Chapter 4
Privacy and Behavioral Economics

Alessandro Acquisti, Laura Brandimarte, and George Loewenstein

Abstract There are diverse streams of empirical research attempting to study complex privacy behaviors in different scenarios. In this chapter, we connect those streams and present them under three themes: (1) individuals' uncertainty about their own preferences as well as their uncertainty about the consequences of information disclosure; (2) the context-dependence of individuals' concern, or lack thereof, about privacy; (3) the degree to which privacy concerns are malleable and prone to manipulations by commercial and government entities. Building on these themes, we discuss the role of public policy in the protection of privacy in the information age.

4.1 Introduction

If this is the age of information, then privacy is the issue of our times. Activities that were once private or shared with the few now leave trails of data that expose our interests, traits, beliefs, and intentions. We communicate using e-mails, texts, and social media; find partners on dating sites; learn via online courses; seek responses to mundane and sensitive questions using search engines; read news and books in the cloud; navigate streets with geotracking systems; and celebrate our newborns, and mourn our dead, on social media profiles. Through these and other activities, we reveal information—both knowingly and unwittingly—to one another, to commercial entities, and to our governments. The monitoring of personal

A. Acquisti (✉)
H. John Heinz III College, Carnegie Mellon University, Pittsburgh, PA, USA
e-mail: acquisti@andrew.cmu.edu

L. Brandimarte
Eller College of Management, University of Arizona, Tucson, AZ, USA
e-mail: lbrandimarte@arizona.edu

G. Loewenstein
Dietrich College, Social and Decision Sciences, Carnegie Mellon University, Pittsburgh, PA, USA
e-mail: gl20@andrew.cmu.edu

B. P. Knijnenburg et al. (eds.), *Modern Socio-Technical Perspectives on Privacy*,
https://doi.org/10.1007/978-3-030-82786-1_4

information is ubiquitous; its storage is so durable as to render one's past undeletable [1], a modern digital skeleton in the closet. Accompanying the acceleration in data collection are steady advancements in the ability to aggregate, analyze, and draw sensitive inferences from individuals' data [2].

Both firms and individuals can benefit from the sharing of once hidden data and from the application of increasingly sophisticated analytics to larger and more interconnected databases [3]. So too can society as a whole; for instance, when electronic medical records are combined to observe novel drug interactions [4]. On the other hand, analytics of this data can pose risks to individuals; not many years ago, it was possible to predict one's social security number using their location and date of birth [5]. Such risks are not limited to individuals; the potential for personal data to be abused for economic and social discrimination, hidden influence and manipulation, coercion, or censorship is alarming. The erosion of privacy can threaten our autonomy, not merely as consumers but as citizens [6]. Sharing more personal data does not necessarily always translate into more progress, efficiency, or equality [7].

Because of the seismic nature of these developments, there has been considerable debate about individuals' ability to navigate a rapidly evolving privacy landscape, and about what, if anything, should be done about privacy at a policy level. Some trust people's ability to make self-interested decisions about information disclosing and withholding. Those holding this view tend to see regulatory protection of privacy as interfering with the fundamentally benign trajectory of information technologies and the benefits such technologies may unlock [8]. Others are concerned about the ability of individuals to manage privacy amid increasingly complex trade-offs. Traditional tools for privacy decision-making such as choice and consent, according to this perspective, no longer provide adequate protection [9]. Instead of individual responsibility, regulatory intervention may be needed to balance the interests of the subjects of data against the power of commercial entities and governments holding that data.

Are individuals up to the challenge of navigating privacy in the information age? To address this question, we review diverse streams of empirical privacy research from the social and behavioral sciences. We highlight factors that influence decisions to protect or surrender privacy and how, in turn, privacy protections or violations affect people's behavior. Information technologies have progressively become part of every aspect of our personal and professional lives. Thus, the problem of control over personal data has become inextricably linked to problems of personal choice, autonomy, and socioeconomic power. Accordingly, this chapter focuses on the concept of, and literature around, informational privacy (i.e., privacy of personal data) but also touches on other conceptions of privacy, such as anonymity or seclusion. Such notions all ultimately relate to the permeable yet pivotal boundaries between public and private [10].

We use three themes to organize and draw connections between streams of privacy research that, in many cases, have unfolded independently.

- **Uncertainty**: The first theme is people's uncertainty about the nature of privacy trade-offs, and their own preferences over them.
- **Context-dependence**: The second theme is the powerful context-dependence aspect of privacy preferences; the same person can in some situations be oblivious to, but in other situations be acutely concerned about, issues of privacy.
- **Malleability and influence**: The third theme is the malleability of privacy preferences, by which we mean that privacy preferences are subject to influence by those possessing greater insight into their determinants. Although most individuals are probably unaware of the diverse influences on their concern about privacy, entities whose interests depend on information revelation by others are not. The manipulation of subtle factors that activate or suppress privacy concern can be seen in myriad realms such as the choice of sharing defaults on social networks, or the provision of greater control on social media which creates an illusion of safety and encourages greater sharing.

Uncertainty, context-dependence, and malleability are closely connected. Context dependence is amplified by uncertainty. Because people are often "at sea" when it comes to the consequences of, and their feelings about, privacy, they cast around for cues to guide their behavior. Privacy preferences and behaviors are, in turn, malleable and subject to influence in large part because they are context-dependent and because those with an interest in information divulgence are able to manipulate context to their advantage.

4.2 Uncertainty

Individuals manage the boundaries between their private and public spheres in numerous ways: via separateness (separation from others), reserve (creating barriers against unwanted intrusion), or anonymity [11], by protecting personal information, but also through deception and dissimulation [12]. People establish such boundaries for many reasons, including the need for intimacy and psychological respite and the desire for protection from social influence and control [13]. Sometimes, these motivations are so visceral and primal that privacy-seeking behavior emerges swiftly and naturally. This is often the case when physical privacy is intruded such as when a stranger encroaches in one's personal space [14–16] or demonstratively eavesdrops on a conversation. However, at other times (often including when informational privacy is at stake), people experience considerable uncertainty about whether, and to what degree, they should be concerned about privacy.

