Chapter 2
Privacy Theories and Frameworks

Pamela J. Wisniewski and Xinru Page

Abstract This chapter introduces relevant privacy frameworks from academic literature that can be useful to practitioners and researchers who want to better understand privacy and how to apply it in their own contexts. We retrace the history of how networked privacy research first began by focusing on privacy as information disclosure. Privacy frameworks have since evolved into conceptualizing privacy as a process of interpersonal boundary regulation, appropriate information flows, design-based frameworks, and, finally, user-centered privacy that accounts for individual differences. These frameworks can be used to identify privacy needs and violations, as well as inform design. This chapter provides actionable guidelines for how these different frameworks can be applied in research, design, and product development.

2.1 Introduction

Since privacy is a complex, multifaceted concept, it is unlikely that a single theory or framework can provide the foundation for all privacy research. Yet, a comprehensive understanding of the relevant privacy theories can lead to better connections between research and practice. In this chapter, we provide an overview of some of the most prominent privacy frameworks in the human-computer interaction (HCI) networked privacy literature. One way to solve the problem of the often fragmented and erratic use of the term privacy is to converge on a set of core privacy theories and frameworks that can meaningfully inform our scholarly work and provide a common foundation in which to move our field forward.

P. J. Wisniewski (✉)
Department of Computer Science, University of Central Florida, Orlando, FL, USA
e-mail: pamwis@ucf.edu

X. Page
Brigham Young University, Provo, UT, USA
e-mail: xinrupage@byu.edu

B. P. Knijnenburg et al. (eds.), *Modern Socio-Technical Perspectives on Privacy*,
https://doi.org/10.1007/978-3-030-82786-1_2

In this chapter, we provide an overview of the following:

- Privacy as information disclosure
- Privacy as interpersonal boundary regulation
- Privacy as contextual norms
- Privacy as affordances and design
- User-centered privacy and individual differences

By consolidating this knowledge and providing practical guidelines on how to apply these theories, this chapter will also help researchers and practitioners ascertain which privacy theories and/or frameworks may be useful when conducting empirical social computing research in HCI or when attempting to translate this research into practice. In the following sections, we compare and contrast four primary ways in which privacy frameworks have been constructed and studied in the human-computer interaction and computing literature: (1) privacy as information disclosure, (2) privacy as interpersonal boundary regulation, (3) privacy as context and norms, and (4) privacy as design. We present the case that modern privacy research is moving toward more user-centered and proactive approaches, which attempt to consider individual differences (see Chaps. 7 and 16), including the needs of vulnerable populations (see Chap. 15). By applying these frameworks, researchers and practitioners will be more equipped to meet users' privacy needs in an era of intense public scrutiny around networked technologies and privacy protection.

2.2 Privacy as Information Disclosure

Section Highlights

- Before the advent of social media, **networked privacy was viewed as a form of information disclosure** in which individuals control what personal information to withhold from others.
- **Privacy concern** has been studied as a key factor in individuals' information disclosure decisions, and people have been shown to perform a **privacy calculus** to weigh the **benefit versus the cost** of disclosing personal information.
- Yet, **privacy paradox** research has shown that there is often a **disconnect between an individual's privacy concern and their information disclosure behavior**.

Privacy, particularly within the Information Systems (IS) field, is often defined as "the ability of individuals to control when, to what extent, and how information about the self is communicated to others" [1]. Even with the different conceptualizations of privacy, one commonality among many fields is the unilateral emphasis on privacy as it relates to *information disclosures*. Viewing privacy as control over one's information disclosures treats privacy as a somewhat dichotomous boundary between private and public information disclosures [2]. As such, several information privacy models have been developed; a commonality among these frameworks is

that the focus has been on privacy as withholding or divulging information [3]. For example, Smith et al. (1996) [4] developed the **concern for information privacy** (CFIP) scale in the context of offline direct marketing. It consisted of 15 items and 4 dimensions: collection, errors, secondary use, and unauthorized access to information. Each dimension represented a privacy concern for a type of information misuse. People differed in their concern for (1) data collection, (2) whether the data was represented faithfully, (3) whether data was used for its originally intended purpose, and (4) if data was used by an unauthorized third party. They used this scale to measure an individual's concern about organizational information privacy practices, as they considered information privacy one of the most important ethical concerns of the information age.

Malhotra et al. (2004) [5] extended this work from organizational contexts to the online world to develop the **Internet users' information privacy concerns** (IUIPC) scale. This scale consisted of three dimensions identified as the most pressing for online privacy concerns: collection, control, and awareness of privacy practices. Anton et al. (2010) [6] provided a more fine-grained version of IUIPC by including access/participation, information collection, information storage, information transfer, notice/awareness, and personalization as additional factors to consider. CFIP and IUIPC have been and continue to be widely used in many studies as a way to characterize privacy concerns. Xu et al. [3] also studied information privacy online and developed their "information boundary theory" by studying privacy attitudes on information disclosure across e-commerce, finance, healthcare, and social networking websites. They found that privacy intrusion, risk, and control were all important factors related to privacy concerns in the context of social networking websites. This provided guidance on the common elements to be considered when studying information privacy across various online contexts.

In 2011, Smith et al. [7] created a comprehensive framework widely used for understanding information privacy research, called the Antecedents-Privacy Concerns-Outcomes model (or "APCO" model; see Chap. 3). It considers not only the privacy concerns that people have but also the antecedents that shape those concerns, as well as the consequences or outcomes of such concerns. Antecedents such as personal traits, contextual factors, regulatory forces, and technology attributes have been connected to increased or decreased privacy concerns [8, 9]. Consequences resulting from privacy concerns include fewer disclosures or reduced technology use [10]. Much of the privacy research in this space unpacks how heightened privacy concerns can adversely affect users' online engagement. In fact, researchers have studied in detail how people translate their privacy appraisals into information disclosure behaviors across multiple domains from retail online consumerism, social networking, to healthcare. In the next section, we introduce this decision-making process, which is called privacy calculus.

2.2.1 *Privacy Calculus: Assessing the Benefit vs. Cost of Information Disclosures*

When privacy is framed as withholding or disclosing personal information, researchers have found that people often undergo a cost-benefit analysis to make privacy decisions. In other words, they consider the tradeoff between the cost and gain of disclosing their personal information to a particular source, a phenomenon known as "privacy calculus" [11]. This view of privacy decision-making explains how, despite privacy concerns, people may still disclose information if they perceive that the benefits outweigh the risks. Conversely, the absence of privacy concern is not enough to lead to disclosure when there is no perceived benefit. This aligns with a commodity view of privacy where it can be given up for some sort of benefit. Much of the privacy economic research community takes this view on privacy, putting a monetary value on the cost of giving up one's privacy versus a monetary value on the benefits reaped by doing so [12, 13].

Over the past decade, researchers have identified both positive and negative outcomes associated with online personal information disclosures, ranging from how disclosure facilitates access to social support and resources [14–16] to how it may make some users more vulnerable to harassment [17–19]. Much research has focused on how disclosing on social networking sites allows users to gain social capital [16, 20], strengthen their relationships with others [15], improve their well-being [21], and even increase employee performance [22] and innovation [23]. However, there is also research that has uncovered drawbacks of disclosure, including reputational harm, losing one's job, and financial harm [24, 25].

In terms of systematically assessing the drawbacks of information disclosures, there are various types of activities that can pose threats to one's privacy. Most notably, Solove developed a framework consisting of privacy violations that can arise from information disclosure. Solove's **taxonomy of privacy threats** identifies four types of threats [26]. *Information collection* describes threats resulting from collecting sensitive information (e.g., financial or location information) about someone. *Information processing* threats arise from how collected data is used or stored and often can occur when data is used in a way that differs from its originally intended usage. *Information dissemination* threats arise from sharing collected information with others not originally intended to have access to the data. *Invasion*-type threats have to do with disturbing one's solitude or tranquility (e.g., inundating them with too much information or constantly interrupting them).

Another theoretical lens commonly used in information privacy research is **uses and gratification theory** [27, 28]. This theory focuses on user goals and ties user behaviors to those goals. Disclosure is not driven purely by degree of privacy sensitivity; it is rather driven by higher-level motivations of use and the associated privacy concerns that may impact technology use [29]. In fact, different ways of disclosing information often stem from different goals; for instance, posting a status on a Facebook timeline is not the same as sharing through a different mechanism, despite similar capabilities [30]. In practice, people are likely to differ

in terms of what kinds of privacy benefits and violations they consider important for themselves. For instance, Page et al. [31] point out that collecting one's location data might unsettle some people but not others. Namely, some users avoid posting information about themselves online because of privacy concerns, while others consider it a matter of convenience to be able to do so [32].

