaviors. Visualizations of personal data [91], audiences of social media posts [78, 96], or ambient privacy and security warnings [25] attempt to create greater awareness of potential privacy risks. Some tools are designed to support the work of other privacy designers and researchers [61], such as mathematical models to represent user mental models [54], or privacy risk assessment tools [52, 60].

In *design to inform and support*, the problem posed by privacy is conceptualized as an informational problem for users, or as a lack of the right tools for designers. Thus *design to inform and support privacy decision making* focuses on providing information to users in ways that will encourage them to make privacy-enhancing decisions, or providing tools and methods to designers so that they can more easily address privacy in their technical practices. This implicitly assumes that if users receive the "right" types of information to users, or designers have the "right" tools, then they will choose to act in more privacy-preserving ways.

To Explore People and Situations. (22%: 13 ACM, 1 USENIX papers) Third, design is used to explore the relevance of privacy to people or situations. One approach to do this uses design as the method of inquiry to understand people and situations. Design activities may be used to engage stakeholders; designers, researchers, and stakeholders create or discuss design concepts together to understand stakeholders' experiences and concerns about privacy [67, 80, 121]. Relatedly, technology probes or conceptual design artifacts can be shared with stakeholders to understand how privacy arises in the context of their daily activities [95, 114]. Design sketches and conceptual designs can help researchers analyze empirical data, teasing out perceptions and concerns about privacy [68].

Another approach uses a range of qualitative and quantitative methods—such as ethnography, interviews, or surveys—to understand people, privacy beliefs, and behaviors. This includes studying: specific populations, such as older adults [79], children [98], or medical practitioners [17]; locations such as workplace organizations [84]; or specific technologies, such as social media and online communities [95]. Here researchers generally do not conduct design work themselves, but frame design as something to make use of empirical findings, often termed "implications for design." For instance after studying disclosure practices of older adults, McNeill et al. write "[privacy] controls should be flexible and sufficiently expressive and granular to deal with the subtleties and changing nature of relationships" [79:6433].

In *design to explore people and situations*, privacy is conceptualized as situated in relation to varying social and cultural contexts and practices, in line with recent theorizations in privacy scholarship [83, 88]. In *design to explore*, design and privacy are related in two ways. In the first approach, design methods are utilized to empirically explore what conceptions of privacy are at play. In the second, other empirical methods are used to explore what conceptions of privacy are at play, and design can then make use of those findings. There is some controversy about whether "implications for design" should be how empirical work, particularly ethnography, is discussed in relation to design [27]. We raise this not to present an argument for how design and empirical investigation should epistemologically relate to one another, but rather to highlight how design is deeply intertwined with other practices and methods (such as ethnography, user research, and evaluation).

To Critique, Speculate, or Present Critical Alternatives. (11%: 7 ACM, 0 USENIX papers) Fourth, design can create spaces in which people can discuss values, ethics, and morals. However, *design to critique, speculate, or present critical alternatives* is not necessarily about exploring the world as it is, but focuses on how the world could be. This work is often discussed under the broad rubric of critically oriented HCI. Rather than create design solutions that are deployable at scale, critically oriented HCI creates conceptual designs and design artifacts that subvert expectations, provoke, or exaggerate existing trends in order to surface, critique, and discuss values issues, and utilizes different evaluation criteria than performance, efficiency, or usability [28, 65, 93]. From our corpus, this approach has been used to probe privacy implications of systems by conceptually designing: a fictional drone regulatory system [74], a range of fictional human biosensing products deployed in a variety of contexts [122], and conceptual search engine technologies that embed alternate sets of values [68].

Similar to design *to explore*, design *to critique* also considers privacy as situated in relation to varying social and cultural contexts and practices. However, it serves to ask a different set of questions, such as "what should be considered as privacy?", "privacy for whom?", and "how does privacy emerge from technical, social, and legal entanglements?"

Design Work By and Design Work For

The second and third dimensions that arose from our analysis consider who is involved in privacy design processes: who does the design work (*design work by*), and who the design work is meant to benefit (*design work for*). We discuss two meta-categories of actors involved: design authorities and stakeholders. We use the term "design authority" to refer to the subject position of designer: someone who inhabits a social role where they have the social license and power to create or design systems. This includes HCI researchers and practitioners, interaction designers, engineers, anthropologists, behavioral scientists, and so on [128]. The dimension *design work by* allows us to capture who does design work in practice, whether or not they are a design authority. We use the term stakeholders as it is used in value sensitive design to include all those affected by systems, such as direct users, indirect users, or non-users [35]. The design authority and stakeholder categorization is simplifying, as there is not always a clear distinction between them [10]. Given the blurriness of these categories, we view them as a continuous spectrum rather than binary qualities. Acknowledging these simplifications, we attempt to map the space of actors involved in design by varying design authorities and stakeholders along two perpendicular axes: *design work by* and *design work for* to gain a sense of how the relationships between actors and the practice of design may differ (Fig 2).

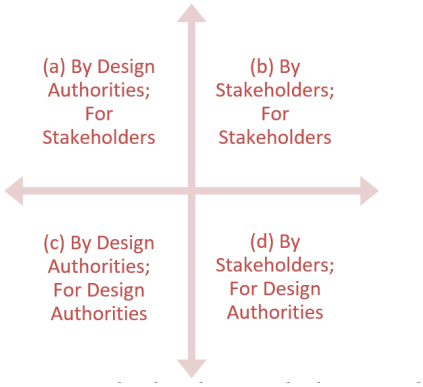

Figure 2: Actors involved in design. The horizontal axis represents a spectrum of design work by. The vertical axis represents a spectrum of design work for. Combining those provides 4 categories: By design authorities, for stakeholders (89%); By stakeholders, for stakeholders (13%); By design authorities for design authorities (17%); and By stakeholders, for design authorities (3%).

(a) By design authorities, for stakeholders. (89%: 47 ACM, 10 USENIX papers) Most often, design work is done by design authorities for stakeholders, generally users. In these cases, the design authority might be a designer (visual, interaction, UX, etc.), an engineer, or a researcher. There is variation in how stakeholders are conceptualized. Several papers conceptualize stakeholders as specific populations (e.g. users in the Middle East [1] or medical workers [17]) with specific privacy practices and needs. Other papers discuss heterogeneous groups of stakeholders, such as considering parent-child relationships when designing [127], thinking about families and their guests [24], or designing for crowdsourcing collectives [18]. Other papers refer to designing for "the user" in a general sense [64, 76].

The design of privacy design and engineering tools [40, 62] can also be considered design by design authorities, for stakeholders, because designers and engineers are conceptualized as users of the tool. For instance Hong et al. design a privacy risk modelling process for other design authorities to use when building systems [52]. Other design authorities are conceptualized as users of their modelling process.

(b) By stakeholders, for stakeholders. (13%: 8 ACM, 0 USENIX papers) In its purist form, this recognizes bottom-up forms of design that emerge from users and stakeholders, often in acts of re-appropriation or self-help. In a study that placed cameras and screens in an organization's break rooms to facilitate non-collocated interactions, some users modified the system by putting up signs to block the cameras' view [59]. In a more moderated form, researchers may invite users and stakeholders to take a larger part in the design process,

though these are generally facilitated by a design authority. For example, a workshop inviting children to help design location-sharing apps represents design work by stakeholders (and by design authorities) [80]. These approaches recognize (or provide) agency that non-design authorities have in (re)designing systems toward their own goals.

(c) By design authorities, for design authorities. (17%: 11 ACM, 0 USENIX papers) Design authorities can design for themselves through reflexive design practices, in which they use conceptual designs as a way to explore the problem space of privacy, and create room to critically reflect on and discuss the social and ethical issues at the intersection of technology, society, and privacy [68, 74, 122]. These designs might be created and reflected on individually or with other design authorities. For example, Wong et al.'s design workbooks of privacy scenarios were created as a way for the authors themselves to reflect on the nature of emerging privacy concerns related to sensing technologies [122].