A first and most obvious source of privacy uncertainty arises from incomplete and asymmetric information. Advancements in information technology have made the collection and usage of personal data often invisible. As a result, individuals rarely have clear knowledge of what information other people, firms, and governments have about them or how that information is used and with what consequences. To the extent that people lack such information, or are aware of their ignorance, they are likely to be uncertain about how much information to share.

Two factors exacerbate the difficulty of ascertaining the potential consequences of privacy behavior:

1. **It is hard to think about privacy.** Whereas some privacy harms are tangible, such as the financial costs associated with identity theft, many others, such as having strangers become aware of one's life history, are intangible.
2. **Privacy is rarely an unalloyed good.** It typically involves trade-offs [17]. For example, ensuring the privacy of a consumer's purchases may protect them from price discrimination but also deny the potential benefits of targeted advertisements.

Elements that mitigate one or both of these exacerbating factors, by either increasing the tangibility of privacy harms or making trade-offs explicit and simple to understand, will generally affect privacy-related decisions. This is illustrated by one laboratory experiment in which participants were asked to use a specially designed search engine to find online merchants and purchase from them, with their own credit cards, either a set of batteries or a sex toy [18]. When the search engine only provided links to the merchants' sites and a comparison of the products' prices from the different sellers, a majority of participants did not pay any attention to the merchants' privacy policies; they purchased from those offering the lowest price. However, when the search engine also provided participants with salient, easily accessible information about the differences in privacy protection afforded by the various merchants, a majority of participants paid a roughly 5% premium to buy products from (and share their credit card information with) more privacy-protecting merchants.

A second source of privacy uncertainty relates to preferences. Even when aware of the consequences of privacy decisions, people are still likely to be uncertain about their own privacy preferences. Research on preference uncertainty [19] shows that individuals often have little sense of how much they like goods, services, or other people. Privacy does not seem to be an exception. This can be illustrated by research in which people were asked sensitive and potentially incriminating questions either point-blank, or followed by credible assurances of confidentiality [20]. Although logically such assurances should lead to greater divulgence, they often had the opposite effect because they elevated respondents' privacy concerns, which without assurances would have remained dormant. The remarkable uncertainty of privacy preferences comes into play in efforts to measure individual and group differences in preference for privacy [21]. For example, Westin [22] famously used broad (i.e., not contextually specific) privacy questions in surveys to cluster individuals into privacy segments: privacy fundamentalists, pragmatists, and unconcerned. When asked directly, many people fall in the first segment: They profess to care a lot about privacy and express particular concern over losing control of their personal information or others gaining unauthorized access to it [23, 24]. However, doubts about the power of attitudinal scales to predict actual privacy behavior arose early in the literature [25]. This discrepancy between attitudes and behaviors has become known as the "privacy paradox."

In one early study illustrating the paradox, participants were first classified into categories of privacy concern inspired by Westin's categorization based on their responses to a survey dealing with attitudes toward sharing data [26]. Next, they were presented with products to purchase at a discount with the assistance of an anthropomorphic shopping agent. Few, regardless of the group they were categorized in, exhibited much reluctance to answering the increasingly sensitive questions the agent plied them with.

Why do people who claim to care about privacy often show little concern about it in their daily behavior? One possibility is that the paradox is illusory—that privacy attitudes, which are defined broadly, and intentions and behaviors, which are defined narrowly, should not be expected to be closely related [27, 28]. Thus, one might care deeply about privacy in general but, depending on the costs and benefits prevailing in a specific situation, seek or not seek privacy protection [29].

This explanation for the privacy paradox, however, is not entirely satisfactory for two reasons. The first is that it fails to account for situations in which attitude-behavior dichotomies arise under high correspondence between expressed concerns and behavioral actions. For example, one study compared attitudinal survey answers to actual social media behavior [30]. Even within the subset of participants who expressed the highest degree of concern over strangers being able to easily find out their sexual orientation, political views, and partners' names, 48% did in fact publicly reveal their sexual orientation online, 47% revealed their political orientation, and 21% revealed their current partner's name. The second reason is that privacy decision-making is only in part the result of a rational "calculus" of costs and benefits [17, 29]; it is also affected by misperceptions of those costs and benefits, as well as social norms, emotions, and heuristics. Any of these factors may affect behavior differently from how they affect attitudes. For instance, present-bias can cause even the privacy-conscious to engage in risky revelations of information, if the immediate gratification from disclosure trumps the delayed, and hence discounted, future consequences [31].

Preference uncertainty is evident not only in studies that compare stated attitudes with behaviors but also in those that estimate monetary valuations of privacy. "Explicit" investigations ask people to make direct trade-offs, typically between privacy of data and money. For instance, in a study conducted both in Singapore and the United States, students made a series of hypothetical choices about sharing information with websites that differed in protection of personal information and prices for accessing services [32]. Using conjoint analysis, the authors concluded that subjects valued protection against errors, improper access, and secondary use of personal information between $30.49 and $44.62. Similar to direct questions about attitudes and intentions, such explicit investigations of privacy valuation spotlight privacy as an issue that respondents should take account of and, as a result, increase the weight they place on privacy in their responses.