Yet, while individual differences are to be expected, research has uncovered inconsistencies at the individual level, where some claims to be privacy concerned, yet their behavior seems to reflect a lack of this concern [33]. As such, the disconnect between an individual's stated privacy concerns and the privacy calculus people use to make information disclosure decisions gave rise to a new body of research on the privacy paradox, which we cover next.

2.2.2 *Privacy Paradox: The Discrepancy Between Users' Privacy Concerns and Information Disclosure Behavior*

Studies that have tried to predict users' information disclosure behavior have produced mixed results, often showing an individual's information disclosure behavior does not reflect their stated privacy concerns [13, 34, 35]. This mismatch between stated concerns and actual behavior has been called the "privacy paradox" [34, 36]. This research concludes that users may not always weigh costs and benefits in what one might consider to be a rational way. Some scholars explain how limits on human memory and reasoning capabilities lead to a *bounded rationality*, where people resort to satisficing behaviors and heuristics to make decisions [37]. For example, privacy research shows hyperbolic discounting, where future consequences are not weighted as heavily as immediate gratifications [38]. Research also shows that certain individuals are more likely to rely on heuristics than others [39]. Moreover, while users claim to *want* full control over their data (c.f., [40–48]), they do not actually exploit this control, which also creates a paradox between privacy and control [33, 49].

As user interactions and transactions increasingly move online [50], people must learn how to manage their online privacy, which requires more intentional and explicit disclosure decisions. Indeed, networked social interactions can be much more difficult to navigate when one's audience and social contexts shift often and blur [13, 51]. The nuance of nonverbal and social cues that people have acquired and mastered in offline contexts over the years and the ambiguity and fleeting nature of interactions possible offline give way to explicit online actions and digitized representations [52]. Being able to anticipate audience and subsequent consequence of a disclosure can be extremely challenging and difficult, given the design and properties of online technologies. Thus, people often imagine they are disclosing to a given audience, but this does not match up with the reality of who is privy to that information [40, 53]. This disconnect may partially explain why people's expressed privacy concerns do not always match up with their information disclosure behaviors.

2.2.3 *Westin's Privacy Taxonomy: The Classification of Consumers' Privacy Knowledge and Preferences*

Many scholars have attempted to classify people based on their information disclosure behaviors and/or preferences. One of the most commonly cited is the **Westin classification of consumers' privacy knowledge and preferences**, which maintains that people can be categorized as *privacy fundamentalists* who highly value protecting their privacy, *privacy pragmatists* who are willing to weigh pros and cons of disclosure, and *privacy unconcerned* who do not value privacy [54–56]. However, these classifications lack empirical support, and recent work has questioned their effectiveness for predicting online behavior [57]. In fact, research shows that classification may need to consider not just the amount of disclosure that one is willing to make but also the type of information that people are willing to share [57, 58]. Furthermore, even types of online activity may differ. Rather than looking just at disclosure, scholars should consider the use of privacy protecting measures, feature use, and type of interactions [30, 59, 60].

As Westin's taxonomy suggests, there are many individual differences that can help explain seemingly paradoxical information disclosure behaviors. Studies have uncovered differences in gender [61–63], age [51], and prior experiences [64] as well as varying social norms [65, 66] and network compositions [67] that shape whether and how people choose to disclose information, leverage privacy features, and manage their privacy. And while people may deal with the context collapse of their many social circles colliding (e.g., boss, friend, and family) by adjusting what they disclose or using privacy features, others may not for fear of harming their relationships [60] or may lack digital literacy to realize the issue or how to fix it, leading to regrets [18, 24, 68]. Researchers continue to identify other individual and group-level factors and social contexts that help explain the privacy paradox [52, 69]. These factors involve understanding social norms and context, as well as viewing privacy behaviors at a dyadic level by honing in on interpersonal relationships [70]. We discuss these approaches in more detail in the sections that follow.

2.3 Privacy as an Interpersonal Boundary Regulation Process

Section Highlights

- Privacy has been conceptualized as a **dialectical process of managing interpersonal boundaries with others**. In other words, it is a dynamic and ongoing process of setting boundaries between, e.g., what is shared or withheld, being accessible or inaccessible to interaction with others, presenting a certain identity and not others.

- **Altman saw boundary regulation as a process of opening and closing oneself to others**, which could lead to a state of social isolation on one extreme or social crowding on the other extreme, when boundary mechanisms did not allow people to achieve their desired level of privacy.
- **Petronio created a framework of communication privacy management**, which is the process of disclosing or withholding personal information. When information is shared, it becomes co-owned by others who then are participants in privacy management.

The networked privacy research community has studied the type of information people share online and the factors that influence what they share [71, 72]. However, privacy is not limited to what people share online. Privacy, as a construct for social contexts, extends beyond information disclosure decisions to a broader range of social interactions that require regulating interpersonal boundaries. It also involves the management of interpersonal boundaries that help regulate users' interactions, both positive and negative [73]. This includes physical and communicative accessibility, emotional and psychological well-being, and reputation and impression management boundaries. As such, scholars have drawn from a broader *social privacy* perspective to explain privacy as a process of boundary regulation. We describe some of the most prominently used theories below.

2.3.1 Altman's Conceptualization of Privacy

Social psychologist Irwin Altman defined privacy as "an **interpersonal boundary process** by which a person or group regulates interaction with others," by altering the degree of openness of the self to others [74]. This process is dialectic in nature, balancing both the restriction and seeking of social interaction with others. Interpersonal boundaries are important because they help users define self, give protection (physically and emotionally), help manage our personal resources, and forge deeper relationships with others [74]. The boundary regulation process allows for feedback and readjustment along with a dynamic need for varying levels of separateness and togetherness. According to Altman, boundary mechanisms are behaviors (e.g., body language, eye contact, physical distance) employed in combination and adjusted over time to achieve one's desired level of privacy. Individuals have different mechanisms for erecting boundaries, and they adjust these mechanisms as their needs change [74].

Although Altman's work on boundary regulation was initially confined to the physical world, it has been used heavily to frame research in privacy in social media [2, 75, 76], which will be covered in more detail in Chap. 7. For instance, Stutzman and Hartzog [75] examined the creation of multiple profiles on social media websites, primarily Facebook, as an information regulation mechanism. They identified three types of boundary regulation within this context: (1) *pseudonymity*, a profile that was fully disassociated from personally identifiable information as

to conceal one's identity; (2) *practical obscurity*, an alternate profile created by obscuring some aspect of personally identifiable information to make it harder to find; and (3) *transparent separations*, no attempt to obscure or conceal information but multiple profiles for the sake of practical separation (e.g., personal versus professional) [75]. Lampinen et al. [2] likewise focused on boundary management strategies and created a framework for managing private versus public disclosures. Their framework defined three dimensions by which strategies differed: behavioral vs. mental, individual vs. collaborative, and preventative vs. corrective. For instance, a preventative strategy would be sharing content to a limited audience, while a corrective strategy would be deleting content after the fact. Wisniewski et al. [77] also built upon Altman's theory to empirically show how different social media users have different privacy management strategies (which they refer to as "profiles") on Facebook. A user's privacy strategy related to their awareness of the privacy settings and features available to manage privacy desires. The concept of creating privacy profiles for user-tailored privacy will be covered in more depth in Chap. 16.

Most notably, Palen and Dourish [78] explain how extending Altman's work to the networked world manifests in more than the boundary regulation of disclosures. It also manifests as other privacy boundaries, such as identity (i.e., choosing who you appear as to others and how you behave toward them) and temporality (i.e., the persistence of content and performing actions based on perceptions of the past or future). Furthermore, while disclosing or withholding information is commonly recognized as a privacy boundary that, respectively, lowers or increases privacy, the authors point out that each of these mechanisms can serve the opposite privacy goal. For example, disclosing information can actually serve to increase privacy. Posting information might be a way to prevent people from asking for the information and protect the discloser from interruptions and a deluge of requests. In the next section, we introduce Petronio's communication privacy management theory, which was an extension of Altman's earlier work.

2.3.2 Petronio's Communication Privacy Management Theory

Building on Altman's conceptualization of privacy, Petronio's **communication privacy management** (CPM) **theory** [79] outlined five suppositions related to disclosure boundaries. First, a boundary exists between private and public information. Second, disclosure privacy deals specifically with the disclosure of private information (as opposed to information that is not considered private). Third, individuals have a sense of ownership or control regarding this private information. Fourth, a rule-based system defines how individuals manage this privacy boundary. Namely, Petronio defines boundary linkages, which are "connections that form boundary alliances" [79]. These are the people who have come to know this private information, whether it be an intentional disclosure or someone overhearing a conversation. The idea of co-ownership deals with the privilege to have joint

ownership of one's private information, and permeability deals with "how opened or closed the collective boundaries are once they are formed" [79]. If only a single person knows, the boundary is very thick and less permeable than if many people know, and there is more of a chance of disclosure. Therefore, disclosure boundaries require a coordination process between co-owners of private information. Fifth, this process is dialectical in nature. In other words, Petronio drew from Altman's theory to reiterate that an individual's desire for information privacy may change over time.

