23 The Consumer Psychology of Online Privacy

Insights and Opportunities from Behavioral Decision Theory

Leslie K. John

As people spend more time shopping, gaming, and socializing online, and as data-gathering technology has become more sophisticated, consumer privacy has been dubbed "one of the most important issues facing management practice" (Awad & Krishnan, 2006, p. 14). The Internet, in its seemingly boundless capacity to facilitate information disclosure, dissemination, aggregation, and storage, has added great complexity to consumers' management of their personal data. Consumers face, on the one hand, risks of privacy invasions – from receiving spam e-mails to identity theft – and on the other, benefits such as improved convenience and personalization.

From a firm's perspective, the Internet has dramatically changed the way offerings are marketed. With respect to promotions, for example, in the past, marketers had strong control over the message and the medium. Marketers could "push" their promotions onto consumers, who had little say in when and how they were contacted. Today, however, people consume media on their own terms, rendering traditional methods of marketing communications – such as primetime television advertisements – less effective. Now more than ever, marketers must "be in the right place at the right time," which requires having detailed information on their customers. Fortunately for firms, just as the Internet has heightened the importance of understanding the customer, new Internet technologies have increased the ease of obtaining and using detailed customer data.

As a result, online advertising, and behavioral targeting in particular, has become of central importance to marketing. Behavioral targeting refers to the delivery of advertisements tailored to a user's revealed preferences (for an overview, see Gilbert, 2008). Unlike mere targeting, which refers to the traditional practice of tailoring messages to groups of consumers with similar interests and demographic characteristics, behavioral targeting is more invasive, since it is conducted at the individual level. Information is gleaned about the individual consumer by tracking his online behavior. This information is then used to show him customized advertisements.

How do consumers navigate the new complexities of information sharing in this context of unprecedented openness? How do firms maximize the new marketing capabilities afforded by new technologies, while respecting consumers' privacy? Behavioral decision theory (BDT) and, more broadly, social psychology provide answers. In this chapter, I first discuss how research in these fields can account for the privacy paradox – people's tendency to say they

care about their privacy despite their willingness to reveal extremely sensitive personal information online. Drawing on this understanding, in the second section I show how this perspective can account for many of the seemingly paradoxical choices consumers make with respect to the management of their personal data and their reactions to behavioral targeting in particular. In doing so, I highlight recent research and venture into more speculative areas that represent opportunities for future inquiry. I conclude with a discussion of broad topics worthy of future research, including interventions to help consumers better navigate issues of online privacy.

Part 1: The Privacy Paradox Explained

In polls and surveys, consumers indicate profound and increasing concern for their privacy (ConsumersUnion.org, 2008; Federal Trade Commission, 2000, 2006; Jupiter Research, 2002; Goldfarb & Tucker, 2011a), and for good reason – it is fundamental to human development (Berscheid, 1977). Yet, from the posting of suggestive photographs on social networking sites (SNSs) to the impulsive broadcasting of illicit activities on Twitter, consumers' behavior often suggests a remarkable lack of concern for privacy. In addition to being inconsistent with stated attitudes, this behavior is also surprising because, as regularly highlighted in the media, there are very real dangers to online disclosure. For example, Virgin Atlantic flight attendants were fired after the company discovered that they had posted derogatory statements about the company on Facebook (Conway, 2008).

The privacy paradox (Norberg & Horne, 2007) – the discrepancy between people's stated and revealed preferences for privacy – has been documented empirically: those who indicate serious privacy concern nevertheless reveal intimate details of their lives for trivial rewards (Acquisti & Gross, 2009; Spiekermann, Grossklags, & Berendt, 2001; Tufecki, 2008). The paradox is also readily apparent in consumers' responses to behavioral targeting – consumers say they reject behavioral targeting, yet research suggests that it can be effective (Goldfarb & Tucker, 2011b; Lambrecht & Tucker, 2013). What accounts for this paradox? Behavioral decision theory provides some answers.