Implicit investigations, in contrast, infer valuations of privacy from day-to-day decisions in which privacy is only one of many considerations and is typically not highlighted. Individuals engage in privacy-related transactions all the time, even when the privacy trade-offs may be intangible or when the exchange of

personal data may not be a visible or primary component of a transaction. For instance, completing a query on a search engine is akin to selling personal data (one's preferences and contextual interests) to the engine in exchange for a service (search results). "Revealed preference" economic arguments would then conclude that because technologies for information sharing have been enormously successful, whereas technologies for information protection have not, individuals hold overall low valuations of privacy. However, that is not always the case: Although individuals at times give up personal data for small benefits or discounts, at other times they voluntarily incur substantial costs to protect their privacy. Context, as further discussed in the next section, matters.

In fact, attempts to pinpoint exact valuations that people assign to privacy may be misguided, as suggested by research calling into question the stability, and hence validity, of privacy estimates. In one field experiment inspired by the literature on endowment effects [33], shoppers at a mall were offered gift cards for participating in a nonsensitive survey. The cards could be used online or in stores, just like debit cards. Participants were either given a $10 "anonymous" gift card (transactions done with that card would not be traceable to the subject) or a $12 trackable card (transactions done with that card would be linked to the name of the subject). Initially, half of the participants were given one type of card, and half the other. Then, they were all offered the opportunity to switch. Some shoppers, for example, were given the anonymous $10 card and were asked whether they would accept $2 to "allow my name to be linked to transactions done with the card"; other subjects were asked whether they would accept a card with $2 less value to "prevent my name from being linked to transactions done with the card." Of the subjects who originally held the less valuable but anonymous card, five times as many (52.1%) chose it and kept it over the other card than did those who originally held the more valuable card (9.7%). This suggests that people value privacy more when they have it than when they do not.

The consistency of preferences for privacy is also complicated by the existence of a powerful countervailing motivation: the desire to be public, share, and disclose. Humans are social animals, and information sharing is a central feature of human connection. Social penetration theory [34] suggests that progressively increasing levels of self-disclosure are an essential feature of the natural and desirable evolution of interpersonal relationships from superficial to intimate. Such a progression is only possible when people begin social interactions with a baseline level of privacy. Paradoxically, therefore, privacy provides an essential foundation for intimate disclosure. Similar to privacy, self-disclosure confers numerous objective and subjective benefits, including psychological and physical health [35, 36]. The desire for interaction, socialization, disclosure, and recognition or fame (and, conversely, the fear of anonymous unimportance) are human motives no less fundamental than the need for privacy. The electronic media of the current age provide unprecedented opportunities for acting on them. Through social media, disclosures can build social capital, increase self-esteem [37], and fulfill ego needs [38]. In a series of functional magnetic resonance imaging experiments, self-disclosure was even found to engage neural mechanisms associated with reward; people highly value the ability to share

thoughts and feelings with others. Indeed, subjects in one of the experiments were willing to forgo money in order to disclose about themselves [39].

To summarize, there can be several reasons contributing to uncertainty in privacy decision-making. It is a good practice for system providers to acknowledge these factors and try to address them.

- **Users are rarely aware of the information that others might have about them.** Trade-offs associated with privacy decisions with intangible risks even worsen the situation. A potential remedy is to make trade-offs explicit, so that users will have less difficulty understanding them—however, that may not always be possible.
- **Users are uncertain about their privacy preferences.** Their preference can indeed be constructed at the moment. Continuing consent may be a potential solution to this problem—unfortunately, a system can ask for consent only every so often.

4.3 Context-Dependence

Much evidence suggests that privacy is a universal human need [40]. However, when people are uncertain about their preferences, they often search for cues in their environment to provide guidance. And because cues are a function of context, behavior is as well. Applied to privacy, context-dependence means that individuals can, depending on the situation, exhibit anything ranging from extreme concern to apathy about privacy. Adopting the terminology of Westin, we are all privacy pragmatists, privacy fundamentalists, or privacy unconcerned, depending on time and place [41].

The way we construe and negotiate public and private spheres is context-dependent because the boundaries between the two are murky [42]: The rules people follow for managing privacy vary by situation, are learned over time, and are based on cultural, motivational, and purely situational criteria. For instance, usually we may be more comfortable sharing secrets with friends, but at times we may reveal surprisingly personal information to a stranger on a plane [43]. The theory of contextual "integrity" posits that social expectations affect our beliefs regarding what is private and what is public and that such expectations vary with specific contexts [44]. Thus, seeking privacy in public is not a contradiction; individuals can manage privacy even while sharing information, and even on social media [45]. For instance, Fig. 4.1 shows the results of actual disclosure behavior of online social network users in a longitudinal study [46]. The results suggest that over time, many users increased the amount of personal information revealed to their friends (those connected to them on the network) while simultaneously decreasing the amounts revealed to strangers (those unconnected to them). In 2005 over 89% of profiles publicly revealed their birthday, while in 2011 just 20% of the profiles were public. Decreasing disclosures for several years, the percentage of profiles that publicly

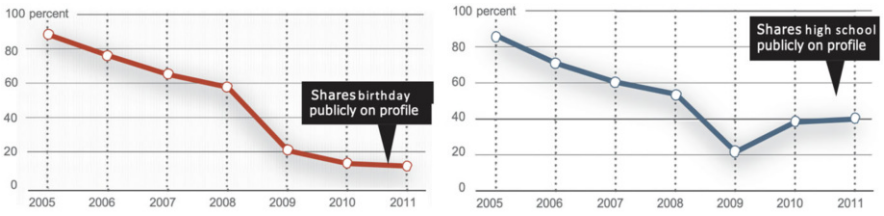

Fig. 4.1 Privacy behavior is affected both by endogenous motivations (i.e., subjective preferences: downtrend on the graphs suggests users disclose less as the time passes) and exogenous factors (i.e., changes in user interfaces: Facebook changed the default visibility settings for various fields on its profiles, including high school (bottom) but not birthday (top)) [46]