CPM also delineated between two different interpersonal boundaries: personal and collective. *Personal boundaries* deal with how one shares private information about one's self, while *collective boundaries* involve private information shared with others. "A boundary is transformed from a personal to a collective when someone self-discloses to a confidant," [79] explained Petronio. Child and Agyeman-Budu [80] applied Petronio's CPM to blogging disclosures made by young adults on websites such as MySpace, Facebook, and LiveJournal. They found that high self-monitoring bloggers displayed more privacy-oriented management practices than bloggers who were low self-monitors, but high self-monitors also tended to blog more often. They further found support that individuals with higher Concern for Appropriateness (CFA), aka cared more about whether they come across appropriately, had more permeable privacy boundaries, so they disclosed in more detail and with higher frequency than bloggers with low CFA [80]. A number of other researchers have extended Petronio's CPM theory into the domain of HCI by trying to design interfaces and create models to help users understand and alleviate collective privacy concerns [81, 82]. For example, Jia and Xu developed the SNS collective privacy concerns (SNSCPC) scale to measure an individual's collective privacy concerns across three dimensions: collective information control, access, and diffusion [82].

In contrast to treating privacy as information disclosure, viewing privacy as a process of interpersonal boundary regulation broadens the conceptualization of privacy to include varying aspects of human behavior. For instance, Wisniewski et al. [69] identified and measured the multidimensional facets of interpersonal privacy preferences for social networking site users. They found that privacy boundaries included self-disclosure decisions but went beyond self-disclosure to also include confidant disclosures (co-owned information shared by others), relationship boundaries (e.g., deciding with whom to connect), network boundaries (e.g., giving others access to one's connections), territorial boundaries (e.g., managing content and interactions across public, semipublic, and private spaces), and interactional boundaries (e.g., the ability to make oneself unavailable to others). Taking this more interpersonal perspective to modern privacy acknowledges that people are inherently social, and privacy must be considered in relation to sociality rather than in isolation.

In the next section, we discuss how researchers have started to embed privacy more fully within social contexts by considering contextual factors beyond information and interpersonal relationships. They also consider how social contexts, norms, and values shape privacy outcomes.

2.4 Privacy as Social Context, Norms, and Values

Section Highlights

- **Nissenbaum's framework of contextual integrity describes privacy as the appropriate flow of information** based on contextual factors, such as social norms.
- **Privacy decisions cannot be made optimally without considering context**, which includes the type of information being shared, the actors involved, and the mechanisms and purpose in which information sharing occurs.
- **Social norms and values are critically important when identifying appropriate information flows** and whether privacy violations are likely to occur.

Most recently, a norm-based theory of privacy has gained traction. Nissenbaum's **contextual integrity** (CI) has been used to identify privacy violations in diverse situations. In fact, the theory recognizes that people interact within a wide variety of contexts, where each context is associated with expectations for who should share what type of information to whom and in what circumstances. Privacy management is a process of negotiating these social norms and assumptions held by the individuals [83].

More specifically, the CI framework defines elements that should be considered in determining or defining privacy violations [84]. First, the *context* (e.g., school, work) is the social space that sets the stage for privacy expectations. Next, there are several *actors* involved, such as the information sender, recipient, and the individual who is the subject of the information. Also relevant is the *type* of the information being shared (e.g., medical, academic records). Finally, there are *transmission principles* which are rules for how the information can be transferred from actor to actor.

Often a change in one element causes privacy expectations to be violated. For example, a school sending a student's parents their academic records through a password-protected parent portal may be appropriate. However, once any of those actors change, there can be problems. If it is a different student's records, or if the recipient is a journalist, these are all privacy violations. Or if the transmission mechanism changes, such as using a publicly accessible website, again a privacy violation occurs. In fact, when we apply this framework to the latest developments in personalized and algorithmically driven technologies, we see that there may be ambiguity and uncertainty about social norms. Sometimes the actor is not human but an autonomous agent acting on behalf of someone or some organizational entity. Considering whether these are appropriate flows of information is crucial when defining how information should flow in a privacy-sensitive way.

In the following sections, we elaborate on how to apply the CI framework when designing new technologies or studying the use of existing ones. It can serve as a set of heuristics that can be used systematically to guide researchers and practitioners toward the elements important to privacy. We first describe how social contexts need to be considered in designing for privacy. Then, we can turn to the privacy norms and human values [84]. Finally, we discuss how to put CI into practice.

2.4.1 Considering Social Contexts

Information sharing and interpretation and interpersonal interaction occur within a broader social context (e.g., at school, doctor's office, at home). These social contexts are what shape and define social life, each consisting of "canonical activities, roles, relationships, norms (or rules), and internal values (goals, ends, purposes)" [84]. The roles and activities that occur at school are different than the ones found in a doctor's office. Thus, sharing one's weight with the doctor will be interpreted and used for different purposes by the physician than if it were disclosed in a class setting with classmates and the teacher. While much past privacy research has emphasized giving users control over their data, the CI framework asserts that people are more interested in *appropriate* information disclosures. Social contexts provide an existing social structure for determining appropriate information sharing (i.e., sharing for what purpose, in what way, and by, to, and about whom). Being able to rely on these social contexts that have shaped our collective expectations of appropriate behavior and information sharing allows people to establish shared expectations around what values are being furthered and thus what is the appropriate behavior. In an educational setting, information sharing and behaviors should be aimed at student growth and learning. In this context, a common technique is identifying mistakes, so that students can learn from these mistakes and demonstrate mastery by the end of the course. This could be contrasted with the workplace value of productivity where the employee may be expected to have a high level of performance and identifying a mistake instead negatively impacts the employee's performance evaluation. Information that serves a helpful purpose in one social context may be harmful in another. Similarly, in a healthcare context, sharing accurate details about patient behavior and health habits may help physicians hone in on a more accurate diagnosis, improving quality of life. Yet, the same information may be considered incriminating in a workplace context if health information can lead to discrimination against those whose are perceived as having less healthy habits. These examples illustrate how social context sets the backdrop for interpreting appropriateness of information sharing. While many social contexts are now facilitated online, such as patient portals in healthcare, we can still draw on those values and norms that are implicit in these social contexts to understand expectations of privacy online.

2.4.2 Identifying Privacy Norms and Human Values in Design

Given a social context, there are privacy norms around who can share what information about whom and with whom and under what circumstances (i.e., when, where, how, for what purpose). All these factors can play a part in determining "appropriate information flows," namely, when it is acceptable to share information. Probing on these various dimensions of who, what, where, when, why, and how can

give a fuller picture of privacy norms. For example, a common factor that determines appropriateness is the recipient of information. Medical records shared with one's doctor may be appropriate, while sharing with one's employer may be less so. Other research has found that revealing one's location to people located in the same city may be more acceptable than doing so to those further away [85]. Another important dimension that is relevant to privacy norms is the type of information being shared. For instance, studies have shown that people may worry about inferences made based on their past purchases, web browsing history, or emails [58]. Especially without an understanding of the context in which these behaviors occurred, the information could prove embarrassing when shared with certain audiences [86] or be perceived by an employer in a way that could threaten one's employment. As such, norms around privacy are an important consideration across different contexts, groups, individuals, and cultures.

Understanding the norms that are considered appropriate across different social contexts allows us to identify the expectations that people have established around privacy. However, when introducing new technologies, there may be new factors to consider such as competing values embedded by the technology, new information dissemination mechanisms, and human and nonhuman actors. Online technologies may even create new social contexts or allow disparate ones to converge into one virtual space. This convergence of values and technology capabilities can lead to conflicts between actors and make it difficult to anticipate what the privacy norms should be. Friedman et al.'s value-sensitive design framework identifies how considering different values can uncover these tensions and should be a part of the design process [87]. Value sensitive design is a theoretically grounded approach to systems design that accounts for human values in a principled manner throughout the design process, including conceptual, empirical, and technical investigations. Value sensitive design helps researchers and designs both reflectively identify and proactively embed values that are of moral importance in the design of systems [87].