(In)tangibility

Privacy is a "faceless" issue – an amorphous concept, its definition long debated by scientists, philosophers, and legal scholars alike (Altman, 1975; Culnan & Armstrong, 1999; Jourard, 1966; Laufer & Wolfe, 1977; Margulis, 2003; Smith, Milberg, & Burke, 1996; Warren & Brandeis, 1890; Westin, 1991).[1] Research has shown that people's thoughts and behaviors are much more strongly

1 This chapter skirts discussion of how to define privacy and is based on the definition of privacy as concern over the security of one's personal information (Smith, Milberg, & Burke, 1996).

affected by issues that are specific and concrete relative to those that are abstract, such as privacy (Jenni & Loewenstein, 1997; Nisbett & Ross, 1980; Schelling, 1968). For example, people are more likely to donate to victims who are highly identifiable (and hence tangible) as opposed to those who are not (Cryder, Loewenstein, Scheines, 2013; Small & Loewenstein, 2003). The latter are mere statistics that fail to evoke the affective responses that stimulate giving.

Further contributing to its intangibility is the fact that the benefits of privacy are abstract and difficult to quantify. How much privacy have you lost if someone catches a glimpse of your naked body? What privacy intrusions have you prevented by providing a fictitious email address to a commercial website? The material value of privacy is extremely difficult to estimate (Hann, Hui, Lee, & Png, 2002a). Its psychological value is therefore likely to be even less well defined, causing consumers to prioritize other, more tangible considerations, which are often associated with sacrifices in privacy – for example, divulging personal data to receive store discounts.

Because privacy is an intangible, hard-to-quantify concept, concern for it is likely to be latent – privacy is not an issue that is typically at the forefront of people's minds. This can explain the incongruence between stated privacy attitudes and behaviors. By explicitly asking about the issue, public opinion polls rouse and hence are able to measure privacy concerns that often remain latent.[2] Privacy's intangibility can also explain why public outcry about privacy ebbs and flows with media coverage of salient privacy breaches. For example, after news of the National Security Agency's mass electronic surveillance data mining program broke in June 2013, people were less likely to enter privacy-sensitive search terms into Google (Marthews & Tucker, 2014).

Consistent with this line of thinking, consumers are much more willing to part with their information when it is collected covertly as opposed to overtly. For example, John, Acquisti, and Loewenstein (2011) asked New York Times readers (N = 890) whether they had engaged in a series of sensitive, if not also illegal, behaviors such as "Making a false insurance claim." The method of inquiry varied between subjects. In the overt inquiry condition, for each behavior subjects were asked, "Have you ever done this behavior?" and to rate its unethicality. In the covert inquiry condition, subjects had the choice of answering, "If you have ever done this behavior, how unethical do you think it was?" or, "If you have never done this behavior, how unethical do you think it would be, if you were to choose to do it?" Subjects in the covert inquiry condition were about 1.5 times more likely to admit to having engaged in the sensitive behaviors compared to those in the direct inquiry condition. Although the information requested was the same across conditions, covert inquiry made

2 Caveat: these polls are prone to overstating concern due to acquiescent response bias and the fact that there is no cost in saying you care about privacy. Conjoint analyses of concern for privacy are typically more compelling, although some go to extremes in attempting to quantify the unquantifiable (Hann, Hui, Lee, & Png, 2002a; Png, 2007).

the act of admission secondary – almost an afterthought – which increased self-disclosure by keeping privacy concern latent.

Broadly, intangibility accounts for why much of the covert tracking of individuals' online behavior, a necessary condition for behavioral targeting, fails to rouse concern. It also explains how, when it comes to the delivery of behaviorally targeted advertisements, overly personalized advertisements can backfire because they bring privacy concerns to the fore (White, Zahay, Thorbjorsen, & Shavitt, 2008). For example, the retail chain Target endured a public relations nightmare when it marketed diapers to a teen who the company (correctly) inferred to be pregnant due to her shopping patterns (Duhigg, 2012; Hill, 2012).

Multiple Motives: Balancing the Desire for Privacy with the Desire to Divulge

At the same time as they express grave concerns over their privacy, people also have a desire to divulge, and for good reason. A wealth of research has documented benefits of confiding in others. For example, disclosure yields health benefits, such as reduced blood pressure and increased blood hemoglobin (Pennebaker, 1984; Pennebaker, Kiecolt-Glaser, & Glaser, 1988; Smyth, 1998); professional benefits, such as better grades and employment (Spera, Buhrfeind, & Pennebaker, 1994); and psychological benefits, such as intimacy (Jourard, 1959; Mikulincer & Nachson, 1991; Reis & Shaver, 1988) and liking (Collins & Miller, 1994; Cozby, 1972). Moreover, recent neuroscientific research suggests that self-disclosure is intrinsically rewarding (Tamir & Mitchell, 2012).