(d) By stakeholders, for design authorities. (3%: 2 ACM, 0 USENIX papers) The corpus did not provide much evidence for or examples of this quadrant within HCI. Potentially some user feedback mechanisms could be considered here, such as the PIPWatch browser toolbar which allows users to see information about websites' privacy practices and contact websites' privacy officers [18]. However, feedback mechanisms fall short of allowing stakeholders to practice design. This speaks to structural differences between design authorities and stakeholders. Users might have choices to configure settings or leave a service, but generally have little opportunity to practice design work with the same latitude that design authorities have. Future privacy research might explore more ways for design to be practiced *by stakeholders, for design authorities.*

5 MAPPING DESIGN APPROACHES TO PRIVACY

In the previous section, we identified three dimensions along which the privacy and design papers varied: the purpose of design; who does design work; and who design work is meant to benefit. In this section, we map existing design orientations—collections of approaches and methods—that appeared in papers in the corpus onto our dimensions, and suggest how they might support different ways of approaching privacy (summarized in Fig 3). While these design orientations are also used in HCI to address issues beyond privacy, they emerged in our corpus as common ways that design was positioned in relation to privacy.

As researchers who do privacy work in HCI, design, and legal communities, we argue that PBD should engage with the richness of ways of why and how design is used for privacy—and that HCI researchers and practitioners are uniquely positioned to help PBD broaden and productively use alternative design approaches. We present this mapping in the spirit of other meta-reviews of HCI work, such as [119]. However, we provide this specific synthesis and mapping to help build bridges among the PBD, privacy, and design communities. If design is used to address privacy, the ability to articulate and specify among these multiple relations of how and why to use design, and who should do design work for whom, will become important for collaborating across disciplines.

Software and System Engineering & Design

Software and system engineering is predominantly oriented toward *solving a problem*, although it might also be used to design systems that *inform or support*. This includes designing a system's architecture or creating and applying software design patterns. This design work is generally done *by design authorities* (engineers), *for stakeholders* to use. This orientation usually begins with a well-defined conception of privacy, then derives system requirements to engineer. Software engineering lends itself well to issues of data privacy. If privacy is conceptualized as maintaining control over personal data, then appropriate access control mechanisms can be designed; if privacy is conceptualized as data disclosure, then sharing mechanisms can be designed, and so on. Some work has taken the FIPs as a set of principles from which to derive engineering requirements [60, 69]. Beyond our corpus, privacy engineering has used engineering design practices toward privacy, such as software design patterns applied to privacy [45]. Others have looked to sector-specific laws or theories of privacy to derive formal privacy definitions and engineering requirements [8, 11]. The growth of privacy-specific engineering techniques, methods, and degree programs [12, 42, 44, 109] suggests that privacy engineering is developing as its own subfield.

User Centered Design

User centered design approaches have been at the center of HCI practices for several decades. User centered design's purpose is primarily *to solve a problem* or create a system *to support and inform*, but often secondarily includes methods *to explore people and situations*. Design is conducted *by design authorities, for stakeholders*, where stakeholders are conceptualized as users. User centered design emerged from human factors and cognitive science, originally focusing on aligning mental models between humans and machines to improve usability, efficiency, and reduce the cognitive burden placed on users, and has expanded to consider a broader set of user needs. Privacy research with this design orientation has focused on improving the usability of privacy notices, making them easier to comprehend, easier to compare across services and products, and timing their display to be more useful to users (e.g., [41, 64, 102]). Systems are designed to

Design Orientation	Purpose(s)	Design work by	Design work for	How does design relate to privacy?
Software Engineering	Solve a problem; Inform and support	Design authorities	Stakeholders	Conceptions and problem of privacy defined in advance. Lends itself well to data privacy
User-Centered Design	Solve a problem; Inform and support; Explore	Design authorities	Stakeholders	Could have conception of privacy defined in advance, or might surface from users. Lends itself well to individual-based conceptions of privacy
Participatory Engagement & Values Centered	Solve a problem; Inform and support; Explore;	Design authorities; Stakeholders	Stakeholders	Surface stakeholder conceptions of privacy, involve stakeholders in the design process
Resistance, Re-Design, Re-Appropriation	Solve a problem; Critique	Design authorities; Stakeholders	Stakeholders	Shows breakdown or contestation in current conceptions of privacy
Speculative and Critical Design	Explore; Critique	Design authorities	Design authorities; Stakeholders	Critique current conceptions of privacy, explores and shows potential ways privacy might emerge in new situations

Figure 3: Summary of design orientations mapped to design dimensions.

match users' understandings and mental models of privacy [78, 85, 116, 125, 127].

Implicitly, this work assumes that if privacy tools and settings are made more usable or better align with users' expectations of privacy, then people will make more privacy-preserving decisions. Usable privacy often operationalizes an individual control orientation to privacy, where privacy is about an individual's ability to control or make choices about their data. This aligns well with the Fair Information Practices which take a similar individual control orientation to privacy, such that many usable privacy projects focus on improving forms of notice, choice, and control for users [30, 41, 46, 63, 64, 94]. User centered design can also surface other conceptualizations that users have about privacy but generally it focuses on addressing individuals' current understandings, preferences, and behaviors related to privacy that affect their ability to control personal information.

Participatory Engagement & Value Centered Design

While participatory and value centered design have different histories, we discuss them together, as they share properties when seen through the lens of our privacy and design dimensions. HCI adopted participatory design from its original Scandinavian form to allow users and stakeholders to take more active roles in the design process (rather than being merely end users or usability test subjects) [3]. Value centered design approaches originated from a set of perspectives and techniques to consider social values beyond those of efficiency and usability during design [35, 66, 87, 104]. The end purpose of these orientations is also to create a system that *solves a privacy problem* or one that helps *inform or support privacy*. But to arrive at this end goal, design is used to explore people and situations. Design work is done *for stakeholders* both *by design authorities* and *by stakeholders*, by inviting stakeholders to participate in the design process often through group activities or workshops to help elicit stakeholders' values and expertise (e.g., [79, 80]). For example, Abokhodair proposes using a value sensitive design methodology to explore and learn about privacy and social media use among Saudi Arabian youth by doing design activities with them, with the goal of developing culturally-sensitive design principles to help solve a privacy problem and support this population [1]. Müller et al. use a participatory design process to involve young girls in designing and evaluating sketches of several location-based mobile apps for youths [80]. These approaches highlight how privacy solutions can be sensitive to sociocultural differences and specificities by incorporating design work *by stakeholders* or using design *to explore peoples' and situations'* values and desires. In participatory and value centered design, stakeholders are often broader than users, including people such as indirect users, administrators, and non-users.

Privacy in these orientations is seen as contextual and sociocultural. Rather than starting with a pre-defined conception or definition of privacy, the privacy concept emerges from a participatory or exploratory process. By understanding how privacy arises for a variety of stakeholders, systems can be better designed in ways that are sensitive to multiple communities and populations. Privacy is viewed as a property of users, stakeholders, and the social, cultural, and institutional contexts in which they are situated.

Re-Design, Re-Appropriation, and Resistance

Design is not solely in the hands of design authorities; users and stakeholders can change or use systems in unexpected ways. Usually this is done to try *to solve a problem* that the current system does not address; other times it might be to try *to critique or present critical alternatives*. For instance, Martin et al.'s urban camouflage workshop created a space for people to design resistance and obfuscation strategies to urban surveillance systems, presenting alternative ways for people to relate to surveillance systems [77]. This resistance and

re-design was done *by stakeholders, for stakeholders*, as the people in the workshop were not designers of surveillance systems, but were stakeholders (potential subjects of surveillance system). In an example of re-appropriation, Chen and Xu document how hospital employees employ workarounds when their computer systems' privacy features mismatch their work practices. Chen and Xu suggest a set of recommendations for "privacy-by-redesign" [17] in order to solve a problem currently unaddressed by the current system. Beyond privacy, HCI has explored these types of design practices by studying stakeholders' repair, maintenance, and re-appropriation of systems (e.g., [26, 55, 99]).

Moments of re-design, re-appropriation, and resistance for privacy suggest that the meaning of privacy is being contested. The way privacy is considered by the existing system, if at all—including who and what privacy should protect, the theory and operationalization of privacy, and who or what is responsible for providing privacy—does not match the needs, beliefs, and lived experiences of stakeholders. In these cases, some stakeholders modify systems or behaviors towards alternative privacy ends.