Privacy norms and values go together. Identifying the appropriate privacy norms involves answering questions around appropriate ways to collect information and what type of data is necessary to support the values of the given social context in a technology-mediated form. Considering the feature capabilities and data format preferences of users is also relevant for uncovering factors that could affect attitudes about appropriateness of information flows. Although users commonly provide systems with feedback about their preferences [88], they may not be able to accurately anticipate and express their data collection preferences [89], given the complexity of understanding how information is collected, stored, processed, and used [90]. To determine appropriate data collection and information flow, starting by observing people's disclosure behaviors [91] can allow designers to discover expectations of appropriate information sharing for a social context. Then, they must work to uphold those expectations in the way the data is handled by the system, being sensitive to the social context and not letting technology capabilities override the values and norms of that context. For instance, one of the values emphasized in healthcare is confidentiality, an underlying principle of the Hippocratic Oath: "I will respect the privacy of my patients, for their problems are not disclosed to me

that the world may know" [92]. However, healthcare technologies may have the default values of storing information indefinitely and making it easily accessible to anyone. Thus, the conflicting capabilities and norms around the social context and the medium through which information is conveyed (and recorded) must be reconciled. Designers can decide to respect the norms of the social context and build strict access limitations so that the principle of confidentiality is supported.

Next, we give an example how the framework of CI can be applied in practice.

2.4.3 Applying Contextual Integrity to Practice

Empirical research has shown that people's contextual privacy concerns align well with the CI framework. Wang et al.'s study on drone bystanders' privacy shows that people's privacy concerns about drone usage are highly dependent on context and purpose (e.g., using a drone in a friend's party for personal recording use causes less concerns) [93]. In another example, Ayalon and Toch concluded that users were less willing to share older content on online social networks as a result of norm changes [94]. Yet, some research suggests that the CI framework (as well as other theoretical and conceptual frameworks) is often mentioned within empirical privacy research without a strong integration of the theory [95]. For instance, Badillo-Urquiola et al.'s [38] initial review of the recent HCI literature that invoked CI as a privacy framework found that most of these studies did not deeply engage with CI beyond mentioning it in the background or discussion sections either to motivate or explain their findings.

Figure 2.1 summarizes the key dimensions of contextual integrity, and we use this framework to unpack two examples of how CI could be applied to understand recent privacy violations that surfaced in the news media.

In 2018, Uber and Lyft garnered negative press from news media as some drivers were caught livestreaming their rides over the Internet [96]. By applying the framework of contextual integrity, we can understand why this was considered a violation of privacy and trust. The type of information being shared was a video/audio feed. The actors involved included the passengers (subject), driver (sender), and the public (recipient). The transmission principle involved sending this information without the consent of the subject and for the profit of the recipient. Given that notice and informed consent are often social norms around sharing personal content about an individual, this was clearly a violation of privacy. However, what if the recipient of the information and transmission principle changed, while all other factors remained constant? For instance, if Lyft or Uber (sender) made it standard policy that all drivers post a notice that video recording was implemented for security purposes (transmission principle) and only shared with the security company (recipient) who was contractually hired by the company, the public discourse around this issue would be very different. Instead of outcries about privacy violations, it is possible that Uber or Lyft could have been lauded for their efforts in protecting the physical safety of both drivers and passengers.

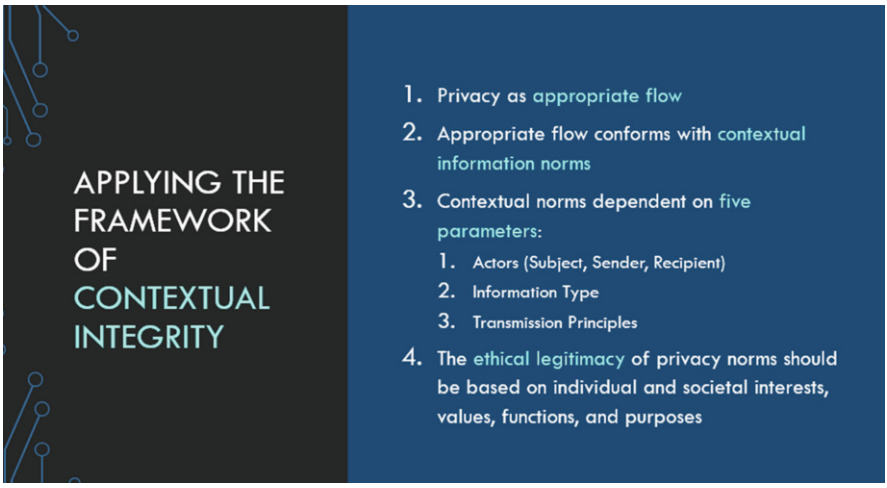

Fig. 2.1 Summary of the framework of contextual integrity

While many of the examples in the previous sections involve data connected to a readily identifiable individual, note that privacy threats still exist even when data is collected from anonymous users [97]. The data can still lead to identification of an individual because of inferences made from the content or the record of the user's social connections [98]. Thus, context is key to the interpretability of any given information, and simply removing typical personal identifiers does not guarantee privacy.

In short, context matters when it comes to the appropriate flow of information. As such, future research could benefit from using CI to inform the design of their study, system, or even their qualitative codebooks. Meanwhile, some researchers have chosen to focus on more tangible elements of privacy, such as design.

2.5 A Privacy Affordance and Design Perspective

Section Highlights

- **Affordances** are perceptions of what the user can do with a technical object, e.g., deleting information or recording a conversation.
- **Privacy expectations** and behaviors are shaped by affordances of technology.
- **Privacy by Design** is a set of principles for translating privacy concepts proactively into the **design of systems**.

The end goal of developing privacy theories and frameworks is often to translate these principles into actionable design guidelines or system specifications that meet end users' needs. Given that networked privacy hails primarily from the HCI research community, privacy affordances and design are two major streams

of research that are useful to this end. Unlike the previous frameworks and theories, the affordance and design perspectives focus more on tangible outcomes toward implementation. Therefore, it might be beneficial to apply the former research when conducting formative analyses of users' needs and the approaches below when further down the systems developmental life cycle. In other words, combining these multiple perspectives can both inform what users' needs should be considered, how design can meet these needs, and how systems can be built and deployed in a privacy conscious way.

2.5.1 Privacy Affordances

Several researchers [99–102] have taken an affordance perspective on privacy. **Technological affordances** represent "relationship between a technical object and a specified user (or user group) that identifies what the user may be able to do with the object, given the user's capabilities and goals" (p. 622) [103]. In other words, objects can be used by people in certain ways based on their physical or technical properties. In the offline world, a dial is designed to be turnable and a button pushable, which is perceived by the user and facilitated by the physical properties of the object. Similarly, in the digital realm, technology affordances support certain tasks, such as allowing users to share content with a broader audience at a lower cost than offline. Privacy researchers have started to investigate how the affordances of digital technologies shape privacy behaviors, attitudes, and expectations [104, 105]. Affordances, such as editability and persistence of data, impact privacy practices [102, 106]. Namely, if people can share information online and have the ability later to edit or delete it, then they have the ability to manipulate disclosure on a temporal dimension. Users can share something temporarily and then revoke that access. However, if others can copy that information and save it, then there may never be a guarantee of revocability once information has been shared. All these technology affordances (e.g., editing, deletion, copying, saving) shape user's privacy practices and expectation of privacy.

Research has indeed shown that the affordances of an interface affect people's privacy behaviors. Vitak and Kim [102] revealed how the high visibility of content and its persistence on social media platforms made it much easier to locate content about an individual, prompting people to think harder about making self-disclosures online. In face-to-face conversations and other more ephemeral communication medium, people did not worry as much about information being available after the fact or to as wide of an audience. On the other hand, Trepte et al. [101] found that by introducing the affordance of *association* to social media, they could manipulate users' self-disclosures. By showing that many other similar social media users were self-disclosing, they could increase a user's self-disclosures. This leveraged the principle of association by showing that if people felt others who were similar to them were less privacy concerned, they were also less privacy concerned and more likely to disclose. Introducing features, such as those that enable people to associate

with other users, enables new affordances that can shape people's perceptions and subsequently their privacy behaviors. Next, we turn to discuss the proactive practice of Privacy by Design (PbD).

2.5.2 Privacy by Design

While much research has focused on uncovering privacy issues, there has been more effort recently to integrate privacy insights into the design of information systems from the get-go. One set of principles for integrating privacy into design was promoted by Ann Cavoukian, former privacy commissioner of Ontario, Canada. The set of principles and strategies referred to as "Privacy by Design" (PbD) aims to incorporate the value of privacy into the design of systems from beginning to end [40, 95, 107]. PbD engages perspectives from industry, academia, as well as civil society. There has been a lot of work incorporating principles of legal compliance and data protection into requirements engineering, but there is still a need for PbD to provide more concrete guidance on how to design for privacy in the actual design of systems [99]. Indeed, the Federal Trade Commission's 2012 consumer privacy report encouraged companies to utilize PbD, but there was not much guidance for how to address privacy in the design process [40]. Other attempts to incorporate privacy into the design process, such as with privacy-enhancing technologies (PETs) and privacy-preserving technologies (PPTs), have also encountered such challenges and have met with mixed success [38, 42].