What is the relationship between the desire to divulge and the desire for privacy? Most people at different times and in different situations experience each motivation; sometimes they experience both simultaneously. For example, a newly pregnant woman might have the urge to divulge her pregnancy, but at the same time wish to keep it private initially, until the risk of miscarriage is significantly reduced (or until the shotgun wedding). The notion that one can have simultaneous, seemingly contradictory, preferences for information to be both shared *and* withheld is characterized by multiple motive models of behavior (Loewenstein & O'Donoghue, 2005), which capture the familiar feeling of being of two minds. Applied to privacy, this perspective suggests that to understand variation in information revelation across situations, one must understand the operation of both motives – the desire to protect versus that to share information.

Multiple motives help to explain the privacy paradox. The Internet, perhaps more than any other communication medium, makes the desire to divulge salient. Facebook, for example, is riddled with cues that heighten the desire to disclose; users are perpetually posed the question, "What's on your mind?" and are peppered with prompts urging them to comment on others' postings. The desire for privacy, on the other hand, is simultaneously downplayed; privacy settings are accessible only by clicking on a cryptic-looking icon on a user's profile. Understood within this multiple-motive framework, the

Internet's tendency to heighten the desire to divulge while simultaneously downplaying the desire for privacy accounts for consumers' willingness to divulge in online contexts despite their privacy concern.

Preliminary evidence suggests that the success of behavioral targeting, and in particular dynamic retargeting (described later in this section) depends on the delicate interplay between two desires: personalization versus privacy (Tucker, 2014; Wathieu & Friedman, 2009). Consumers' desire for relevant, personalized content predicts that they will accept highly targeted (i.e., relevant) advertisements. And although salient advertisements are likely to be noticed, consumers' desire for privacy predicts that they will reject highly salient – and hence obtrusive – advertisements. What happens when an advertisement is both highly relevant *and* highly obtrusive? Goldfarb and Tucker (2011c) suggest that privacy concerns trump relevance concerns. Specifically, they found that contextually targeted advertisements, ones that promote products that are highly relevant to the web page on which they appear, decrease in effectiveness as they become more obtrusive. For example, an advertisement for a vacation package presented on a travel news site will be effective when presented in a discreet, text-based format (i.e., when it is relevant but not obtrusive), as opposed to a more intrusive format, such as a large pop-up window (i.e., when it is both relevant and obtrusive). In other words, a multiple-motive framework accounts for why advertisements that are highly targeted *and* highly obtrusive are ineffective when compared with those that have only one of these characteristics.

For its part, the effectiveness of dynamic retargeting is not yet well understood; a consideration of multiple motives could help. In dynamic retargeting, consumers are shown an advertisement for an offering that they recently viewed. For example, if on Monday the consumer views a coat on Amazon.com, on Tuesday he is shown an advertisement for the identical product, though perhaps on a different website. A multiple motive account might suggest that the success of such dynamic retargeting depends on the likeness of the advertisement to the initially viewed offering, in this case, the coat viewed on Monday. It could be that dynamically retargeted ads of *similar* products are more effective than those of *identical* products. Although the latter satisfies the desire for personalization, it does so by potentially rousing privacy concerns – seeing the identical product makes it salient to the consumer that he is being tracked. Behaviorally retargeting similar, but not identical, advertisements may hit the "sweet spot" in appealing to these two motives. Future research is needed to better understand how behaviorally retargeted ads affect the delicate interplay of conflicting motives. Such an understanding will facilitate the design of advertisements that are more palatable from the consumer's standpoint, and in turn more effective from the marketer's standpoint.

Synthesis of Part 1

Taken together, intangibility and mixed motives account for the privacy paradox and suggest that privacy is likely to be a domain characterized by great

preference uncertainty. In the next section, I describe how this perspective accounts for a variety of seemingly inconsistent choices people make with respect to their privacy.