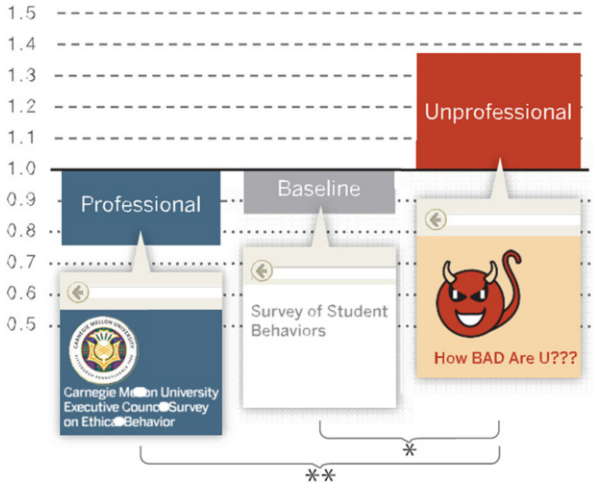

Fig. 4.2 The impact of cues on disclosure behavior. Subjects revealed more personal and even incriminating information on the website with a more casual design rather than a professionally developed website. The y axis captures the mean affirmative admission rates (AARs) normed, question by question, on the overall average AAR for the question

revealed their high school roughly doubled between 2009 and 2010 after Facebook changed the default visibility settings for various fields on its profiles, including high school (bottom), but not birthday (top).

The cues that people use to judge the importance of privacy sometimes result in sensible behavior. For instance, the presence of government regulation has been shown to reduce consumer concern and increase trust; it is a cue that people use to infer the existence of some degree of privacy protection [47]. In other situations, however, cues can be unrelated, or even negatively related, to normative bases of decision-making. For example, in one online experiment [48], individuals were more likely to reveal personal and even incriminating information on a website with an unprofessional and casual design with the banner "How Bad R U" than on a site with a formal interface even though the site with the formal interface was judged by other respondents to be much safer (Fig. 4.2). The study illustrates how cues

can influence privacy behavior in a fashion that is unrelated, or even negatively related, to normative bases of decision-making. Yet in other situations, it is the physical environment that influences privacy concern and associated behavior [49], sometimes even unconsciously. For instance, all else being equal, intimacy of self-disclosure is higher in warm, comfortable rooms, with soft lighting, than in cold rooms with bare cement and overhead fluorescent lighting [50].

Some of the cues that influence perceptions of privacy are one's culture and the behavior of other people, either through the mechanism of descriptive norms (imitation) or via reciprocity [51]. Observing other people reveal information increases the likelihood that one will reveal it oneself [52]. In one study, survey-takers were asked a series of sensitive personal questions regarding their engagement in illegal or ethically questionable behaviors. After answering each question, participants were provided with information, manipulated unbeknownst to them, about the percentage of other participants who in the same survey had admitted to having engaged in a given behavior. Being provided with information that suggested that a majority of survey takers had admitted a certain questionable behavior increased participants' willingness to disclose their engagement in other, also sensitive, behaviors. Other studies have found that the tendency to reciprocate information disclosure is so ingrained that people will reveal more information even to a computer agent that provides information about itself [53]. Findings such as this may help to explain the escalating amounts of self-disclosure we witness online: If others are doing it, people seem to reason unconsciously, doing so oneself must be desirable or safe.

Other people's behavior affects privacy concerns in other ways, too. Sharing personal information with others makes them "co-owners" of that information [54] and, as such, responsible for its protection. Mismanagement of shared information by one or more co-owners causes "turbulence" of the privacy boundaries and, consequently, negative reactions, including anger or mistrust. In a study of undergraduate Facebook users [55], for instance, turbulence of privacy boundaries, as a result of having one's profile exposed to unintended audiences, dramatically increased the odds that a user would restrict profile visibility to friends-only.

Likewise, privacy concerns are often a function of past experiences. When something in an environment changes, such as the introduction of a camera or other monitoring devices, privacy concern is likely to be activated. For instance, surveillance can produce discomfort [56] and negatively affect worker productivity [57]. However, privacy concern, like other motivations, is adaptive; people get used to levels of intrusion that do not change over time. In an experiment conducted in Helsinki [58], the installation of sensing and monitoring technology in households led family members initially to change their behavior, particularly in relation to conversations, nudity, and sex. And yet, if they accidentally performed an activity, such as walking naked into the kitchen in front of the sensors, it seemed to have the effect of "breaking the ice"; participants then showed less concern about repeating the behavior. More generally, participants became inured to the presence of the technology over time.

The context-dependence of privacy concern has major implications for the risks associated with modern information and communication technology [59]. With

online interactions, we no longer have a clear sense of the spatial boundaries of our listeners. Who is reading our blog post? Who is looking at our photos online? Adding complexity to privacy decision-making, boundaries between public and private become even less defined in the online world [60] where we become social media friends with our coworkers and post pictures to an indistinct flock of followers. With different social groups mixing on the Internet, separating online and offline identities and meeting our and others' expectations regarding privacy becomes more difficult and consequential [61]. Hence, it is important for system designers to account for context-dependence aspect of privacy. There might not be a global solution that fully addresses the issues caused by context-dependence aspect of privacy decisions, but being aware of that might lead to some best practice approaches to empower users' decisions. As a summary:

- **Privacy is context-dependent.** People might have different preferences based on a myriad of different, even inconspicuous factors. For instance, self-disclosure may be higher in a warm and comfortable room, compared to a cold and dark room.
- **Privacy concern is a function of users' past experiences in an environment.** Such concerns can change in response to changes in the environment (i.e., when setting up a surveillance camera for the first time). However, users can adapt to the new environment and get used to it too.