The next challenge for PbD to tackle is to make privacy principles and guidelines that can be readily implemented by design practitioners. There has been a widening gap between academic work, which involves identifying theoretical privacy principles, and having a set of principles that are useful at a practical level [41]. One challenge is that privacy design is relevant at all levels of product development, not just at the user-visible interface. The data representation and the protocols used to communicate between different aspects of the system can all have privacy implications. Furthermore, the fast-paced change characteristic of today's technologies makes it difficult to track implications to privacy. The movement toward algorithmic transparency could be a move in the right direction, enabling outsiders to access the way information is processed and how decisions are made. This could be a promising direction to help people understand how the data is being collected, processed, and used.

Designing for privacy is a difficult challenge, but users are demanding more contextual understanding and nuance and the ability to keep certain aspects of their lives separate rather than the trend toward online social contexts all colliding [85, 108]. People are losing trust toward systems which reach beyond the data and responsibilities that are appropriate for their social context, and collecting unnecessary data or encroaching on other life domains [109]. However, in designing to regain user trust in systems, it is important to do so ethically and to make sure the system is supporting appropriate privacy practices that are in the interest of the user.

Masking potentially privacy-invasive data flows just to avoid user alarm would not be in line with the principles of PbD.

In summary, modern privacy perspectives have shifted and matured over time from viewing privacy as a transactional process of information disclosure, to making privacy interpersonal, to viewing privacy as a socially constructed phenomenon that we continually strive to embed in the design of the technologies we use daily. In the next section, we show how this progression has become more human-centered over time and is, what we believe, the future of modern privacy.

2.6 The Future of Modern Privacy: Individual Differences and User-Centered Privacy

Section Highlights

- **Individual** differences play a key role in users' privacy preferences, goals, and outcomes.
- However**,** individual **differences are rarely accounted for** in the design of systems.
- As modern privacy research advances, **it will be critical to develop solutions that take individual differences into consideration**, so that those who are the most vulnerable to privacy violations are protected.

Modern privacy research is increasingly focusing on applying user-centered principles to privacy research and design, such as helping users achieve a level of privacy relative to their own desires [110, 111]. Because privacy is a complex and highly normative construct [112], individual differences have been shown to play a key role in shaping attitudes related to various privacy concerns (e.g., interactional preferences on social media [113]) and influence subsequent on- or offline behaviors [114]. As such, we discuss why individual differences are important to consider when thinking about privacy and how we might design for them.

Research suggests that privacy preferences vary drastically from individual to individual, can change over time, and are based on context [83]. Individuals also have different privacy preferences that are influenced by contextual factors (e.g., [41, 84, 115]) that significantly affect their privacy decisions and their interaction with others online [41, 107, 116]. An individual's digital privacy behavior and preferences are influenced by personal factors, such as time available [41, 107], recipient [85], age [62, 63], gender [61, 117, 118], personality [119], network compositions [67, 102], social norms [84], culture [115], and previous experiences [108, 120]. Several chapters in this book unpack salient individual differences, including privacy with respect to cross-cultural contexts (Chap. 12), adolescents (Chap. 14), the elderly (Chap. 13), and other vulnerable populations (Chap. 15).

Despite recent research on the importance of individual differences in privacy, this scholarship has yet to make a major impact on product design and software development [121]. The disconnect between academic research and the work of

practitioners suggests a need for collaborative conversations to help ensure that research on individual privacy differences is taken into consideration in the design of networked platforms. For example, communication style, which has been a strong predictor of behavior in the offline world, also influences online privacy behaviors. Recent research shows how an "FYI communication style" trait strongly predicts privacy attitudes and resulting behaviors in social media [32]. Generally, privacy behaviors and levels of privacy feature awareness vary among end users along informational boundaries (e.g., what I share), interactional boundaries (e.g., blocking other users or hiding one's online status to avoid unwanted chats on social networks), and territorial boundaries (e.g., untagging posts or photos or deleting unwanted content posted by others on social networks) [69, 73]. Users can therefore be categorized by their disclosure styles, management strategies, and proficiency. However, there is a need to further unpack the most important contributing factors that lead to individual privacy differences, thereby allowing us to better design for them and offer more personalized user privacy support.

While recent privacy research has shown that accounting for individual differences in privacy preferences and behaviors can have a positive impact [122], there is still little work done on designing systems that support these individual differences. Part of the issue is that there is little consensus on which of the individual differences are the ones most influential when it comes to privacy concerns and behaviors [123]. Furthermore, it may not be practical to expect users to fully understand the privacy implications of every action on every technology, given the complexities and many differences between the various systems they use. One promising avenue could be to extend privacy nudging solutions, which prompt users toward more privacy-sensitive behaviors and currently do not yet account for individual differences [124, 125].

Along these lines, a more recent paradigm is that of "user-tailored privacy" [110, 111, 126] (see Chap. 16), which provides nudges (e.g., automatic initial default settings) that are tailored to users' individual differences. In this approach, the user is no longer solely responsible for their own privacy management; instead, an algorithm will support this practice, taking individual differences (e.g., the context, the user's known characteristics, their decision history, and the decision history of like-minded other users) into account. Several researchers have developed "intelligent" privacy designs to meet users' privacy needs in light of their individual differences, but they are yet to be fully utilized in the information systems we use in our daily lives. In the subsequent chapters of this book, we will further unpack modern privacy research that will help future researchers and practitioners achieve these goals.

Next, we will provide actionable guidelines for how existing privacy theories, frameworks, and paradigms can be immediately applied in practice.

2.7 Guidelines for Applying Privacy Frameworks in Practice

Section Highlights

- Identify **framework(s) relevant to the context** of your product.
- **Use the framework to uncover privacy norms and privacy threats**. Take special note of **individual differences** that are relevant to privacy expectations and preferences for your target market.
- **Design affordances into the technology that will support privacy.** Convey those affordances to the user.

Privacy frameworks can help you understand existing and potential networked privacy concerns and violations. But how do you use them? Here is a practical guideline for selecting and applying different frameworks:

Choose a privacy framework that is relevant to your design space. This chapter presented several frameworks describing the concept of privacy. Analyzing your users and their context using a framework can help you uncover potential issues. Or if you start with complaints from users, you could use a framework to reverse-engineer why they might be upset. For example, if your product supports interpersonal communication and interaction between small groups of individuals, it may make sense to draw on communication privacy management theory. The framework could guide you to ask a user (or look for evidence of) the set of people that they feel should be co-owners of their private information. It can also sensitize you to probe on the rules around when it is appropriate for co-owners to share that information. If there is not a clear theory that maps to your design space, a more general framework, such as contextual integrity, can be applied. Analyze user behaviors to understand what people feel comfortable sharing and to whom. This can help you understand the norms of privacy behaviors in your user base. Break your data down by contextual integrity factors, such as data subject and data type. Also take product maturity into consideration. If you are designing something from scratch, privacy by design would be a useful approach. If you are evaluating an existing product, you may want to consider the privacy paradox and not only ask users about their concerns but measure their behaviors to see if those concerns map to behaviors.

Apply the framework in a way that is relevant to the maturity of your product/problem space. If you are exploring a new market or problem space, you may use a framework to guide your research questions at a high level (e.g., what are people's expectations of privacy in this social context). The questions you ask people and the phenomenon you take note of during observations or analysis of materials (e.g., written and digital artifacts) should also be informed by the privacy framework. For example, drawing on privacy calculus would guide you toward probing on both benefits and drawbacks that may be playing into user's decisions. In identifying the pros and cons, you may have a better understanding of the tradeoffs people are making and the relative importance of focusing on one problem over another. If the exploratory research has already been conducted, you can still use the framework to guide your analysis of the situation. It can uncover patterns in

situations that are considered privacy violations. If you are designing a solution, you can use the framework to guide your design principles. For instance, focusing on affordances and making sure that your user interface communicates the privacy abilities that you want to communicate to the user is key. It is often important to make sure that the user understands *who* can see *what* and *when* (and even communicating *why* can help users internalize the privacy rules of your product). After you've deployed a product, you can still leverage a framework to evaluate whether user privacy needs are being met or to identify the cause of issues that arise.

Operationalizing the framework. Once you have decided on the framework and how to apply it, you will need to get down to low-level details such as what survey instruments to use to measure the privacy concepts embedded in these frameworks. Research in this area is ongoing, and new instruments, methods, and processes are constantly being developed.