Part 2: How Behavioral Decision Theory Explains Privacy-Decision Making Phenomena

Context Effects

When people are uncertain of their preferences, inconsistencies in their judgments and decision making abound (Fox & Tversky, 1995; Hsee, Loewenstein, Blount, & Bazerman, 1999; Slovic, 1995). One way that people try to resolve this uncertainty is to rely on contextual cues. Importantly, the contextual cues that guide privacy concerns are often incommensurate with the prevailing costs and benefits of divulgence. This distortion can help account for the seemingly self-destructive, or at least inconsistent, choices consumers make. As I describe in the next three paragraphs, context effects account for why consumers' willingness to reveal personal data is (1) insensitive to cues to which they should be sensitive; (2) sensitive to cues to which they should be insensitive; and (3) responsive to contextual cues in exactly the wrong way. Compliance with marketers' requests for personal data can have negative outcomes for the consumer; for example, having one's identity stolen as a result of divulging one's social security number. As I explain in the following paragraphs, contextual cues can cause consumers to comply with requests for information in precisely the situations in which it is against their self-interest to do so, that is, in situations in which their information is more likely to be used for nefarious, as opposed to legitimate, purposes.

Privacy policies are contextual cues that should, but fail to, stimulate privacy concerns. A privacy policy is an institutionally provided statement detailing how consumer data are gathered, stored, and used. It therefore contains information relevant to the costs and benefits of disclosure. Consider the website realage.com, on which users divulge intensely personal health information in exchange for the simple knowledge of how their calendar age compares to their biological age. The privacy policy provides a long list of permissions that users implicitly provide. For example, users allow the company to "disclose your personally identifiable information" to "affiliates, strategic partners, agents, and third-party marketers" for "research, administrative, and/or business purposes" and "to offer you products." Translation: "you are giving us permission to do almost anything with your data" – for example, to sell personally identifying information of (self-identified) HIV patients to health insurance companies. The privacy policy thus contains information that should cause users to think twice about the relative imbalance of the benefits they glean versus provide to realage.com in complying with the site's requests for personal data. Whether it is because privacy policies are commonplace (leading to

desensitization, discussed further in the "Comparative Judgments" subsection), or because they can be intimidatingly long (according to McDonald & Cranor, 2008, it would take Americans 54 billion hours annually to read the policy of each new site they visited), privacy policies usually go completely unread. As a result, they fail to rouse privacy considerations even when they should. Moreover, requests for consumers' information are typically decoupled from their accompanying privacy policy. When decontextualized in this manner, even the most diligently read policies fail to affect people's behavior (Adjerid, Acquisti, Brandimarte, & Loewenstein, 2013).

Peoples' willingness to part with their personal data has also been found to be affected by irrelevant factors, such as whether the disclosure experience is fluent. People disclose less when questions are presented in a disfluent manner (Alter & Oppenheimer, 2009), and curiously, emphasizing that a disclosure is *reversible* (e.g., that providing an email address to a mailing list can be "undone" by unsubscribing) *or* that it is *irreversible*, increases people's reluctance to part with their information (Peer, Acquisti, & Loewenstein, n.d.). Even though fluency and reversibility can be independent from the risks of disclosure, they can cue people to think about the sensitivity of their data and appear to increase the focus on privacy more generally.

It is also possible that the contextual cues guiding privacy decision making are inversely related to the objective dangers of divulgence. Thus, contextual cues can lead people to react in precisely the *wrong* way: to divulge when it is unsafe to do so and vice versa. For example, although it is more dangerous to divulge on unprofessional-looking websites (Cranor, 2002; Ivory & Hearst, 2002a, 2002b; Ivory, Sinha, & Hearst, 2001), their casual look and feel downplays privacy concerns and elicits disclosure (John, Acquisti, & Loewenstein, 2011). By contrast, recent research on the (in)effectiveness of the randomized response technique (RRT) provides empirical evidence of withholding in a context in which disclosure is relatively safe. The RRT is a method of asking sensitive questions, and although it increases objective privacy protection, its heavy-handedness can exacerbate the very concerns it is intended to assuage. The result is that people are ironically less willing to divulge using RRTs as opposed to when they are asked in a less privacy-protective manner (John, Loewenstein, Acquisti, & Vosgerau, n.d.). Similarly, heavy-handed confidentiality assurances can cause people to 'clam up' (Brandimarte, Acquisti, & Gino, n.d; Frey, 1986; John, Acquisti, & Loewenstein, 2008; Singer, Hippler, & Schwarz, 1992; Singer, von Thurn, & Miller, 1995). Assurances serve as a cue that triggers privacy concern, resulting in decreased disclosure in the face of increased protection.