Speculative and Critical Design

Speculative and critical design employs design *to explore* and *to critique, speculate, and present critical alternatives* [28, 93, 103, 120]. This is generally done *by design authorities, for design authorities* to reflect on or discuss social issues, but recent work has experimented using speculative and critical design *for stakeholders* [31]. These methods focus on exploring problem spaces, foregrounding alternative or speculative social values and politics (rather than alternative or speculative technical solutions).

Design authorities create conceptual designs or artifacts that encourage viewers to imagine a world in which these objects could exist as everyday objects and ask what social, economic, political, and technical configurations of the world would allow for these objects to exist, and how would that world differ from the present? This research prompts discussions about future worlds we might strive to achieve or avoid. Lindley and Coulton's *Game of Drones* surfaces privacy concerns within an world of personal drone use, presenting a speculative regulatory framework, enforcement notices, public infrastructures, and drone controller designs, raising questions about what types of privacy concerns emerge from drone use, and whether or not gamification mechanisms are appropriate tools to use to address privacy [74]. Wong et al. create a booklet of imagined privacy-invasive sensing technologies to engage technologists in discussions to surface what conceptions of privacy might be at stake in different contexts where individual control, notice, and choice may not be adequate to protect privacy [121].

Speculative and critical design can help explore and critique privacy shortcomings in current systems, and explore what might be considered "privacy" in emerging sociotechnical contexts. The focus of these projects is not about accurately predicting the future. Instead, their motivating questions ask "What values, practices, and politics are implicated in a system and its deployment?", or "In a world like this, whose and what privacies are at stake, what threatens privacy, and where might we place responsibility for addressing privacy?" Importantly, speculative and critical design encourages critical reflection and reflexivity on the part of design authorities, and acknowledges the different subject positions people have in relation to technologies and institutions. These methods are useful for engaging with the interconnectedness of social, economic, political, and technical configurations of the world to try to surface new conceptualizations of privacy. Rather than trying to solve privacy, speculative and critical design can be used to interrogate and broaden the problem space of what is considered "privacy" in the first place.

6 DISCUSSION

After surfacing design dimensions from the corpus of privacy and design HCI papers, and synthesizing them with existing design orientations in HCI, we reflect on the role of design in privacy research, practice, and policy. We first discuss opportunities for design to unearth contextual understandings of privacy's situated meaning and to explore and critique—rather than just solve—privacy problems. We next discuss the utility for PBD of viewing privacy as sociotechnical (rather than purely technical or social). We then reflect on the politics and potential limitations in choosing to address privacy via design practices.

Utilizing Design's Multiple Purposes

Most papers in the corpus used design *to solve a problem* (56%) or *to support or inform* privacy decision making (52%), often utilizing software engineering or user centered design practices. Indeed, regulators and practitioners are already looking to software engineering and user centered design to implement PBD. However, the corpus reveals a broader set of design approaches for privacy employed in HCI, including design *to explore people and situations* and *to critique, speculate, or present critical alternatives*. These design purposes are largely absent from the policy discussion and practice of PBD. Given the contested, contextual, and positional nature of privacy, we believe utilizing design for these purposes is crucial to advancing PBD in design, policy, and practice.

Design practices that aim to *solve* or *support* privacy work best when the problem or goal of privacy is well known and clearly defined, such as privacy as anonymity, privacy as individual control over personal data, or privacy as the

FIPs. These conceptions of privacy often drive system and software engineering and user centered design.

In contrast, other design orientations are most productive when the conception of privacy that ought to guide design is unknown or contested. Participatory engagement & value centered design can surface relevant conceptions or experiences of privacy through the study of stakeholders in context. Speculative and critical design can surface, suggest, and explore alternative conceptions of privacy. Re-design, re-appropriation, and resistance can challenge dominant conceptions of privacy (such as individual control over personal data) and propose competing concepts of what privacy is for.

Design thus is not just a tool for solving privacy problems, but also a tool to broaden our understanding and stretch our imagination about what privacy might entail, and encourage forward-looking, sociotechnical, and reflexive thinking about privacy. Bamberger and Mulligan provide an overview of how privacy professionals struggle to address concepts of privacy beyond data protection and to address situated experiences of privacy in light of sociotechnical change. They argue that "to successfully protect privacy, firms…must integrate…collective, contextual, and varied understandings of the ways that corporate use of personal information can intrude on the personal sphere, individual autonomy, and the public good of privacy" [7:27]. The PBD movement will miss this broader view of privacy if it restricts its view of design to engineering solutions to implement regulatory demands. Viewing design through a solutionism lens misses the opportunity to further push and develop the exploratory, critical, and speculative design practices that could and should enable the contextual and inductive privacy work necessary to build privacy protections that respond to challenges of the future rather than solely those of the present and past.

A Sociotechnical Stance Towards Privacy

If design is to be used to address privacy in ways beyond *solving* or *supporting and informing* where the "right" definition of privacy might not be known at the outset, how might privacy be approached in ways additional to formal definitions and requirements? We argue that the practice of PBD must recognize privacy as inherently sociotechnical and situated—even if the design output at first seems solely technological or non-technological. This sociotechnical stance could be used with many theories of privacy that HCI researchers already draw on, including contextual integrity [88], Solove's privacy harms and conceptualizations of privacy [107, 108], privacy regulation theory [2], and communication privacy management [92], or frameworks like the Fair Information Practices [38]. Different privacy theories or frameworks may make more sense in some sociotechnical contexts over others.

A sociotechnical stance towards privacy recognizes that social values are not stable and universal phenomena, but are instantiated through specific practices and ongoing processes [55, 58, 72]. Mulligan et al.'s discussion of privacy as an essentially contested concept provides a mapping of the multiplicity of concepts of privacy that might be at stake in a given situation or practice, which must take into account both social and technical aspects to understand: different conceptions of why privacy should exist, from whom privacy is sought, and what privacy protects [83]. Mulligan et al. also suggest that responsibility for privacy protection may be split among different institutions and modalities including technology design, law, and social norms.

Design approaches that explore people and situations and critique, speculate, and present critical alternatives are well suited to identify the multiple aspects and concepts of privacy at play in a given situation or context, as these help identify and think about entangled relationships among the social, technical, and legal. Furthermore, values are always being enacted and contested, thus design solutions are in some sense always partial. This is important to recognize when designing to solve a problem or to inform and support privacy. As Baumer and Silberman write, not all problems are best solved through technical design solutions [9], and in many instances privacy protection will require designing both technical and human processes. Explicitly acknowledging the partialness of design solutions for privacy—by specifying the theory of privacy used, who and what privacy protects (and does not protect), as well as why privacy is needed—can allow other mechanisms (such as law, regulation, markets, or social norms) to be deployed to address additional aspects of privacy if necessary.

Recognizing Design's Politics

The notion of design has become attractive in many fields. Sims describes the proliferation of design thinking in business management, statecraft, and education as a "romancing" of design that has the "tendency to fixate on design's apparently positive characteristics" [105:440]. Given the status and power associated with design, Sims calls for "a nuanced discussion about how design does and can do political work, in different situations, for and with differently located participants" [105:440]. While we often turn to design in HCI work as a matter of course, it is worth reflecting on the politics implicitly entailed in this choice.

What are the politics in the turn to "design" in privacy research and practice vis a vis Privacy By Design? Design is not an equal, neutral replacement of regulators' policy mechanisms. Design has its own set of affordances and politics which may provide new opportunities, risks, and ways to approach privacy. A long history of work has described how

technological artifacts are not neutral, but promote particular values and ways of order [36, 70, 87, 117]. Similarly, the act of design is not neutral. How we use design to frame and address problems has a set of politics. In this paper, the dimension of purpose(s) of how privacy is addressed by design (Fig 1) describes design's multiple political orientations.

It is perhaps easier to see how design *to explore* or *to critique* concepts of privacy uses design in political ways. However, all design has politics. Even when a conception of privacy seems like it has already been settled, as is often the case in design *to solve* or *to inform and support*, the very act of choosing design as a tool is a political act. It can have a potentially subversive politics in that through design, political ends can be both enacted and concealed [117]. Yet when the political ends and values being designed are those societies have chosen to privilege—e.g., human rights—then design may help us double down on our political commitments.