2.8 Chapter Summary

We have given an overview of various conceptualizations of privacy which has guided privacy research. Some frameworks have been heavily utilized in the research community while others have yet to be widely applied but could potentially uncover new insights into how privacy is perceived and enacted. It is important that those researching networked privacy take time to consider how systems, norms, and behaviors may evolve in the future. However, platforms are constantly emerging, restructuring, and disappearing. Users flock from one site to the next, interact across platforms, and may develop distinct or overlapping networks and identities based on their primary goals. The increasingly blurry distinction between public and private spheres further complicates privacy management, with platforms only now beginning to consider solutions to make privacy and disclosure easier to manage. It will only become more important to understand users' mental models of privacy, which shape individual and group behavior around privacy in unexpected and often underappreciated ways. User mental models that understand privacy as control [27], privacy as contextual integrity [21], privacy as an emotional variable [34, 49, 70], privacy as a commodity [15], or privacy as a universal right [68] are just a few possible ways of evaluating privacy needs and explaining concerns and behaviors. Drawing on these privacy conceptualizations can guide researchers, designers, and policymakers even as technologies continually change and social norms evolve.

References

1. Ellison, N.B., J. Vitak, C. Steinfield, R. Gray, and C. Lampe. 2011. Negotiating privacy concerns and social capital needs in a social media environments. In *Privacy Online*, ed. S. Trepte and L. Reinecke, 19–32. Berlin: Springer.

2. Lampinen, Airi, Vilma Lehtinen, Asko Lehmuskallio, and Sakari Tamminen. 2011. We're in it together: Interpersonal management of disclosure in social network services. In *SIGCHI Conference on Human Factors in Computing Systems*: 3217–3226.
3. Xu, Heng, Tamara Dinev, H. Jeff Smith, and Paul Hart. 2008. *Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View.*
4. Smith, H.J., J.S. Milberg, and J.S. Burke. 1996. Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly* 20 (2): 167–196.
5. Malhotra, Naresh K., Sung S. Kim, and James Agarwal. 2004. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research* 15 (4): 336–355.
6. Anton, Annie I., Julia B. Earp, and Jessica D. Young. 2010. How Internet users' privacy concerns have evolved since 2002. *IEEE Security and Privacy* 8 (1): 21–27.
7. Smith, H. Jeff, Tamara Dinev, and Xu. Heng. 2011. Information privacy research: An interdisciplinary review. *MIS Quarterly* 35 (4): 989–1016.
8. Krasnova, Hanna, Natasha F. Veltri, and Oliver Günther. 2012. Self-disclosure and privacy calculus on social networking sites: The role of culture. *Business & Information Systems Engineering* 4 (3): 127–135.
9. Xu, Heng, Hock-Hai Teo, Bernard C.Y. Tan, and Ritu Agarwal. 2012. Research Note—Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: A study of location-based services. *Information Systems Research* 23 (4): 1342–1363.
10. Vitak, Jessica. 2012. The impact of context collapse and privacy on social network site disclosures. *Journal of Broadcasting & Electronic Media* 56 (4): 451–470.
11. Laufer, Robert S., and Maxine Wolfe. 2010. Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues* 33 (3): 22–42.
12. Acquisti, A., and J. Grossklags. 2008. What can behavioral economics teach us about privacy? *Digital Privacy: Theory, Technologies, and Practices*: 363–377.
13. Acquisti, Alessandro, and Ralph Gross. 2006. Imagined communities: Awareness, information sharing, and privacy on the Facebook. In *Privacy enhancing technologies*. 36–58.
14. Burke, Moira, and Mike Develin. 2016. Once more with feeling: Supportive responses to social sharing on Facebook. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*, Association for Computing Machinery, 1462–1474.
15. Burke, Moira, Robert Kraut, and Cameron Marlow. 2011. Social capital on Facebook: Differentiating uses and users. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, 571–580.
16. Ellison, Nicole B., Jessica Vitak, Rebecca Gray, and Cliff Lampe. 2014. Cultivating social resources on social network sites: Facebook relationship maintenance behaviors and their role in social capital processes. *Journal of Computer-Mediated Communication* 19 (4): 855–870.
17. Page, Xinru, Bart P. Knijnenburg, Pamela Wisniewski, and Moses Namara. 2018. Avoiding online harassment: The socially disenfranchised. In *Online Harassment*, ed. J. Golbeck, 243–268. Cham: Springer International Publishing.
18. Page, Xinru, Pamela Wisniewski, Bart P. Knijnenburg, and Moses Namara. 2018. Social media's have-nots: An era of social disenfranchisement. *Internet Research*: 00.
19. Sengupta, Anirban, and Anoshua Chaudhuri. 2014. Simply having a social media profile does not make teens more likely to be bullied online. Demographics and online behavior play a larger role. In *LSE American Politics and Policy*. Retrieved Sept 16, 2016 from http://blogs.lse.ac.uk/usappblog/.
20. Ellison, N.B., C. Steinfield, and C. Lampe. 2007. The benefits of Facebook "Friends:" Social capital and college students' use of online social network sites. *Journal of Computer-Mediated Communication* 12 (4): 1143–1168.
21. Burke, Moira, and Robert E. Kraut. 2016. The relationship between Facebook use and well-being depends on communication type and tie strength. *Journal of Computer-Mediated Communication* 21 (4): 265–281.

22. Kuegler, Maurice, Stefan Smolnik, and Gerald Kane. 2015. What's in IT for employees? Understanding the relationship between use and performance in enterprise social software. *The Journal of Strategic Information Systems* 24 (2): 90–112.
23. Newell, Sue. 2015. Managing knowledge and managing knowledge work: What we know and what the future holds. *Journal of Information Technology*.
24. Wang, Yang, Pedro Giovanni Leon, Xiaoxuan Chen, et al. 2013. From Facebook regrets to Facebook privacy nudges.
25. Wisniewski, Pamela, Heather Lipford, and David Wilson. 2012. Fighting for my space: Coping mechanisms for Sns boundary regulation. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, 609–618.
26. Solove, Daniel J. 2006. A taxonomy of privacy. *University of Pennsylvania Law Review* 154 (3): 477–560.
27. Coursaris, Constantinos, Wietske Van Osch, Jieun Sung, and Younghwa Yun. 2013. Disentangling Twitter's adoption and use (dis)continuance: A theoretical and empirical amalgamation of uses and gratifications and diffusion of innovations. *AIS Transactions on Human-Computer Interaction* 5 (1): 57–83.
28. Park, Namsu, Kerk F. Kee, and Sebastián Valenzuela. 2009. Being immersed in social networking environment: Facebook groups, uses and gratifications, and social outcomes. *CyberPsychology & Behavior* 12 (6): 729–733.
29. Sutanto, Juliana, Elia Palme, Chuan-Hoo Tan, and Chee Wei Phang. 2013. Addressing the personalization–privacy paradox: An empirical assessment from a field experiment on smartphone users. *Management Information Systems Quarterly* 37 (4): 1141–1164.
30. Smock, Andrew D., Nicole B. Ellison, Cliff Lampe, and Donghee Yvette Wohn. 2011. Facebook as a toolkit: A uses and gratification approach to unbundling feature use. *Computers in Human Behavior* 27 (6): 2322–2329.
31. Page, Xinru, Alfred Kobsa, and Bart P. Knijnenburg. 2012. Don't disturb my circles! Boundary preservation is at the center of location-sharing concerns. In *Sixth International AAAI Conference on Weblogs and Social Media*.
32. Page, Xinru, Reza Ghaiumy Anaraky, and Bart P. Knijnenburg. 2019. How communication style shapes relationship boundary regulation and social media adoption. In *Proceedings of the 10th International Conference on Social Media and Society*, Association for Computing Machinery, 126–135.
33. Spiekermann, Sarah, Jens Grossklags, and Bettina Berendt. 2001. E-privacy in 2nd generation e-commerce: Privacy preferences versus actual behavior. In *Proceedings of the 3rd ACM conference on Electronic Commerce*, Association for Computing Machinery, 38–47.
34. Barnes, Susan B. 2006. A privacy paradox: Social networking in the United States. *First Monday* 11: 9.
35. Tufekci, Zeynep. 2008. Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society* 28 (1): 20–36.
36. Norberg, Patricia A., Daniel R. Horne, and David A. Horne. 2007. The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs* 41 (1): 100–126.
37. Simon, Herbert A. 1990. Bounded rationality. In *Utility and Probability*, ed. J. Eatwell, M. Milgate, and P. Newman, 15–18. London: Palgrave Macmillan UK.
38. Acquisti, Alessandro, and Jens Grossklags. 2006. Privacy and rationality. In K.J. Strandburg and D.S. Raicu, eds., *Privacy and Technologies of Identity: A Cross-Disciplinary Conversation*. Springer US, 15–29.
39. Ghaiumy, Reza, Kaileigh A. Byrne, Pamela Wisniewski, Xinru Page, and Bart P. Knijnenburg. 2021. To disclose or not to disclose: Examining the privacy decision-making processes of older vs. younger adults. In *Proceedings of the 2021 ACM conference on Human Factors in Computing Systems*.
40. Acquisti, Alessandro, and Ralph Gross. 2006. *Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook*. Berlin: Springer.