Contextual cues can therefore influence privacy decision making in nonnormative ways, suggesting that people are vulnerable to making disclosures that they later stand to regret. Most notably, people can be induced to disclose in unsafe contexts and vice versa. Consistent with these findings, certain websites or programs (dubbed "foistware") offer a casual or fun service for free while surreptitiously installing tracking software, intentionally misleading users about the software's real purpose (e.g., zwinky.com).

Future research could examine how the effectiveness of dynamic retargeting depends on online context. I predict that such advertisements will be more effective when they are presented on the same website on which the product was initially viewed, as opposed to a site other than that from which it originated. Although in both cases a person's information typically passes through an infomediary, an advertising agency conducting real-time auctions for ad space, I predict that retargeted ads presented on the originator site will be perceived as contextually appropriate and hence less invasive.

Loss Aversion/Endowment

Loss aversion refers to how losses are more psychologically powerful than objectively equivalently sized gains (Kahneman & Tversky, 1979). Loss aversion gives rise to the endowment effect (Kahneman, Knetsch, & Thaler, 1990; Langer, 1975): the amount of money people are willing to accept (WTA) to sell a good is typically much higher than the amount they are willing to pay (WTP) to acquire it (according to standard economic theory, valuation should be independent from ownership).

These findings imply that privacy is valued more when a person stands to lose it than when she stands to acquire it. Acquisti, John, & Loewenstein (2013) tested this prediction in a field experiment in which shoppers were given a choice between two different gift cards: a "$12 identified card" that would link their names to their purchases for the gift card merchant to see; or a lower-valued but privacy-protective option: a "$10 anonymous card" that would *not* track their purchases. Some subjects were initially endowed with the $10 card and given the opportunity to switch easily to the $12 card. Other subjects were endowed with the $12 card and could switch to the $10 card. Thus, only the framing of the choice differed between conditions. Those initially given the $10 card faced a decision of whether they would accept $2 to *sell* their privacy by switching to the $12 card (which would track their purchases). In contrast, those initially given the $12 card decided whether they would pay $2 to *buy* privacy by switching to the $10 card (which would not track their purchases). In a third, control condition, subjects were not endowed with a card; they simply selected which of the two cards they wanted. Endowment exerted a large impact on privacy valuations: those who had been endowed with the $10, privacy-protective card were 5 times more likely to choose it relative to those who did not have privacy to begin with (i.e., those who had been endowed with the $12 card) and 1.5 times more likely to choose it relative to controls.

Broadly, loss aversion accounts for why privacy breaches generate outcry and for why privacy gains encourage apathy: breaches are akin to WTA (selling your privacy), and gains to WTP (buying privacy). Increasingly, the default privacy orientation in online contexts seems to be WTP, as new Internet technologies make information accessible by default. Perhaps more so now than ever before, privacy is something that people stand to gain rather than to lose. Consistent with this trend, people are generally unwilling to pay to

obtain privacy-preserving technologies (Brunk, 2002; Romanosky & Acquisti, 2009; Stalder, 2002), and when they are, they will pay only a tiny premium (Tsai, Engelman, Cranor, & Acquisti, 2011).

Comparative Judgments

People tend to judge stimuli and make decisions in a comparative fashion (Kahneman & Miller, 1986). For example, Prospect Theory, Kahneman and Tversky's (1979) influential theory of decision making under risk, assumes that people make decisions on the basis of changes in, rather than absolute levels of, wealth. Theories of social utility capture the insight that people care about how their outcomes compare to others': a poor person in the United States might be objectively more affluent than a middle-class person in Bangladesh, but is likely to feel subjectively poorer (John, Loewenstein, & Rick, 2014; Loewenstein, Thompson, & Bazerman, 1989). Comparative judgments are especially likely when there is no objective basis for evaluation, which is also likely the case for privacy, given the extensive preference uncertainty with which it is associated.

Comparative judgments are the basis of "coherent arbitrariness" (Ariely, Loewenstein, & Prelec, 2003), which refers to how consumers' absolute valuations of goods, services, and experiences are often remarkably arbitrary, while their relative valuations tend to be stable and orderly. In the privacy context, people displaying coherent arbitrariness would judge the sensitivity or intrusiveness of an initial personal question in an idiosyncratic, subjective, and ultimately arbitrary fashion, but would judge the sensitivity of subsequent personal questions in a coherent manner relative to that first question. This prediction also arises from the "door-in-the-face" phenomenon (Cialdini et al., 1975; Tybout, Sternthal, & Calder, 1983), whereby people confronted with extreme requests are more likely to accede subsequently to moderate requests than those who are initially confronted with more minor requests. It is also broadly consistent with people's preference for sequences that improve rather than worsen (Loewenstein & Prelec, 1993).