4.4 Malleability and Influence

Whereas individuals are often unaware of the diverse factors that determine their concern about privacy in a particular situation, entities whose prosperity depends on information revelation by others are much more sophisticated. With the emergence of the information age, growing institutional and economic interests have developed around disclosure of personal information, from online social networks to behavioral advertising. It is not surprising, therefore, that some entities have an interest in, and have developed expertise in, exploiting behavioral and psychological processes to promote disclosure [62]. Such efforts play on the malleability of privacy preferences, a term we use to refer to the observation that various, some- times subtle, factors can be used to activate or suppress privacy concerns, which in turn affect behavior.

Default settings are an important tool used by different entities to affect information disclosure. A large body of research has shown that default settings matter for decisions as important as organ donation and retirement saving [63]. Sticking to default settings is convenient, and people often interpret default settings as implicit recommendations [64]. Thus, it is not surprising that default settings for one's profile's visibility on social networks [65], or the existence of opt-in or opt-out privacy policies on websites [66], affect individuals' privacy behavior. Figure 4.3 shows how default visibility settings became more revelatory between 2005 and

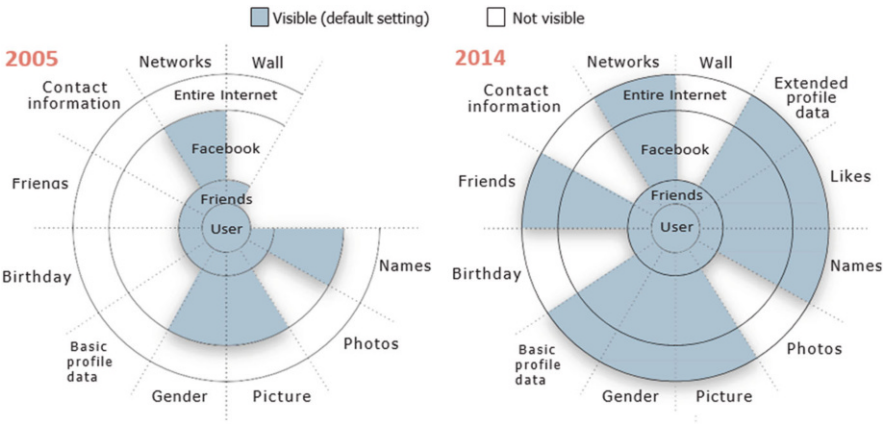

Fig. 4.3 Changes in Facebook default profile visibility settings over time (2005–2014). Fields such as "Likes" and "Extended Profile Data" did not exist in 2005. This figure is based on the authors' data and the original visualization created by M. McKeon, available at http://mattmckeon.com/facebook-privacy

2014, disclosing more personal information to larger audiences, unless the user manually overrode the defaults.

In addition to default settings, websites can also use design features that frustrate or even confuse users into disclosing personal information [67], a practice that has been referred to as "malicious interface design" [68]. Another obvious strategy that commercial entities can use to avoid raising privacy concerns is not to "ring alarm bells" when it comes to data collection. When companies do ring them—for example, by using overly fine-tuned personalized advertisements—consumers are alerted [69] and can respond with negative "reactance" [70].

Various so-called antecedents [71] affect privacy concerns and can be used to influence privacy behavior. For instance, trust in the entity receiving one's personal data soothes concerns. Moreover, because some interventions that are intended to protect privacy can establish trust, concerns can be muted by the very interventions intended to protect privacy. Perversely, 62% of respondents to a survey believed (incorrectly) that the existence of a privacy policy implied that a site could not share their personal information without permission [41], which suggests that simply posting a policy that consumers do not read may lead to misplaced feelings of being protected.

Control is another feature that can inculcate trust and produce paradoxical effects. Perhaps because of its lack of controversiality, control has been one of the capstones of the focus of both industry and policy-makers in attempts to balance privacy needs against the value of sharing. Control over personal information is often perceived as a critical feature of privacy protection [40]. In principle, it does provide users with the means to manage access to their personal information. Research, however, shows that control can reduce privacy concern [47], which in turn can

have unintended effects. For instance, one study found that participants who were provided with greater explicit control over whether and how much of their personal information researchers could publish ended up sharing more sensitive information with a broader audience, the opposite of the ostensible purpose of providing such control [72].

Similar to the normative perspective on control, increasing the transparency of firms' data practices would seem to be desirable. However, transparency mechanisms can be easily rendered ineffective. Research has highlighted not only that an overwhelming majority of Internet users do not read privacy policies [73], but also that few users would benefit from doing so; nearly half of a sample of online privacy policies were found to be written in language beyond the grasp of most Internet users [74]. Indeed, and somewhat amusingly, it has been estimated that the aggregate opportunity cost if US consumers actually read the privacy policies of the sites they visit would be $781 billion/year [75].

Although uncertainty and context-dependence lead naturally to malleability and manipulation, not all malleability is necessarily sinister. Consider monitoring. Although monitoring can cause discomfort and reduce productivity, the feeling of being observed and accountable can induce people to engage in prosocial behaviors or (for better or for worse) adhere to social norms [76]. Prosocial behavior can be heightened by monitoring cues as simple as three dots in a stylized face configuration [77]. By the same token, the depersonalization induced by computer-mediated interaction [78], either in the form of lack of identifiability or of visual anonymity [79], can have beneficial effects, such as increasing truthful responses to sensitive surveys [80, 81]. Whether elevating or suppressing privacy concerns is socially beneficial critically depends, yet again, on context [a meta-analysis of the impact of de-identification on behavior is provided in [82]]. For example, perceptions of anonymity can alternatively lead to dishonest or prosocial behavior. Illusory anonymity induced by darkness caused participants in an experiment [83] to cheat in order to gain more money. This can be interpreted as a form of disinhibition effect [84], by which perceived anonymity licenses people to act in ways that they would otherwise not even consider. In other circumstances, though, anonymity leads to prosocial behavior for instance, higher willingness to share money in a dictator game, when coupled with priming of religiosity [85].