41. Benisch, Michael, Patrick Gage Kelley, Norman Sadeh, and Lorrie Faith Cranor. 2011. Capturing location-privacy preferences: Quantifying accuracy and user-burden tradeoffs. *Personal Ubiquitous Computing* 15: 679–694.
42. Brodie, C., C. M. Karat, and J. Karat. 2004. Creating an E-commerce environment where consumers are willing to share personal information. *Designing Personalized User Experiences in eCommerce*: 185–206.
43. Kolter, Jan and Günther Pernul. 2009. *Generating User-Understandable Privacy Preferences*. 299–306.
44. Pavlou, Paul A., Huigang Liang, and Yajiong Xue. 2007. Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS Quartely* 31 (1): 105–136.
45. Tang, Karen, Jialiu Lin, Jason Hong, Daniel Siewiorek, and Norman Sadeh. 2010. Rethinking Location Sharing: Exploring the Implications of Social-Driven vs. Purpose-Driven Location Sharing. ACM Press, 85–94.
46. Toch, Eran, Justin Cranshaw, Paul Hankes Drielsma, et al. 2010. Empirical Models of Privacy in Location Sharing. ACM Press, 129–138.
47. Wenning, Rigo, and Matthias Schunter. 2006. *The Platform for Privacy Preferences 1.1 (P3P1.1) Specification*. W3C Working Group Note.
48. Xu, H. 2007. *The Effects of Self-Construal and Perceived Control on Privacy Concerns*. Paper 125.
49. Compañó, Ramón, and Wainer Lusoli. 2010. The policy maker's anguish: Regulating personal data behavior between paradoxes and dilemmas. In *Economics of Information Security and Privacy*, ed. T. Moore, D. Pym, and C. Ioannidis, 169–185. New York, NY: Springer US.
50. Smith, Aaron, and Monica Anderson. 2018. Social media use in 2018. *Pew Research Center: Internet, Science & Tech*. Retrieved Sept 16, 2018 from http://www.pewinternet.org/2018/03/01/social-media-use-in-2018/.
51. Marwick, A.E., and D. Boyd. 2014. Networked privacy: How teenagers negotiate context in social media. *New Media & Society* 16 (7): 1051–1067.
52. Wisniewski, Pamela. 2012. *Understanding and Designing for Interactional Privacy Needs Within Social Networking Sites*.
53. Lipford, H. R., A. Besmer, and J. Watson. 2008. *Understanding Privacy Settings in Facebook with an Audience View*.
54. Harris, Louis, Associates, and Alan F Westin. 1997. *Commerce, Communications, and Privacy Online: A National Survey of Computer Users.*
55. Harris, Louis, Alan F Westin, and Associates. 2003. *Consumer Privacy Attitudes: A Major Shift Since 2000 and Why*. Harris Interactive, Inc.
56. Westin, Alan F., Louis Harris, and Associates. 1981. *The Dimensions of Privacy: A National Opinion Research Survey of Attitudes Toward Privacy*. New York: Garland Publishing.
57. Woodruff, Allison, Vasyl Pihur, Sunny Consolvo, Lauren Schmidt, Laura Brandimarte, and Alessandro Acquisti. 2014. Would a privacy fundamentalist sell their DNA for $1000... if nothing bad happened as a result? The Westin categories, behavioral intentions, and consequences.
58. Knijnenburg, Bart P., Alfred Kobsa, and Hongxia Jin. 2013. Dimensionality of information disclosure behavior. *International Journal of Human-Computer Studies* 71: 1144–1162.
59. Joinson, Adam N., Carina Paine, Tom Buchanan, and Ulf-Dietrich Reips. 2008. Measuring self-disclosure online: Blurring and non-response to sensitive items in web-based surveys. *Computers in Human Behavior* 24 (5): 2158–2171.
60. Page, Xinru, Reza Ghaiumy Anaraky, Bart P. Knijnenburg, and Pamela J. Wisniewski. 2019. Pragmatic tool vs. relational hindrance: Exploring why some social media users avoid privacy features. In *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW: 110:1–110:23.
61. Hoy, Mariea Grubbs, and George Milne. 2010. Gender differences in privacy-related measures for young adult Facebook users. *Journal of Interactive Advertising* 10 (2): 28–45.

62. Litt, Eden. 2012. Knock, knock. who's there? The imagined audience. *Journal of Broadcasting & Electronic Media* 56 (3): 330–345.
63. Madden, Mary. 2012. *Privacy Management on Social Media Sites*. Pew Internet & American Life Project, Pew Research Center, Washington, DC.
64. Wang, Yang, Gregory Norcie, Saranga Komanduri, Alessandro Acquisti, Pedro Giovanni Leon, and Lorrie Faith Cranor. 2011. *"I regretted the minute I pressed share": A Qualitative Study of Regrets on Facebook*. ACM, 10:1–10:16.
65. Abaquita, Denielle, Paritosh Bahirat, Karla A. Badillo-Urquiola, and Pamela Wisniewski. 2020. Privacy norms within the internet of things using contextual integrity. In *Companion of the 2020 ACM International Conference on Supporting Group Work*, Association for Computing Machinery, 131–134.
66. Fono, David, and Kate Raynes-Goldie. 2006. Hyperfriendship and beyond: Friends and social norms on LiveJournal. *Internet Research Annual* 4.
67. Vitak, Jessica, and Nicole B. Ellison. 2013. 'There's a network out there you might as well tap': Exploring the benefits of and barriers to exchanging informational and support-based resources on Facebook. *New Media & Society* 15 (2): 243–259.
68. Davis, Katie, David P. Randall, Anthony Ambrose, and Mania Orand. 2015. 'I was bullied too': Stories of bullying and coping in an online community. *Information, Communication & Society* 18 (4): 357–375.
69. Wisniewski, Pamela, A.K.M. Islam, Heather Richter Lipford, and David Wilson. 2016. Framing and measuring multi-dimensional interpersonal privacy preferences of social networking site users. *Communications of the Association for Information Systems* 38: 1.
70. Barkhuus, Louise. 2012. The mismeasurement of privacy: using contextual integrity to reconsider privacy in HCI. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM 367–376.
71. Hargittai, Eszter, and Alice Marwick. 2016. "What Can I Really Do?" Explaining the privacy paradox with online apathy. *International Journal of Communication* 10: 21.
72. Page, Xinru, and Marco Marabelli. 2017. Changes in social media behavior during life periods of uncertainty. In *Eleventh International AAAI Conference on Web and Social Media.*
73. Karr-Wisniewski, Pamela, David C. Wilson, and Heather Richter-Lipford. 2011. A new social order: Mechanisms for social network site boundary regulation. In *AMCIS 2011 Proceedings*, Paper 101.
74. Altman, I. 1975. *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*. Monterey, CA: Brooks/Cole Publishing.
75. Stutzman, Fred, and W Hartzog. 2009. *Boundary Regulation in Social Media.*
76. Tufekci, Zeynep. 2008. Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society* 28 (1): 20–36.
77. Wisniewski, Pamela J., Bart P. Knijnenburg, and Heather Richter Lipford. 2017. Making privacy personal. *International Journal of Human-Computer Studies* 98 (C): 95–108.
78. Palen, Leysia, and Paul Dourish. 2003. *Unpacking "Privacy" for a Networked World*. ACM, 129–136.
79. Petronio, Sandra Sporbert. 2002. *Boundaries of Privacy: Dialects of Disclosure*. SUNY Press.
80. Child, Jeffrey T., and Esther A. Agyeman-Budu. 2010. Blogging privacy management rule development: The impact of self-monitoring skills, concern for appropriateness, and blogging frequency. *Computers in Human Behavior* 26 (5): 957–963.
81. Dourish, Paul, and Ken Anderson. 2006. Collective Information practice: Exploring privacy and security as social and cultural phenomena. *Human–Computer Interaction* 21 (3): 319–342.
82. Jia, Haiyan, and Xu. Heng. 2016. Measuring individuals' concerns over collective privacy on social networking sites. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 10: 1.
83. Nissenbaum, Helen. 2004. Privacy as contextual integrity. *Washington Law Review* 79: 119.