This prediction was supported in a series of experiments in which changing degrees of privacy intrusions were simulated by altering the order in which subjects in an online questionnaire were asked questions of varying sensitivity (Acquisti, John, & Loewenstein, 2012). Subjects judged the severity of the privacy intrusions experienced in the present by comparing them to those they had experienced in the recent past. Questions of increasing sensitivity inhibited information disclosure, as if the contrast between the early and later questions accentuates privacy concern. Similarly, consumers' willingness to part with their personal data is impacted by changes in, rather than absolute levels of, the protectiveness of privacy policies. Consumers are more likely to trust a commercial website that has recently improved its privacy policy when compared to one that has always had an objectively superior policy (Brandimarte, Acquisti, & Loewenstein, 2012).

Coherent arbitrariness implies that although people are highly attuned to changes and deviations from common reference points, they tend to adapt to ongoing situations, getting used to and ceasing to notice them (Freedman & Fraser, 1966). This adaptation process occurs rapidly and operates by creating a new reference point to which subsequent changes are compared (Frederick & Loewenstein, 1999). As a result, people with chronic health conditions report happiness levels indistinguishable from healthy counterparts, and lottery winners are not happier than less wealthy individuals (Brickman, Coates, & Janoff-Bulman, 1978; Riis et al., 2005). Applied to privacy, adaptation suggests that privacy violations are sticky – once privacy is lost, it is difficult to regain.

Adaptation in the privacy domain can account for the recurrent pattern in which initial outrage over privacy invasions fades and ultimately turns into acceptance. For example, in September 2006, Facebook launched the "News Feed" feature, a running list of Facebook activities of a user's friends. By making available salient information that had previously been obscure, "News Feed" understandably generated backlash (Denham, 2009, p. 113; Parr, 2006; Zuckerberg, 2006). Over time, however, the outrage waned and people adapted to the change (Jesdanun, 2006). In fact, "News Feed" has since become a – if not *the* – central feature of Facebook.[3]

Adaptation is also readily apparent in the many cases in which people show little concern about dramatic violations of privacy if those violations have occurred for a long time. In Pittsburgh, the sale price of houses is easily available online, accessible by the address of the property or the name of the homeowner. New homeowners in Pittsburgh are often shocked when they discover that how much they paid is public knowledge. But over time, people stop caring about the public availability of this information because they adapt to it.

Broadly, the influence of comparative judgments on privacy concern can explain the success of Facebook's apparent "door-in-the-face" strategy of introducing reductions in user privacy. In December 2009, for example, the company reduced user privacy by making profiles public and web-searchable by default. Sure enough, uproar ensued (Bankston, 2009; BBCNews, 2009; Evangelista, 2010; O'Connell, 2009; Tate, 2009). Facebook reacted by improving the privacy policy, but only *slightly*. Users generally accepted the revised policy. According to coherent arbitrariness, the revised policy was accepted because it was evaluated relative to the initial one, which was weak; hence the revised policy represented an improvement. Had the revised policy been introduced initially, I suspect that it would not have been met with approval.

3 I once asked a Facebook engineer about the experiments run on its user base. The response was that the company typically tests the effect of only subtle changes to the interface, such as font size. The engineer went on to joke that the company would not do anything "anger-inducing like turning off 'News Feed.'" It seems that "News Feed" has become so accepted that users would get upset at its removal – a total reversal of the outcry it had initially generated.

Coupled with the endowment effect, comparative judgments suggest a vicious cycle of privacy erosion, because when information is public, people value privacy less, and when people value privacy less, they are more willing to part with it.

Illusion of Control

People overestimate the extent to which they can control events, an illusion that leads them to mistakenly act as if they can control random processes (Langer, 1975). For example, in the casino game of craps, people throw the dice harder when they want high numbers than when they want low numbers, as if they can control the outcome (Henslin, 1967). The Internet gives users unprecedented control over the posting of information, while at the same time reducing other types of control, such as secondary usage (e.g., the ability to sell information to third parties, known as data brokerage, a booming industry that fuels behavioral targeting). Brandimarte, Acquisti, & Loewenstein (2012) showed that the illusion of control leads people to confound control over the publication of information with control over its usage and dissemination, creating a false sense of security when the former is high. Strikingly, granting people control over publication leads to increased divulgence when the privacy risks associated with secondary usage are elevated. In sum, consumers' failure to discriminate among these different types of control impedes their ability to manage their personal data.