Furthermore, design is not a discrete and separate from the rest of society. Jackson et al. describe design, practice, and policy as a metaphorical knot: "the nominally separate moments of design, practice and policy show up as deeply intertwined... They are mutually constitutive... informing one another in forceful and sometimes subtle ways" [56:589]. Gürses and van Hoboken analyze the intertwining of privacy governance and software development with the shift to agile development practices, creating new relationships among people, companies, and data [43]. Design shapes and is shaped by the sociopolitical in ways that frame, foreground, and foreclose what and whose privacies are possible.

Moreover, design practices are not static; they change and move over time. Design practices once viewed as radical or critical interventions, such as participatory design, have become adopted by mainstream HCI and design practice. It is possible that speculative and critical design practices, currently a practice on the peripheries of HCI, will move closer to the center of HCI practice over time (indeed, the 2018 ACM GROUP Conference on Supporting Group Work included a track for submissions of speculative "design fiction" work). As design practices move and shift into new situated environments, their politics may shift as well. For instance, when participatory design was moved from the context of Scandinavian workers' unions into a U.S. business context, it took on different traits and commitments that were less related to the needs of organized labor [3].

When advocating for the use of design as privacy and HCI scholars, we need to acknowledge the complexity of design's power—its multiple political orientations, its limitations, its dynamism, and its entanglement with other sociotechnical systems—which affects when, where, how, and by whom design can best be used.

7 IMPLICATIONS: BRINGING DESIGN TO THE PBD TABLE

Given the range of actors related to PBD, we diffract our paper's findings through specific sub-communities relevant to PBD research and practice to discuss implications.

PBD researchers can benefit by expanding design orientations used in privacy research, utilizing methods from Participatory & Values Centered Design, Re-Design, and Speculative and Critical Design, adding to the already rich body of privacy engineering and usable privacy research. Not all problems posed by privacy are problems of engineering or usability. These additional design orientations can help solve, inform, explore, and critique other types of problems posed by privacy. Fully utilizing this range of design orientations in HCI, particularly ones that center design *to explore* and *to critique*, requires a commitment to creating and maintaining spaces and opportunities (perhaps building on the success of multiple privacy workshops at HCI conferences [4, 110, 115, 118]) for interdisciplinary research and engagement across multiple epistemologies spanning engineering, social sciences, humanities, and arts.

Privacy researchers in HCI can similarly expand the design orientation utilized in privacy research. While our corpus may not be representative of all privacy and design research, our findings begin to suggest that privacy and design work in HCI is heavily weighted towards design to *solve a privacy problem* or *to inform and support privacy*, and are designed *by design authorities, for stakeholders* (often through software engineering and user centered design orientations). Other orientations which use design toward other purposes and involve different roles for stakeholders appear underused in HCI privacy research, but could beneficially complement privacy engineering and usable privacy approaches. HCI privacy research can usefully broaden its design perspectives and orientations, making greater use of participatory, exploratory, and critical design traditions in HCI, or collaborating with those already utilizing those design research approaches.

HCI design researchers, particularly those practicing speculative and critical design, could engage with HCI privacy researchers, and engage with regulatory and commercial processes, broadening beyond doing design work *for design authorities*, to also doing design for stakeholders. The potential value of speculative and critical design approaches to the work of others in the PBD field and to the protection of privacy suggests engaging with these stakeholders. This follows Elsden et al.'s call for speculative and critical design to engage with "applied, participatory and experience-centered" aspects of HCI [31]. These can contribute to PBD by critiquing current conceptions of privacy, and exploring

what and how privacy might emerge in new sociotechnical situations. The complicated forward-looking work that corporate privacy practitioners do could benefit from approaches that help not only see around corners but imagine new or alternative corners to see around. While speculative and critical design are sometimes seen as impractical, these practices may resonate with existing corporate speculative practices such as scenario planning or visioning videos [120]. Tactically utilizing these resonances may allow speculative and critical design to gain legitimacy in corporate spaces while still maintaining their political commitments. Design researchers can also bring to privacy research approaches that foreground exploration or critique of social values, but were not reflected in our corpus, such as critical making, adversarial design, or social justice oriented design.

Privacy practitioners, particularly industry privacy officers, have sought to find contextual and anticipatory privacy tools [7]. While privacy engineering provides a useful set of tools for addressing well-defined privacy threats, the design orientations in Section 5 and Fig 3 can aid in addressing privacy in contextual and anticipatory ways. Many companies already have interaction and UX designers with knowledge of these methods, but they may not be involved in privacy efforts. Inviting designers to the table at companies' privacy teams (which often already include legal and engineering experts) can help address privacy not just as a data problem, but also as problem of contextual sociotechnical practices.

Policymakers, in calling for addressing a range of social values "by design," (e.g., privacy, security, fairness) should consider which values be protected by technology and which should be protected by social or legal processes. Dwork and Mulligan note how design for privacy might conflict with design for fairness [29]; Mulligan and Bamberger argue for the need to prioritize and think across multiple values and their interactions when using technology to regulate [81]. While some design processes like value sensitive design offer some guidance for navigating values conflicts, policymakers might also look to other social or legal processes to debate and address values conflicts. Furthermore, when calling for addressing social values "by design," policymakers should recognize design as a multi-dimensional process with its own politics and affordances (rather than design as static properties of an end product or as a neutral implementation of law and policy goals). Conceptualizing design in PBD as only an engineering process would lead to a different (likely more data-centric) implementation than conceptualizing design in the broader and multiple ways that HCI has used.

8 CONCLUSION

This paper aims to broaden perspectives on why design might be used for privacy, particularly among the Privacy by Design community. For the HCI design and privacy communities, the paper suggests reflection on how design has been predominantly deployed to address privacy, and the paper aims to build bridges to show how these communities' work and approaches can help inform each other and help broaden PBD's design efforts as privacy begins to encompass issues beyond individual control, notice, and choice.

In our literature review of design and privacy research in HCI, we identify three dimensions along which design can be described in relation to privacy: the purpose of design, who does design work, and for whom design work is meant to serve or benefit. Several common HCI design orientations that have been used to address privacy were mapped onto these dimensions. From this analysis, we specify implications for multiple PBD-relevant audiences. Overall, we suggest new roles that HCI and design can play in PBD, by taking up participatory, value centered, and speculative and critical design practices as part of PBD's repertoire. These can help PBD realize its full potential by going beyond deductive, compliance, and checklist-based approaches, and encouraging more holistic reflections and discussions by explicitly drawing connections among privacy's social, legal, and technical aspects.

ACKNOWLEDGMENTS

Thank you to the anonymous reviewers for their useful feedback. Insightful conversations with Nick Merrill, Noura Howell, Sarah Fox, John Chuang, Tara Whalen, Brett Frischmann, Lorrie Cranor, and comments on earlier drafts of this work by attendees of the 2018 Privacy Law Scholars Conference and the Berkeley Privacy Writing Group greatly helped us develop and improve the arguments in this paper. This work was supported in part by the National Science Foundation (NSF) Graduate Research Fellowship Program under Grant No. 1752814, NSF INSPIRE Grant No. 1650589, and the National Security Agency (NSA). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the NSF or NSA.

REFERENCES

[1] Norah Abokhodair. 2015. Transmigrant Saudi Arabian Youth and Social Media: Privacy, Intimacy and Freedom of Expression. In *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems - CHI EA '15*, Vol. 2. ACM, New York, NY, USA, 187–190. https://doi.org/10.1145/2702613.2702629

[2] Irwin Altman. 1975. *The environment and social behavior: privacy, personal space, territory, crowding*. Brooks/Cole, Monterey, CA.

[3] Peter M. Asaro. 2000. Transforming society by transforming technology: The science and politics of participatory design. *Accounting, Management and Information Technologies* 10, 4 (2000), 257–290. https://doi.org/10.1016/S0959-8022(00)00004-7

[4] Karla Badillo-Urquiola, Yaxing Yao, Oshrat Ayalon, Bart Knijnenurg, Xinru Page, Eran Toch, Yang Wang, and Pamela J. Wisniewski. 2018.