84. ———. 2009. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press.
85. Consolvo, Sunny, Ian E. Smith, Tara Matthews, Anthony LaMarca, Jason Tabert, and Pauline Powledge. 2005. Location disclosure to social relations: Why, when, & what people want to share. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Association for Computing Machinery, 81–90.
86. Page, Xinru Woo. 2014. *Factors that Influence Adoption and Use of Location-Sharing Social Media*. Retrieved Jan 21, 2021 from http://search.proquest.com/docview/1493902213/abstract/DA0CC637A21947B3PQ/1.
87. Friedman, Batya, Peter H. Kahn, and Alan Borning. 2006. Value sensitive design and information systems. In *Human-Computer Interaction and Management Information Systems: Foundations.* M.E. Sharpe, 348–372.
88. Lerato, Masupha, Omobayo A. Esan, Ashley-Dejo Ebunoluwa, S. M. Ngwira, and Tranos Zuva. 2015. A survey of recommender system feedback techniques, comparison and evaluation metrics. In *2015 International Conference on Computing, Communication and Security (ICCCS)*, IEEE, 1–4.
89. Knijnenburg, Bart P., Martijn C. Willemsen, and Stefan Hirtbach. 2010. Receiving recommendations and providing feedback: The user-experience of a recommender system. In *E-Commerce and Web Technologies*, ed. F. Buccafurri and G. Semeraro, 207–216. Berlin: Springer.
90. Knijnenburg, Bart P., Niels J.M. Reijmer, and Martijn C. Willemsen. 2011. Each to his own: How different users call for different interaction methods in recommender systems. In *Proceedings of the fifth ACM conference on Recommender systems*, ACM Press, 141–148.
91. Gardner, Damian, and John Marzillier. 1996. Day to day maintenance of confidentiality: Practices and beliefs of trainee and qualified clinical psychologists in the UK. *Clinical Psychology & Psychotherapy* 3 (1): 35–45.
92. Tyson, Peter. 2001. *The Hippocratic Oath Today — NOVA | PBS*. Retrieved Apr 3, 2018 from http://www.pbs.org/wgbh/nova/body/hippocratic-oath-today.html.
93. Wang, Yang, Huichuan Xia, Yaxing Yao, and Yun Huang. 2016. Flying eyes and hidden controllers: A qualitative study of people's privacy perceptions of civilian drones in the US. *Proceedings on Privacy Enhancing Technologies* 2016 (3): 172–190.
94. Ayalon, Oshrat, and Eran Toch. 2017. Not even past: Information aging and temporal privacy in online social networks. *Human-Computer Interaction* 32 (2): 73–102.
95. Badillo-Urquiola, Karla, Yaxing Yao, Oshrat Ayalon, et al. 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*, ACM, 425–431.
96. Dakin Andone CNN. Uber and Lyft drop driver for livestreaming passengers on Twitch. *CNN*. Retrieved Feb 20, 2020 from https://www.cnn.com/2018/07/22/us/uber-lyft-driver-recording-passengers/index.html.
97. Narayanan, Arvind, and Edward W. Felten. 2014. *No Silver Bullet: De-identification Still Doesn't Work*.
98. Zheleva, Elena, and Lise Getoor. 2009. To join or not to join: The illusion of privacy in social networks with mixed public and private user profiles. In *Proceedings of the 18th International Conference on World Wide Web*, Association for Computing Machinery, 531–540.
99. Boyd, Danah. 2010. *Social Network Sites as Networked Publics: Affordances, Dynamics, and Implications*. Routledge.
100. Trepte, Sabine. 2020. The social media privacy model: Privacy and communication in the light of social media affordances. *Communication Theory* qtz035.
101. Trepte, Sabine, Michael Scharkow, and Tobias Dienlin. 2020. The privacy calculus contextualized: The influence of affordances. *Computers in Human Behavior* 104.
102. Vitak, Jessica, and Jinyoung Kim. 2014. "You Can't Block People Offline": Examining how Facebook's affordances shape the disclosure process. In *Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing*, ACM, 461–474.

103. Lynne Markus, M., and Mark Silver. 2008. A foundation for the study of IT effects: A new look at DeSanctis and Poole's concepts of structural features and spirit. *Journal of the Association for Information Systems* 9 (10): 609–632.
104. Gibson, James J. 2014. *The Ecological Approach to Visual Perception: Classic Edition*. New York, London: Psychology Press.
105. Leonardi, Paul M. 2011. When flexible routines meet flexible technologies: Affordance, constraint, and the imbrication of human and material agencies. *MIS Quarterly* 35 (1): 147–167.
106. Treem, Jeffrey W., and Paul M. Leonardi. 2013. Social media use in organizations: Exploring the affordances of visibility, editability, persistence, and association. *Annals of the International Communication Association* 36 (1): 143–189.
107. Dong, Cailing, Hongxia Jin, and Bart P. Knijnenburg. 2015. Predicting privacy behavior on online social networks. In *Ninth International AAAI Conference on Web and Social Media*, AAAI Publications, 91–100.
108. Chen, Hongliang, Christopher E. Beaudoin, and Traci Hong. 2016. Protecting oneself online: The effects of negative privacy experiences on privacy protective behaviors. *Journalism & Mass Communication Quarterly* 93 (2): 409–429.
109. Badillo-Urquiola, Karla, Xinru Page, and Pamela Wisniewski. 2018. Literature Review: Examining contextual integrity within human-computer interaction.
110. Knijnenburg, B. P. 2015. *A User-Tailored Approach to Privacy Decision Support*. http://search.proquest.com/docview/1725139739/abstract.
111. Wilkinson, Daricia, Saadhika Sivakumar, David Cherry, et al. 2017. User-tailored privacy by design. In *Proceedings of the Usable Security Mini Conference*, Internet Society.
112. Turkington, Richard C., and Anita L. Allen. 2002. *Privacy Law: Cases and Materials*. West Academic Publishing.
113. Fogel, Joshua, and Elham Nehmad. 2009. Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior* 25 (1): 153–160.
114. Solove, Daniel J. 2008. *Understanding Privacy*. Rochester, NY: Social Science Research Network.
115. Li, Yao, Alfred Kobsa, Bart P. Knijnenburg, and M.H. Carolyn Nguyen. 2017. Cross-cultural privacy prediction. *Proceedings on Privacy Enhancing Technologies* 2: 93–112.
116. Xie, Jierui, Bart Piet Knijnenburg, and Hongxia Jin. 2014. Location sharing privacy preference: Analysis and personalized recommendation. In *Proceedings of the 19th International Conference on Intelligent User Interfaces*, ACM, 189–198.
117. Hargittai, Eszter. 2010. Facebook privacy settings: Who cares? *First Monday*.
118. Sheehan, Kim Bartel. 1999. An investigation of gender differences in on-line privacy concerns and resultant behaviors. *Journal of Interactive Marketing* 13 (4): 24–38.
119. Weiser, Eric B. 2015. # Me: Narcissism and its facets as predictors of selfie-posting frequency. *Personality and Individual Differences* 86: 477–481.
120. Ramokapane, Kopo M., Gaurav Misra, Jose M. Such, and Sören Preibusch. 2021. *Truth or Dare: Understanding and Predicting How Users Lie and Provide Untruthful Data Online.*
121. Rubinstein, Ira S., and Nathaniel Good. 2013. Privacy by design: A counterfactual analysis of google and facebook privacy incidents. *Berkeley Technology Law Journal* 28: 1333–1414.
122. Wilkinson, Daricia, Moses Namara, Karla Badillo-Urquiola, et al. 2018. Moving beyond a "One-size Fits All": Exploring individual differences in privacy. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*, ACM, W16:1–W16:8.
123. Yao, Mike Z., Ronald E. Rice, and Kier Wallis. 2007. Predicting user concerns about online privacy. *Journal of the Association for Information Science and Technology* 58 (5): 710–722.
124. Wang, Yang, Pedro Giovanni Leon, Kevin Scott, Xiaoxuan Chen, Alessandro Acquisti, and Lorrie Faith Cranor. 2013. Privacy nudges for social media: An exploratory Facebook study. In *Second International Workshop on Privacy and Security in Online Social Media*, 763–770.

125. Wisniewski, Pamela J., Bart P. Knijnenburg, and Heather Richter Lipford. 2017. Making privacy personal: Profiling social network users to inform privacy education and nudging. *International Journal of Human-Computer Studies* 98: 95–108.
126. Knijnenburg, B.P. 2017. Privacy? I Can't Even! Making a case for user-tailored privacy. *IEEE Security Privacy* 15 (4): 62–67.