These findings help account for the popularity of and (over)divulgence on SNSs, which give users great control over posting (i.e., publication). The illusion of control also explains why Facebook's "News Feed" feature initially generated outcry. Although "News Feed" only highlights information that has already been made public, it may have caused backlash because it reduced control over posting.

The illusion of control also suggests that there may be unintended consequences of the Federal Trade Commission and the Organization for Economic Cooperation and Development's premise that consumer choice (i.e., control) is critical to effective industry self-regulation of consumer privacy in general and behavioral targeting in particular (Acquisti, Adjerid, & Brandimarte, 2013; FTC, 2012; OECD, 1980). Giving consumers control over a trivial aspect of their data could cause them to mistakenly believe that they control *all* aspects of their data. For better or for worse, it seems that proponents of industry self-regulation may have already realized this. On the Network Advertising Initiative's "Consumer Opt-Out" site, a consumer is informed of the advertising companies "customizing ads for your browser" (when I checked, I was being behaviorally targeted by 99 of 116 "participating companies").[4] The consumer can then select which companies to opt out of. Endorsing 99 opt-out checkboxes

4 www.networkadvertising.org/choices/.

made me feel in control, but as the fine print indicates, doing so prevents me from receiving targeted advertisements, *not* from being tracked. Ironically, opting out makes it harder for me to understand who is collecting my data and how they are using it: by having opted out of behavioral targeting, I no longer receive tailored ads, the residue of the fact that I am being tracked. Arguably, most people visit this opt-out site not because they dislike advertising that is relevant to them, but because they do not want their online activities recorded by third parties. If I am going to be tracked and if ads are unavoidable, I would like to at least have the benefit of receiving relevant ads.

Future research could look at how this illusion of control affects observers' impressions of disclosers. Consumers may confound control over *disclosing* an outcome with control over the outcome itself, causing them to "shoot the messenger." Suppose, for example, that a firm was forced to raise prices due to a factor out of its control (e.g., an increase in transportation costs). An illusion of control account might predict that consumers confound control over disclosing price increases with control over the price itself, in turn creating unwarrantedly negative impressions of the firm (i.e., more negative than those warranted by the price increase itself).

Norms

People's behavior conforms to that of others, a phenomenon documented in both the economics (Devenow & Welch, 1996) and psychology literatures (Asch, 1956). The importance of others' behavior is closely linked to research on social norms (Bicchieri, 2006), which amply demonstrates that people care about social norms and often infer those norms, at least in part, by observing others' behavior. Theories of social norms predict that people adapt their behaviors to conform to the behaviors of those around them, which also appears to be the case on the Internet, where people "move quickly, like a swarm of killer bees. They often behave in a mob-like fashion" (Solove, 2007, p. 101).

The influence of social norms on disclosure was illustrated in an experiment in which people were provided with simulated information on the societal acceptance of privacy invasions (Acquisti, John, & Loewenstein, 2012). The ostensible distribution of answers that others had provided to a number of highly intrusive questions was manipulated between-subjects. Subjects were more likely to admit to having engaged in sensitive, and in some cases illegal, behaviors when they were given information that led them to believe that others had engaged in those behaviors before them.

Herding phenomena help to explain over-divulgence on SNSs. Facebook, for example, facilitates herding by heightening the salience of others' disclosures. Upon logging in, the user immediately sees "News Feed." Only a small proportion of a user's network may have made recent disclosures, but Facebook's "News Feed" selectively highlights these episodes. "News Feed" therefore creates a norm of divulgence.

What happens when a person's online behavior violates established norms? People dislike norm violation and are willing to pay for norm enforcement (Fehr & Gaechter, 2002). Online, the costs of norm enforcement are reduced, which helps to explain the popularity of digital shaming – the malicious outing of norm violators (Solove, 2007). There are many websites devoted to this purpose; for example, on Bitterwaitress.com, waiters enter the names, locations, and descriptions of stingy customers into the "Shitty Tipper Database." Similarly, on dontdatehimgirl.com, women reveal the identities of philanderers. It is awkward to speak out against a norm violator in person; as these sites attest, it is easy to complain silently and anonymously online.