As a summary, in contrast to unintentional effects of uncertainty and context-dependence which can lead to malleability, in this section we discussed intentional interventions that can nudge people towards disclosing more than what they really want to:

- **Default effects can lead to over-disclosure.** People might interpret default as the recommended option.
- **Malicious interface design is a design practice that aims to influence user behavior**, including nudging the user towards increased disclosures.
- **Having a sense of control can lead to over-disclosure.** Users are more likely to disclosure information in a system that provides granular control. A granular control induces a higher sense of control and in turn decreases privacy concerns.

4.5 Conclusions

Norms and behaviors regarding private and public realms greatly differ across cultures [86]. Americans, for example, are reputed to be more open about sexual matters than are the Chinese, whereas the latter are more open about financial matters (such as income, cost of home, and possessions). And even within cultures, people differ substantially in how much they care about privacy and what information they treat as private. And as we have sought to highlight in this chapter, privacy concerns can vary dramatically for the same individual, and for societies, over time.

If privacy behaviors are culture- and context-dependent, however, the dilemma of what to share and what to keep private is universal across societies and over human history. The task of navigating those boundaries and the consequences of mismanaging them have grown increasingly complex and fateful in the information age, to the point that our natural instincts seem not nearly adequate.

In this chapter, we used three themes to organize and draw connections between the social and behavioral science literature on privacy and behavior. We end the chapter with a brief discussion of the reviewed literature's relevance to privacy policy.

- **Uncertainty and context-dependence** imply that people cannot always be counted on to navigate the complex trade-offs involving privacy in a self-interested fashion. People are often unaware of the information they are sharing, unaware of how it can be used, and even in the rare situations when they have full knowledge of the consequences of sharing, **uncertain** about their own preferences.
- **Malleability**, in turn, implies that people are easily influenced in what and how much they disclose. Moreover, what they share can be used to influence their emotions, thoughts, and behaviors in many aspects of their lives, as individuals, consumers, and citizens. Although such influence is not always or necessarily malevolent or dangerous, relinquishing control over one's personal data and over one's privacy alters the balance of power between those holding the data and those who are the subjects of that data.

Insights from the social and behavioral empirical research on privacy reviewed here suggest that policy approaches that rely exclusively on informing or "empowering" the individual are unlikely to provide adequate protection against the risks posed by recent information technologies. Consider transparency and control, two principles conceived as necessary conditions for privacy protection. The research we highlighted shows that they may provide insufficient protections and even backfire when used apart from other principles of privacy protection.

The research reviewed here suggests that if the goal of policy is to adequately protect privacy (as we believe it should be), then we need policies that protect individuals with minimal requirement of informed and rational decision-making—policies that include a baseline framework of protection, such as the principles embedded in the so-called fair information practices [87]. People need

assistance and even protection to aid in navigating what is otherwise a very uneven playing field. As highlighted by our discussion, a goal of public policy should be to achieve a more even equity of power between individuals, consumers, and citizens on the one hand and, on the other, the data holders such as governments and corporations that currently have the upper hand. To be effective, privacy policy should protect real people—who are naive, uncertain, and vulnerable—and should be sufficiently flexible to evolve with the emerging unpredictable complexities of the information age.

Acknowledgments The authors gratefully acknowledge the American Association for the Advancement of Science for allowing the use of previously published materials [88] and Reza Ghaiumy Anaraky for excellent editing.

References

1. Mayer-Schönberger, V. 2011. *Delete: The Virtue of Forgetting in the Digital Age*. Princeton: Princeton University Press.
2. Sweeney, L. 2002. k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems* 10 (05): 557–570.
3. McAfee, A., E. Brynjolfsson, T.H. Davenport, D. Patil, and D. Barton 2012. Big data: The management revolution. *Harvard Business Review* 90 (10): 60–68.
4. Tatonetti, N.P., P.Y. Patrick, R. Daneshjou, and R.B. Altman. 2012. Data-driven prediction of drug effects and interactions. *Science Translational Medicine* 4 (125): 125ra31–125ra31.
5. Acquisti, A., and R. Gross. 2009. Predicting social security numbers from public data. *Proceedings of the National Academy of Sciences* 106 (27): 10975–10980.
6. Cohen, J.E. 1999. Examined lives: Informational privacy and the subject as object. *Stanford Law Review* 52: 1373.
7. Crawford, K., M.L. Gray, and K. Miltner. 2014. Big data— critiquing big data: Politics, ethics, epistemology—special section introduction. *International Journal of Communication* 8: 10.
8. Posner, R.A. 1981. The economics of privacy. *The American Economic Review* 71 (2): 405–409.
9. Solove, D.J. 2012. Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review* 126: 1880.
10. Solove, D.J. 2005. A taxonomy of privacy. *University of Pennsylvania Law Review* 154: 477.
11. Schoeman, F.D. 1984. *Philosophical Dimensions of Privacy: An Anthology*. Cambridge: Cambridge University Press.
12. DePaulo, B.M., C. Wetzel, R. Weylin Sternglanz, and M.J.W. Wilson. 2003. Verbal and nonverbal dynamics of privacy, secrecy, and deceit. *Journal of Social Issues* 59 (2): 391–410.
13. Margulis, S.T. 2003. Privacy as a social issue and behavioral concept. *Journal of Social Issues* 59 (2): 243–261.
14. Goffman, E. 1971. *Relations in Public: Microstudies of the Public Order*. Milton Park: Routledge.
15. Sundstrom, E., and I. Altman. 1976. Interpersonal relationships and personal space: Research review and theoretical model. *Human Ecology* 4 (1): 47–67.
16. Schwartz, B. 1968. The social psychology of privacy. *American Journal of Sociology* 73 (6): 741–752.
17. Laufer, R.S., and M. Wolfe. 1977. Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues* 33 (3): 22–42.
18. Tsai, J.Y., S. Egelman, L. Cranor, and A. Acquisti. 2011. The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research* 22 (2): 254–268.