Privacy in Context: Critically Engaging with Theory to Guide Privacy Research and Design. In *Companion of the 2018 ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW '18)*. ACM, New York, NY, USA, 425–431. https://doi.org/10.1145/3272973.3273012

[5] Wei Bai, Moses Namara, Yichen Qian, Patrick Gage Kelley, Michelle L. Mazurek, and Doowon Kim. 2016. An Inconvenient Trust: User Attitudes toward Security and Usability Tradeoffs for Key-Directory Encryption Systems. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. USENIX Association, Denver, CO, 113–130. https://www.usenix.org/conference/soups2016/technical-sessions/presentation/bai

[6] Kenneth A. Bamberger and Deidre K. Mulligan. 2011. Privacy on the Books and on the Ground. *Stanford Law Review* 63 (2011), 247–316.

[7] Kenneth A. Bamberger and Deirdre K. Mulligan. 2015. *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe*. The MIT Press, Cambridge, Massachusetts.

[8] Adam Barth, Anupam Datta, J.C. Mitchell, and Helen Nissenbaum. 2006. Privacy and contextual integrity: framework and applications. In *2006 IEEE Symposium on Security and Privacy (S&P'06)*. IEEE, Berkeley/Oakland, CA, USA, 15. https://doi.org/10.1109/SP.2006.32

[9] Eric P.S. Baumer and M. Six Silberman. 2011. When the implication is not to design (technology). In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '11)*. ACM Press, New York, New York, USA, 2271. https://doi.org/10.1145/1978942.1979275

[10] Eric P. S. Baumer and Jed R. Brubaker. 2017. Post-userism. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems - CHI '17*. ACM Press, New York, New York, USA, 6291–6303. https://doi.org/10.1145/3025453.3025740

[11] Travis D. Breaux, Matthew W. Vail, and Annie I. Anton. 2006. Towards Regulatory Compliance: Extracting Rights and Obligations to Align Requirements with Regulations. In *14th IEEE International Requirements Engineering Conference (RE'06)*. IEEE, Minneapolis/St. Paul, MN, USA, 49–58. https://doi.org/10.1109/RE.2006.68

[12] Sean Brooks, Michael Garcia, Naomi Lefkovitz, Suzanne Lightman, and Ellen Nadeau. 2017. *An introduction to privacy engineering and risk management in federal systems*. Technical Report. National Institute of Standards and Technology, Gaithersburg, MD. https://doi.org/10.6028/NIST.IR.8062

[13] Richard Buchanan. 1992. Wicked Problems in Design Thinking. *Design Issues* 8, 2 (1992), 5. https://doi.org/10.2307/1511637

[14] Stuart K. Card, Thomas P. Moran, and Allen Newell. 1983. *The psychology of human-computer interaction*. Lawrence Erlbaum Associates, Inc., Mahwah, New Jersey.

[15] Ann Cavoukian. 2010. *Privacy by design: The 7 foundational principles. Implementation and mapping of fair information practices*. Technical Report. Information and Privacy Commissioner of Ontario. 10 pages. http://www.ontla.on.ca/library/repository/mon/24005/301946.pdf

[16] Daphne Chang, Erin L. Krupka, Eytan Adar, and Alessandro Acquisti. 2016. Engineering Information Disclosure: Norm Shaping Designs. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems - CHI '16*. ACM Press, New York, New York, USA, 587–597. https://doi.org/10.1145/2858036.2858346

[17] Yunan Chen and Heng Xu. 2013. Privacy management in dynamic groups: understanding information privacy in medical practices. In *Proceedings of the 2013 conference on Computer supported cooperative work - CSCW '13*. ACM, New York, NY, USA, 541. https://doi.org/10.1145/2441776.2441837

[18] Andrew Clement and Terry Costantino. 2008. Interactive Demonstration of PIPWatch: The Collaborative Privacy Enhancing and Accountability Toolbar. In *Proceedings of the Tenth Anniversary Conference on Participatory Design 2008 (PDC '08)*. Indiana University, Indianapolis, IN, USA, 328–329. http://dl.acm.org/citation.cfm?id=1795234.1795328

[19] Julie E. Cohen. 2000. Examined Lives: Informational Privacy and the Subject as Object. *Stanford Law Review* 52, 5 (may 2000), 1373. https://doi.org/10.2307/1229517

[20] Computers Freedom & Privacy 2000. 2000. CFP2000 Workshop on Freedom and Privacy by Design: Call for Participation. http://www.cfp2000.org/workshop/

[21] Computing Community Consortium (CCC). 2015. Privacy by Design - State of Research and Practice. http://cra.org/ccc/events/pbd-state-of-research-and-practice/

[22] Computing Community Consortium (CCC). 2015. *Privacy by Design-Engineering Privacy. Workshop 3 Report*. Technical Report. Computing Community Consortium. 1–9 pages. http://cra.org/ccc/wp-content/uploads/sites/2/2015/12/PbD3-Workshop-Report-v2.pdf

[23] Lorrie Faith Cranor and Joseph Reagle. 1997. Designing a Social Protocol: Lessons Learned from the Platform for Privacy Preferences Project. In *Telecommunications Policy Research Conference*. Alexandria, VA, USA, 1–15.

[24] Tyler Davis, Camie Steinhoff, and Maricarmen Vela. 2012. MeCasa: A Family Virtual Space. In *Proceedings of the 2012 ACM annual conference extended abstracts on Human Factors in Computing Systems Extended Abstracts - CHI EA '12*. ACM Press, New York, New York, USA, 1261. https://doi.org/10.1145/2212776.2212437

[25] Alexander De Luca, Bernhard Frauendienst, Max Maurer, and Doris Hausen. 2010. On the design of a "moody" keyboard. In *Proceedings of the 8th ACM Conference on Designing Interactive Systems - DIS '10*. ACM, New York, NY, 236. https://doi.org/10.1145/1858171.1858213

[26] Paul Dourish. 2003. The appropriation of interactive technologies: Some lessons from placeless documents. *Computer Supported Cooperative Work: CSCW: An International Journal* 12, 4 (2003), 465–490. https://doi.org/10.1023/A:1026149119426

[27] Paul Dourish. 2006. Implications for Design. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '06)*. ACM, New York, NY, USA, 541–550. https://doi.org/10.1145/1124772.1124855

[28] Anthony Dunne and Fiona Raby. 2013. *Speculative Everything*. The MIT Press, Cambridge, Massachusetts.

[29] Cynthia Dwork and Mulligan. 2013. It's not privacy, and it's not fair. *Stanford Law Review Online* 66 (2013), 35–40.

[30] Serge Egelman, Janice Tsai, Lorrie Faith Cranor, and Alessandro Acquisti. 2009. Timing is Everything?: The Effects of Timing and Placement of Online Privacy Indicators. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '09)*. ACM, New York, NY, USA, 319–328. https://doi.org/10.1145/1518701.1518752

[31] Chris Elsden, David Chatting, Abigail C. Durrant, Andrew Garbett, Bettina Nissen, John Vines, and David S. Kirk. 2017. On Speculative Enactments. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA, 5386–5399. https://doi.org/10.1145/3025453.3025503

[32] Federal Trade Commission (FTC). 2011. Consent Decree, In the Matter of Facebook, Inc. https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookagree.pdf

[33] Federal Trade Commission (FTC). 2012. Protecting Consumer in an Era of Rapid Change: Recommendations for businesses and policymakers. https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[34] Leonard N. Foner. 2002. Technology and political artifacts: The CFP2000 workshop on freedom and privacy by design. *Information Society* 18, 3 (2002), 153–163. https://doi.org/10.1080/01972240290074922

[35] Batya Friedman, Peter H. Kahn, and Alan Borning. 2008. Value Sensitive Design and Information Systems. In *The Handbook of Information and Computer Ethics*, Kenneth Einar Himma and Herman T. Tavani (Eds.). John Wiley & Sons, Inc., Chapter 4, 69–101.

[36] Batya Friedman and Helen Nissenbaum. 1996. Minimizing bias in computer systems. *ACM Transactions on Information Systems* 14, 3 (1996), 330–347.

[37] William Gaver. 2012. What should we expect from research through design?. In *Proceedings of the 2012 ACM annual conference on Human Factors in Computing Systems - CHI '12*. ACM Press, New York, New York, USA, 937. https://doi.org/10.1145/2207676.2208538

[38] Robert Gellman. 2017. Fair Information Practices: A Basic History (Version 2.18). https://bobgellman.com/rg-docs/rg-FIPshistory.pdf

[39] General Data Protection Regulation (GDPR). 2016. Article 25: Data protection by design and by default. https://gdpr-info.eu/art-25-gdpr/

[40] Alastair J Gill, Asimina Vasalou, Chrysanthi Papoutsi, and Adam N. Joinson. 2011. Privacy dictionary: A Linguistic Taxonomy of Privacy for Content Analysis. In *Proceedings of the 2011 annual conference on Human factors in computing systems - CHI '11*. ACM Press, New York, New York, USA, 3227. https://doi.org/10.1145/1978942.1979421

[41] Joshua Gluck, Florian Schaub, Amy Friedman, Hana Habib, Norman Sadeh, Lorrie Faith Cranor, and Yuvraj Agarwal. 2016. How Short Is Too Short? Implications of Length and Framing on the Effectiveness of Privacy Notices. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. USENIX Association, Denver, CO, 321–340. https://www.usenix.org/conference/soups2016/technical-sessions/presentation/gluck

[42] Seda Gürses and Jose M. Del Alamo. 2016. Privacy Engineering: Shaping an Emerging Field of Research and Practice. *IEEE Security and Privacy* 14, 2 (2016), 40–46. https://doi.org/10.1109/MSP.2016.37

[43] Seda Gürses and Joris Van Hoboken. 2017. Privacy After the Agile Turn. In *Cambridge Handbook of Consumer Privacy*, Jules Polonetsky, Omer Tene, and Evan Selinger (Eds.). Cambridge University Press, Cambridge.

[44] Seda Gürses, Carmela Troncoso, and Claudia Diaz. 2011. Engineering Privacy by Design. In *Computers, Privacy & Data Protection*. Brussels, Belgium, 25.

[45] Munawar Hafiz. 2006. A Collection of Privacy Design Patterns. In *Proceedings of the 2006 Conference on Pattern Languages of Programs (PLoP '06)*. ACM, New York, NY, USA, Article 7, 13 pages. https://doi.org/10.1145/1415472.1415481

[46] Margaret Hagen. 2016. User-Centered Privacy Communication Design. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. USENIX Association, Denver, CO, 7. https://www.usenix.org/conference/soups2016/workshop-program/wfpn/presentation/hagan

[47] Steve Harrison, Deborah Tatar, and Phoebe Sengers. 2007. The three paradigms of HCI. In *Alt. Chi. Session at the SIGCHI Conference on Human Factors in Computing Systems*. San Jose, CA, USA, 1–18.

[48] Woodrow Hartzog. 2018. *Privacy's Blueprint: The Battle to Control the Design of New Technologies*. Harvard Univ. Press, Cambridge, MA.

[49] Justin Hemmings, Marie Le Pichon, and Peter Swire. 2015. Privacy by Design - Privacy Enabling Design: Workshop 2 Report. http://cra.org/ccc/wp-content/uploads/sites/2/2015/05/PbD2-Report-v5.pdf

[50] Mireille Hildebrandt. 2015. *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology*. Edward Elgar Publishing, Cheltenham, UK.

[51] Jaap-Henk Hoepman. 2018. Privacy Design Strategies (The Little Blue Book). https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf

[52] Jason I. Hong, Jennifer D. Ng, Scott Lederer, and James A. Landay. 2004. Privacy Risk Models for Designing Privacy-sensitive Ubiquitous Computing Systems. In *Proceedings of the 5th Conference on Designing Interactive Systems: Processes, Practices, Methods, and Techniques (DIS '04)*. ACM, New York, NY, USA, 91–100. https://doi.org/10.1145/1013115.1013129

[53] Chris Jay Hoofnagle. 2016. Unfair and deceptive practices. In *Federal Trade Commission Privacy Law and Policy*. Cambridge University Press, Cambridge, Chapter 5, 119–142. https://doi.org/10.1017/CBO9781316411292.006

[54] Adam M. Houser and Matthew L Bolton. 2017. Formal Mental Models for Inclusive Privacy and Security. In *Symposium on Usable Privacy and Security (SOUPS) 2017*. USENIX Association, Santa Clara, CA, 1–3. https://www.usenix.org/conference/soups2017/workshop-program/wips2017/houser

[55] Lara Houston, Steven J Jackson, Daniela K Rosner, Syed Ishtiaque Ahmed, Meg Young, and Laewoo Kang. 2016. Values in Repair. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems - CHI '16*. ACM, New York, NY, USA, 1403–1414. https://doi.org/10.1145/2858036.2858470

[56] Steven J. Jackson, Tarleton Gillespie, and Sandy Payette. 2014. The policy knot. In *Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing - CSCW '14*. ACM, New York, NY, USA, 588–602. https://doi.org/10.1145/2531602.2531674

[57] Cindy Jacob and Bruno Dumas. 2014. Designing for intimacy: How Fashion Design Can Address Privacy Issues in Wearable Computing. In *Proceedings of the 2014 ACM International Symposium on Wearable Computers Adjunct Program - ISWC '14 Adjunct*. ACM Press, New York, New York, USA, 185–192. https://doi.org/10.1145/2641248.2641353

[58] Nassim JafariNaimi, Lisa Nathan, and Ian Hargraves. 2015. Values as Hypotheses: Design, Inquiry, and the Service of Values. *Design Issues* 31, 4 (Oct 2015), 91–104. https://doi.org/10.1162/DESI_a_00354

[59] Gavin Jancke, Gina Danielle Venolia, Jonathan Grudin, Jonathan J. Cadiz, and Anoop Gupta. 2001. Linking public spaces: technical and social issues. In *Proceedings of the SIGCHI conference on Human factors in computing systems - CHI '01*. ACM Press, New York, New York, USA, 530–537. https://doi.org/10.1145/365024.365352

[60] Carlos Jensen. 2004. Toward a method for privacy vulnerability analysis. In *Extended abstracts of the 2004 conference on Human factors and computing systems - CHI '04*. ACM Press, New York, New York, USA, 1563. https://doi.org/10.1145/985921.986139

[61] Adam N. Joinson, Jeffrey Hancock, and Pam Briggs. 2008. Secrets and Lies in Computer-mediated Interaction: Theory, Methods and Design.. In *CHI '08 Extended Abstracts on Human Factors in Computing Systems (CHI EA '08)*. ACM, New York, NY, USA, 3993–3996. https://doi.org/10.1145/1358628.1358975

[62] Clare-Marie Karat, John Karat, Carolyn Brodie, and Jinjuan Feng. 2006. Evaluating interfaces for privacy policy rule authoring. In *Proceedings of the SIGCHI conference on Human Factors in computing systems - CHI '06*. ACM, New York, NY, USA, 83. https://doi.org/10.1145/1124772.1124787

[63] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W. Reeder. 2009. A "nutrition label" for privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security - SOUPS '09*. ACM Press, New York, NY, USA, 12. https://doi.org/10.1145/1572532.1572538

[64] Patrick Gage Kelley, Lucian Cesca, Joanna Bresee, and Lorrie Faith Cranor. 2010. Standardizing privacy notices. In *Proceedings of the 28th international conference on Human factors in computing systems - CHI '10*. ACM Press, New York, NY, USA, 1573. https://doi.org/10.1145/1753326.1753561

[65] Vera Khovanskaya, Eric P. S. Baumer, and Phoebe Sengers. 2015. Double Binds and Double Blinds: Evaluation Tactics in Critically Oriented HCI. In *Proceedings of The Fifth Decennial Aarhus Conference on Critical Alternatives (CA '15)*. Aarhus University Press, Aarhus, Denmark, 53–64. https://doi.org/10.7146/aahcc.v1i1.21266

[66] Cory Knobel and Geoffrey C. Bowker. 2011. Values in design. *Commun. ACM* 54 (2011), 26. https://doi.org/10.1145/1965724.1965735

[67] Lakshmi Kumar. 2008. Beginnings in Protecting Privacy by Pretentious Invasion. In *Proceedings of the Tenth Anniversary Conference on Participatory Design 2008 (PDC '08)*. Indiana University, Indianapolis, IN, USA, 242–245. http://dl.acm.org/citation.cfm?id=1795234.1795288

[68] Anastasia Kuzminykh and Edward Lank. 2016. People Searched by People: Context-Based Selectiveness in Online Search. In *Proceedings of the 2016 ACM Conference on Designing Interactive Systems - DIS '16*. ACM, New York, NY, 749–760. https://doi.org/10.1145/2901790.2901853

[69] Marc Langheinrich. 2001. Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems. In *Proceedings of the 3rd International Conference on Ubiquitous Computing*. Springer-Verlag, Berlin, Heidelberg, 273–291. http://dl.acm.org/citation.cfm?id=647987.741336

[70] Bruno Latour. 1992. Where are the missing masses? The sociology of a few mundane artifacts. In *Shaping Technology/Building Society: Studies in Sociotechnical Change*, Wiebe Bijker and John Law (Eds.). MIT Press, Cambridge, MA, USA, 225–258.