19. Slovic, P. 1995. The construction of preference. *American Psychologist* 50 (5): 364.
20. Singer, E., H.J. Hippler, and N. Schwarz. 1992. Confidentiality assurances in surveys: Reassurance or threat? *International Journal of Public Opinion Research* 4 (3): 256–268. (1992)
21. Skotko, V.P., and D. Langmeyer. 1977. The effects of interaction distance and gender on self-disclosure in the dyad. *Sociometry* 40: 178–182.
22. Louis Harris and Associates, Inc. 1991. Equifax-Harris consumer privacy survey. Equifax, Inc. https://hdl.handle.net/1902.29/H-912046
23. Culnan, M.J., and P.K. Armstrong. 1999. Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science* 10 (1): 104–115.
24. Smith, H.J., S.J. Milberg, and S.J. Burke. 1996. Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly* 20: 167–196.
25. Lubin, B., and R.L. Harrison. 1964. Predicting small group behavior with the self-disclosure inventory. *Psychological Reports* 15 (1): 77–78.
26. Spiekermann, S., J. Grossklags, and B. Berendt. 2001. E-privacy in 2nd generation e-commerce: privacy preferences versus actual behavior. In *Proceedings of the 3rd ACM Conference on Electronic Commerce*, 38–47. New York: ACM.
27. Norberg, P.A., D.R. Horne, and D.A. Horne. 2007. The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs* 41 (1): 100–126.
28. Ajzen, I., and M. Fishbein. 1997. Attitude-behavior relations: A theoretical analysis and review of empirical research. *Psychological Bulletin* 84 (5): 888.
29. Klopfer, P.H., and D.I. Rubenstein. 1977. The concept privacy and its biological basis. *Journal of Social Issues* 33 (3): 52–65.
30. Acquisti, A., and R. Gross. 2006. Imagined communities: Awareness, information sharing, and privacy on the facebook. In *International Workshop on Privacy Enhancing Technologies*, 36–58. Berlin: Springer.
31. Acquisti, A. 2004. Privacy in electronic commerce and the economics of immediate gratification. In *Proceedings of the 5th ACM Conference on Electronic Commerce*, 21–29. New York: ACM.
32. Hann, I.H., K.L. Hui, S.Y.T. Lee, and I.P. Png 2007. Overcoming online information privacy concerns: An information-processing theory approach. *Journal of Management Information Systems* 24 (2): 13–42.
33. Acquisti, A., L.K. John, and G. Loewenstein. 2013, What is privacy worth? *The Journal of Legal Studies* 42 (2): 249–274.
34. Altman, I., and D.A. Taylor. 1973. *Social Penetration: The Development of Interpersonal Relationships*. New York: Holt, Rinehart & Winston.
35. Frattaroli, J. 2006. Experimental disclosure and its moderators: A meta-analysis. *Psychological Bulletin* 132 (6): 823.
36. Pennebaker, J.W. 1993. Putting stress into words: Health, linguistic, and therapeutic implications. *Behaviour Research and Therapy* 31 (6): 539–548.
37. Steinfield, C., N.B. Ellison, and C. Lampe. 2008. Social capital, self-esteem, and use of online social network sites: A longitudinal analysis. *Journal of Applied Developmental Psychology* 29 (6): 434–445.
38. Toma, C.L., and J.T. Hancock. 2013. Self-affirmation underlies facebook use. *Personality and Social Psychology Bulletin* 39 (3): 321–331.
39. Tamir, D.I., and J.P. Mitchell. 2012. Disclosing information about the self is intrinsically rewarding. *Proceedings of the National Academy of Sciences* 109 (21): 8038–8043.
40. Westin, A.F. 1967. Privacy and freedom atheneum. *New York* 7: 431–453.
41. Hoofnagle, C.J., and J.M. Urban. 2014 Alan Westin's privacy homo economicus. *Wake Forest Law Review* 49: 261.
42. Marx, G.T. 2001. Murky conceptual waters: The public and the private. *Ethics and Information Technology* 3 (3): 157–169.
43. Thibaut, J.W., and H.H. Kelley. 1959. *The Social Psychology of Groups*. Milton Park: Routledge.

44. Nissenbaum, H. 2009. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Palo Alto: Stanford University Press
45. Boyd, D. 2014. *It's Complicated: The Social Lives of Networked Teens*. New Haven: Yale University Press.
46. Stutzman, F.D., R. Gross, and A. Acquisti. 2013. Silent listeners: The evolution of privacy and disclosure on facebook. *Journal of Privacy and Confidentiality* 4 (2): 2.
47. Xu, H., H.H. Teo, B.C. Tan, and R. Agarwal. 2009. The role of push-pull technology in privacy calculus: The case of location-based services. *Journal of Management Information Systems* 26 (3): 135–174.
48. John, L.K., A. Acquisti, and G. Loewenstein. 2010. Strangers on a plane: Context-dependent willingness to divulge sensitive information. *Journal of Consumer Research* 37 (5): 858–873.
49. Altman, I. 1975. *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*. Pacific Grove: Brooks/Cole.
50. Chaikin, A.L., V.J. Derlega, and S.J. Miller. 1976. Effects of room environment on self-disclosure in a counseling analogue. *Journal of Counseling Psychology* 23 (5): 479.
51. Derlega, V.J., and A.L. Chaikin 1977. Privacy and self-disclosure in social relationships. *Journal of Social Issues* 33 (3): 102–115.
52. Acquisti, A., L.K. John, and G. Loewenstein. 2012. The impact of relative standards on the propensity to disclose. *Journal of Marketing Research* 49 (2): 160–174.
53. Moon, Y. 2000. Intimate exchanges: Using computers to elicit self-disclosure from consumers. *Journal of Consumer Research* 26 (4): 323–339.
54. Petronio, S. 2002. *Boundaries of Privacy: Dialectics of Disclosure*. Albany: State University of New York Press.
55. Stutzman, F., and J. Kramer-Duffield. 2010. Friends only: examining a privacy-enhancing behavior in facebook. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 1553–1562. New York: ACM.
56. Honess, T., and E. Charman. 1992. *Closed Circuit Television in Public Places: Its Acceptability and Perceived Effectiveness*. Home Office Police Research Group.
57. Gagné, M., and E.L. Deci. 2005. Self-determination theory and work motivation. *Journal of Organizational Behavior* 26 (4): 331–362.
58. Oulasvirta, A., A. Pihlajamaa, J. Perkiö, D. Ray, T. Vähäkangas, T. Hasu, N. Vainio, and P. Myllymäki. 2012. Long-term effects of ubiquitous surveillance in the home. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*, 41–50. New York: ACM.
59. Palen, L., and P. Dourish. 2003. Unpacking privacy for a networked world. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 129–136. New York: ACM.
60. Tufekci, Z. 2008. Can you see me now? audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society* 28 (1): 20–36.
61. Bargh, J.A., K.Y. McKenna, and G.M. Fitzsimons. 2002. Can you see the real me? activation and expression of the true self on the internet. *Journal of Social Issues* 58 (1): 33–48.
62. Calo, R. 2013. Digital market manipulation. *The George Washington Law Review* 82:995.
63. Johnson, E.J., and D. Goldstein 2003. Do defaults save lives? *Science* 302: 1338–1339.
64. McKenzie, C.R., M.J. Liersch, and S.R. Finkelstein. 2006. Recommendations implicit in policy defaults. *Psychological Science* 17 (5): 414–420.
65. Gross, R., and A. Acquisti 2005. Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, 71–80. New York: ACM.
66. Johnson, E.J., S. Bellman, and G.L. Lohse. 2002. Defaults, framing and privacy: Why opting in-opting out. *Marketing Letters* 13 (1): 5–15.
67. Hartzog, W. 2010. Website design as contract. *American University Law Review* 60: 1635.
68. Conti, G., and E. Sobiesk 2010. Malicious interface design: exploiting the user. In *Proceedings of the 19th International Conference on World Wide Web*, 271–280. New York: ACM.
69. Goldfarb, A., and C. Tucker. 2011. Online display advertising: Targeting and obtrusiveness. *Marketing Science* 30 (3): 389–404.
70. White, T.B., D.L. Zahay, H. Thorbjørnsen, and S. Shavitt. 2008. Getting too personal: Reactance to highly personalized email solicitations. *Marketing Letters* 19 (1): 39–50.

71. Smith, H.J., T. Dinev, and H. Xu. 2011. Information privacy research: An interdisciplinary review. *MIS Quarterly* 35 (4): 989–1016.
72. Brandimarte, L., A. Acquisti, and G. Loewenstein. 2013. Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science* 4 (3): 340–347.
73. Jensen, C., C. Potts, and C. Jensen. 2005. Privacy practices of internet users: Self-reports versus observed behavior. *International Journal of Human-Computer Studies* 63 (1–2): 203–227.
74. Jensen, C., and C. Potts 2004. Privacy policies as decision-making tools: An evaluation of online privacy notices. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 471–478. New York: ACM.
75. McDonald, A., and L. Cranor. 2008. *I/S: A Journal of Law and Policy for the Information Society* 4: 540–565.
76. Wedekind, C., and M. Milinski. Cooperation through image scoring in humans. *Science* 288 (5467): 850–852.
77. Rigdon, M., K. Ishii, M. Watabe, and S. Kitayama. 2009. Minimal social cues in the dictator game. *Journal of Economic Psychology* 30 (3): 358–367.
78. Kiesler, S., J. Siegel, and T.W. McGuire. 1984. Social psychological aspects of computer-mediated communication. *American Psychologist* 39 (10): 1123.
79. Joinson, A.N. 2001. Self-disclosure in computer-mediated communication: The role of self-awareness and visual anonymity. *European Journal of Social Psychology* 31 (2): 177–192.
80. Weisband, S., and S. Kiesler. 1996. Self disclosure on computer forms: Meta-analysis and implications. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 3–10. New York: ACM.
81. Tourangeau, R., and T. Yan. 2007. Sensitive questions in surveys. *Psychological Bulletin* 133 (5): 859.
82. Postmes, T., and R. Spears. 1998. Deindividuation and antinormative behavior: A meta-analysis. *Psychological Bulletin* 123 (3): 238.
83. Zhong, C.B., V.K. Bohns, and F. Gino. 2010. Good lamps are the best police: Darkness increases dishonesty and self-interested behavior. *Psychological Science* 21 (3): 311–314.
84. Suler, J. 2004. The online disinhibition effect. *Cyberpsychology & Behavior* 7 (3): 321–326.
85. Shariff, A.F., and A. Norenzayan. 2007. God is watching you: Priming god concepts increases prosocial behavior in an anonymous economic game. *Psychological Science* 18 (9): 803–809.
86. Moore Jr, B. 1984. *Privacy: Studies in Social and Cultural History, Armonk, NY: Me Sharpe*. Milton Park: Routledge.
87. Welfare Secretary's Advisory Committee on Automated Personal Data Systems. 1973. Records, computers, and the rights of citizens: report. United States Department of Health, Education, and Welfare; for for sale by the Superintendent of Documents, US.
88. Acquisti, A., L. Brandimarte, and G. Loewenstein. 2015. Privacy and human behavior in the age of information. *Science* 347 (6221): 509–514. https://doi.org/10.1126/science.aaa1465. http://science.sciencemag.org/content/347/6221/509