[71] Bryan Lawson. 2005. *How Designers Think: The Design Process Demystified* (4th ed.). Routledge, London.

[72] Christopher A. Le Dantec, Erika Shehan Poole, and Susan P. Wyche. 2009. Values as lived experience: Evolving value sensitive design in support of value discovery. In *Proceedings of the 27th international conference on Human factors in computing systems - CHI 09*. ACM, New York, NY, USA, 1141. https://doi.org/10.1145/1518701.1518875

[73] Lawrence Lessig. 2006. What Things Regulate. In *Code version 2.0*. Basic Books, New York.

[74] Joseph Lindley and Paul Coulton. 2015. Game of Drones. In *Symposium on Computer-Human Interaction in Play (CHI PLAY '15)*. ACM, New York, NY, 613–618. https://doi.org/10.1145/2793107.2810300

[75] Bin Liu, Mads Schaarup Andersen, Florian Schaub, Hazim Almuhimedi, Shikun (Aerin) Zhang, Norman Sadeh, Yuvraj Agarwal, and Alessandro Acquisti. 2016. Follow My Recommendations: A Personalized Privacy Assistant for Mobile App Permissions. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. USENIX Association, Denver, CO, 27–41. https://www.usenix.org/conference/soups2016/technical-sessions/presentation/liu

[76] Ewa Luger and Tom Rodden. 2013. An informed view on consent for UbiComp. In *Proceedings of the 2013 ACM international joint conference on Pervasive and ubiquitous computing - UbiComp '13*. ACM Press, New York, New York, USA, 529. https://doi.org/10.1145/2493432.2493446

[77] Karen Martin, Ben Dalton, and Matt Jones. 2012. Crafting urban camouflage. In *Proceedings of the Designing Interactive Systems Conference on - DIS '12*. ACM, New York, NY, USA, 797. https://doi.org/10.1145/2317956.2318079

[78] Alessandra Mazzia, Kristen LeFevre, and Eytan Adar. 2012. The PViz comprehension tool for social network privacy settings. In *Proceedings of the Eighth Symposium on Usable Privacy and Security - SOUPS '12*. ACM, New York, NY, 12. https://doi.org/10.1145/2335356.2335374

[79] Andrew R. McNeill, Lynne Coventry, Jake Pywell, and Pam Briggs. 2017. Privacy Considerations when Designing Social Network Systems to Support Successful Ageing. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems - CHI '17*. ACM, New York, NY, USA, 6425–6437. https://doi.org/10.1145/3025453.3025861

[80] Heiko Müller, Jutta Fortmann, Janko Timmermann, Wilko Heuten, and Susanne Boll. 2013. Proximity sensor - Privacy-Aware Location Sharing. In *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services - MobileHCI '13*. ACM, New York, NY, USA, 564–569. https://doi.org/10.1145/2493190.2494443

[81] Deirdre K Mulligan and Kenneth A Bamberger. 2018. Saving Governance-By-Design. *California Law Review* 106, 3 (2018), 697–784. https://doi.org/10.15779/Z38QN5ZB5H

[82] Deirdre K. Mulligan and Jennifer King. 2011. Bridging the gap between privacy and design. *University of Pennsylvania Journal of Constitutional Law* 14, 4 (2011), 989–1034.

[83] Deirdre K. Mulligan, Colin Koopman, and Nick Doty. 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* 374, 2083 (Dec 2016), 17. https://doi.org/10.1098/rsta.2016.0118

[84] Alison R. Murphy, Madhu C. Reddy, and Heng Xu. 2014. Privacy practices in collaborative environments: A study of emergency department staff. In *Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing - CSCW '14*. ACM, New York, NY, USA, 269–282. https://doi.org/10.1145/2531602.2531643

[85] Pardis Emami Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. 2017. Privacy Expectations and Preferences in an IoT World. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. USENIX Association, Santa Clara, CA, 399–412. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/naeini

[86] David Nguyen and Khai Truong. 2003. PHEmail: Designing a Privacy Honoring Email System. In *CHI '03 extended abstracts on Human factors in computing systems - CHI '03*. ACM Press, New York, New York, USA, 922. https://doi.org/10.1145/765891.766072

[87] Helen Nissenbaum. 2001. How computer systems embody values. *Computer* 34, 3 (Mar 2001), 120–119. https://doi.org/10.1109/2.910905

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

[89] Donald A. Norman. 1988. *The Design of Everyday Things*. Basic Books, New York.

[90] Sangkeun Park, Emilia-Stefania Ilincai, Jeungmin Oh, Sujin Kwon, Rabeb Mizouni, and Uichin Lee. 2017. Facilitating Pervasive Community Policing on the Road with Mobile Roadwatch. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems - CHI '17*. ACM, New York, NY, USA, 3538–3550. https://doi.org/10.1145/3025453.3025867

[91] Sameer Patil and Apu Kapadia. 2012. Are you exposed? Conveying information exposure. In *Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work Companion - CSCW '12*. ACM, New York, NY, USA, 191. https://doi.org/10.1145/2141512.2141575

[92] Sandra Petronio. 2002. *Boundaries of Privacy: Dialetics of Disclosure*. State University of New York Press, Albany.

[93] James Pierce, Phoebe Sengers, Tad Hirsch, Tom Jenkins, William Gaver, and Carl DiSalvo. 2015. Expanding and Refining Design and Criticality in HCI. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 2083–2092. https://doi.org/10.1145/2702123.2702438

[94] Stefanie Pötzsch, Peter Wolkerstorfer, and Cornelia Graf. 2010. Privacy-awareness information for web forums: Results from an Empirical Study. In *Proceedings of the 6th Nordic Conference on Human-Computer Interaction Extending Boundaries - NordiCHI '10*. ACM, New York, NY, USA, 363. https://doi.org/10.1145/1868914.1868957

[95] Yang Qin, Bin Xu, and Dan Cosley. 2017. Designing the Interplay between Anonymity and Publicity for Online Social Support. In *Companion of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing - CSCW '17 Companion*. ACM, New York, NY, USA, 283–286. https://doi.org/10.1145/3022198.3026318

[96] Frederic Raber, Alexander De Luca, and Moritz Graus. 2016. Privacy Wedges: Area-Based Audience Selection for Social Network Posts. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. USENIX Association, Denver, CO, 7. https://www.usenix.org/conference/soups2016/workshop-program/wpi/presentation/raber

[97] Prashanth Rajivan and Jean Camp. 2016. Influence of Privacy Attitude and Privacy Cue Framing on Android App Choices. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. USENIX Association, Denver, CO, 7. https://www.usenix.org/conference/soups2016/workshop-program/wpi/presentation/rajivan

[98] Jennifer A. Rode. 2009. Digital Parenting: Designing Children's Safety. In *Proceedings of the 23rd British HCI Group Annual Conference on People and Computers: Celebrating People and Technology (BCS-HCI '09)*. British Computer Society, Swinton, UK, 244–251. http://dl.acm.org/citation.cfm?id=1671011.1671041

[99] Daniela K. Rosner and Morgan Ames. 2014. Designing for Repair?: Infrastructures and Materialities of Breakdown. In *Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW '14)*. ACM, New York, NY, USA, 319–331. https://doi.org/10.1145/2531602.2531692

[100] Ira S. Rubenstein and Nathaniel Good. 2013. Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents. *Berkeley Technology Law Journal* 28, 2 (2013), 1333–1413.

[101] Matthew Rueben, Frank J. Bernieri, Cindy M. Grimm, and William D. Smart. 2016. User feedback on physical marker interfaces for protecting visual privacy from mobile robots. In *2016 11th ACM/IEEE International Conference on Human-Robot Interaction (HRI)*. IEEE, Christchurch, New Zealand, 507–508. https://doi.org/10.1109/HRI.2016.7451829

[102] Florian Schaub, Rebecca Balebako, Adam L. Durity, and Lorrie Faith Cranor. 2015. A Design Space for Effective Privacy Notices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. USENIX Association, Ottawa, 1–17. https://www.usenix.org/conference/soups2015/proceedings/presentation/schaub

[103] Phoebe Sengers, Kirsten Boehner, Shay David, and Joseph 'Jofish' Kaye. 2005. Reflective Design. In *Proceedings of the 4th Decennial Conference on Critical Computing: Between Sense and Sensibility (CC '05)*. ACM, New York, NY, USA, 49–58. https://doi.org/10.1145/1094562.1094569

[104] Katie Shilton. 2018. Values and Ethics in Human-Computer Interaction. *Foundations and Trends® in Human–Computer Interaction* 12, 2 (2018), 107–171. https://doi.org/10.1561/1100000073

[105] Christo Sims. 2017. The Politics of Design, Design as Politics. In *The Routledge Companion to Digital Ethnography*, Larissa Hjorth, Heather Horst, Anne Galloway, and Genevieve Bell (Eds.). Routledge, New York, Chapter 40, 439–447.

[106] Indrajeet Singh, Srikanth V. Krishnamurthy, Harsha V. Madhyastha, and Iulian Neamtiu. 2015. ZapDroid: Managing Infrequently Used Applications on Smartphones. In *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '15)*. ACM, New York, NY, USA, 1185–1196. https://doi.org/10.1145/2750858.2807550

[107] Daniel J. Solove. 2002. Conceptualizing privacy. *California Law Review* 90 (2002), 1087–1155.

[108] Daniel J. Solove. 2003. A Taxonomy of Privacy. *University of Pennsylvania Law Review* 154, 3 (2003), 477–560.

[109] Sarah Spiekermann and Lorrie Faith Cranor. 2009. Engineering Privacy. *IEEE Transactions on Software Engineering* 35, 1 (Jan 2009), 67–82. https://doi.org/10.1109/TSE.2008.88

[110] Luke Stark, Jen King, Xinru Page, Airi Lampinen, Jessica Vitak, Pamela Wisniewski, Tara Whalen, and Nathaniel Good. 2016. Bridging the Gap between Privacy by Design and Privacy in Practice. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA '16)*. ACM, New York, NY, USA, 3415–3422. https://doi.org/10.1145/2851581.2856503

[111] April Suknot, Timothy Chavez, Nathan Rackley, and Patrick Gage Kelley. 2014. Immaculacy: A Game of Privacy. In *Proceedings of the first ACM SIGCHI annual symposium on Computer-human interaction in play - CHI PLAY '14*. ACM Press, New York, New York, USA, 383–386. https://doi.org/10.1145/2658537.2662971

[112] Karen Tang, Jason Hong, and Dan Siewiorek. 2012. The implications of offering more disclosure choices for social location sharing. In *Proceedings of the 2012 ACM annual conference on Human Factors in Computing Systems - CHI '12*. ACM Press, New York, New York, USA, 391. https://doi.org/10.1145/2207676.2207730

[113] U.S. Department of Homeland Security. 2008. Privacy Impact Assessment for TSA Whole Body Imaging. https://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-tsa-wbi-jan2008.pdf

[114] Max Van Kleek, Dave Murray-Rust, Amy Guy, Kieron O'Hara, and Nigel Shadbolt. 2016. Computationally Mediated Pro-Social Deception. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems - CHI '16*. ACM, New York, NY, USA, 552–563. https://doi.org/10.1145/2858036.2858060

[115] Jessica Vitak, Pamela Wisniewski, Xinru Page, Airi Lampinen, Eden Litt, Ralf De Wolf, Patrick Gage Kelley, and Manya Sleeper. 2015. The Future of Networked Privacy: Challenges and Opportunities. In *Proceedings of the 18th ACM Conference Companion on Computer Supported Cooperative Work & Social Computing (CSCW'15 Companion)*. ACM, New York, NY, USA, 267–272. https://doi.org/10.1145/2685553.2685554

[116] Jeffrey Warshaw, Nina Taft, and Allison Woodruff. 2016. Intuitions, Analytics, and Killing Ants: Inference Literacy of High School-educated Adults in the US. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. USENIX Association, Denver, CO, 271–285. https://www.usenix.org/conference/soups2016/technical-sessions/presentation/warshaw

[117] Langdon Winner. 1980. Do Artifacts Have Politics? *Daedalus* 109, 1 (1980), 121–136.

[118] Pamela Wisniewski, Jessica Vitak, Xinru Page, Bart Knijnenburg, Yang Wang, and Casey Fiesler. 2017. In Whose Best Interest? Exploring the Real, Potential, and Imagined Ethical Concerns in Privacy-Focused Agenda. In *Companion of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW '17 Companion)*. ACM, New York, NY, USA, 377–382. https://doi.org/10.1145/3022198.3022660

[119] Jacob O. Wobbrock and Julie A. Kientz. 2016. Research Contributions in Human-computer Interaction. *Interactions* 23, 3 (April 2016), 38–44. https://doi.org/10.1145/2907069

[120] Richmond Y. Wong and Vera Khovanskaya. 2018. Speculative Design in HCI: From Corporate Imaginations to Critical Orientations. In *New Directions in 3rd Wave HCI*, Michael Filimowicz (Ed.). Springer International, Cham, 175–202. https://doi.org/10.1007/978-3-319-73374-6_10

[121] Richmond Y. Wong, Deirdre K. Mulligan, Ellen Van Wyk, James Pierce, and John Chuang. 2017. Eliciting Values Reflections by Engaging Privacy Futures Using Design Workbooks. *Proc. ACM Hum.-Comput. Interact.* 1, CSCW, Article 111 (Dec. 2017), 26 pages. https://doi.org/10.1145/3134746

[122] Richmond Y. Wong, Ellen Van Wyk, and James Pierce. 2017. Real-Fictional Entanglements: Using Science Fiction and Design Fiction to Interrogate Sensing Technologies. In *Proceedings of the 2017 Conference on Designing Interactive Systems (DIS '17)*. ACM, New York, NY, USA, 567–579. https://doi.org/10.1145/3064663.3064682

[123] Bin Xu, Pamara Chang, Christopher L Welker, Natalya N Bazarova, and Dan Cosley. 2016. Automatic Archiving versus Default Deletion: What Snapchat Tells Us About Ephemerality in Design. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing - CSCW '16*. ACM Press, New York, New York, USA, 1660–1673. https://doi.org/10.1145/2818048.2819948

[124] Yaxing Yao, Huichuan Xia, Yun Huang, and Yang Wang. 2017. Privacy Mechanisms for Drones: Perceptions of Drone Controllers and Bystanders. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems - CHI '17*. ACM Press, New York, New York, USA, 6777–6788. https://doi.org/10.1145/3025453.3025907

[125] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End User Security and Privacy Concerns with Smart Homes. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. USENIX Association, Santa Clara, CA, 65–80. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/zeng

[126] Leah Zhang-Kennedy and Sonia Chiasson. 2016. Teaching with an Interactive E-book to Improve Children's Online Privacy Knowledge. In *Proceedings of the The 15th International Conference on Interaction Design and Children - IDC '16*. ACM, New York, NY, USA, 506–511. https://doi.org/10.1145/2930674.2935984

[127] Leah Zhang-Kennedy, Christine Mekhail, Yomna Abdelaziz, and Sonia Chiasson. 2016. From Nosy Little Brothers to Stranger-Danger: Children and Parents' Perception of Mobile Threats. In *Proceedings of the The 15th International Conference on Interaction Design and Children - IDC '16*. ACM, New York, NY, USA, 388–399. https://doi.org/10.1145/2930674.2930716

[128] John Zimmerman, Jodi Forlizzi, and Shelley Evenson. 2007. Research through design as a method for interaction design research in HCI. In *Proceedings of the SIGCHI conference on Human factors in computing systems (CHI '07)*. ACM, New York, NY, USA, 493. https://doi.org/10.1145/1240624.1240704