Traditional forms of communication (e.g., face-to-face, telephone, written letters) have strong social norms associated with them, which people are generally adept at following (Grice, 1975). People seamlessly match the tone and content of others' disclosures (Sedikides, Campbell, Reeder, & Elliot, 1999) and nonverbal behavior (van Baaren, Horgan, Chartrand, & Dijkmans, 2004); norm deviations are salient and eligible for social sanctions (Fehr & Gaechter, 2002). Thus, a natural starting point for consumers in navigating issues of privacy and disclosure in foreign, online contexts is to apply these well-established norms (Nissenbaum, 2004). But the problem is that "digital environments [. . .] confound the traditional ways in which we control our audiences and negotiate the boundary between the private and the public, the past and the future, disclosure and privacy" (Tufecki, 2008, p. 20). For example, the Internet makes information dissemination – through email, texts, blogs, or tweets – fast and easy. But at the same time, it has heightened the permanence of disclosures. Impulsive disclosures are forever catalogued in cyberspace (and, in the case of tweets, also in the Library of Congress! Lohr, 2010). Indeed, "what was once ephemeral, with evidence of it living only in the memory of the current witness – a conversation in a café, a cash purchase in a store, a nod toward an acquaintance while walking down the street – is increasingly enacted online, where it leaves a potentially lasting footprint" (Tufecki, 2008, p. 21).

What are the consumer privacy implications of this new permanence? For one, it can leave consumers vulnerable to making disclosures that they later stand to regret. Although it is sometimes possible to remove the information source (e.g., deleting a tweet), it is impossible to expunge its every trace. Moreover, the very content that people are most likely to regret (e.g., seductive photos posted when intoxicated) is often disproportionately likely to "go viral." Indeed, some have warned that the permanence of online disclosure means the "end of forgetting" (Rosen, 2010) or the "end of privacy" (Angwin, 2014; Nussbaum, 2007; Tanner, 2014). Today's youth are amassing digital "skeletons in the closet" that could haunt them in adulthood (Mayer-Schoenberger, 2011; Nussbaum, 2007). Political candidates are already subject to intense scrutiny; imagine the kind of scrutiny that could arise if digital records of their entire lives were available. Other commentators are less concerned about permanence, arguing that the sheer volume of publicly available information will make it possible to "hide in plain sight" (Mallon, 2014). But recent research suggests

that concern is warranted. Disclosures of immoral acts have enduring (negative) impacts on impression formation, whereas observers quickly discount disclosures of moral acts (Brandimarte, Vosgerau, & Acquisti, n.d.). The long-term effects of online disclosure offer an important topic for future research.

The (mis)application of norms associated with traditional communication to digital environments has implications for behavioral targeting. Surveillance enables behavioral targeting and is conducted by two different technologies: web bugs and cookies. Both technologies track and record consumers' clickstreams, but they may not be perceived as equally invasive. Whereas web bugs are embedded into web pages (and hence do not reside on one's computer), cookies are downloaded and housed on one's hard drive. If informed of this difference, consumers are apt to feel less comfortable with cookies than web bugs.[5] Because cookies are stored on one's own computer, they represent a violation of physical space and hence are likely to be deemed invasive.

Similarly, consumers' acceptance of surveillance might depend on the entity through which it is conducted. In traditional face-to-face communication, people are typically willing to share personal information only with those they trust (i.e., not strangers). Stemming from this fact, people disclose more when they communicate online as opposed to face to face (Tourangeau & Yan, 2007; Whitty & Joinson, 2009). Surveillance technologies operated by humans are therefore likely to be perceived as more invasive relative to those operated by machines or robots, even when both technologies collect the same information. Airport full-body scanners generate images that are monitored by humans; perhaps it is not a coincidence that they are loathed (Cooper, 2010). Many email clients such as Gmail present users with target advertisements based on the content of their emails. Interestingly, Google downplays the role of humans in describing how the ads are generated: "All targeting in Gmail is fully automated, and no humans read your email or Google Account information in order to show you advertisements or related information" (https://support.google.com/mail/answer/6603).

I recently conducted a simple experiment to test this notion – that surveillance is deemed relatively noninvasive if perceived to be conducted by inanimate agents. Subjects (N = 174) read a brief description of how email clients generate targeted advertisements. Half were told: "engineers have written computer programs that read through your email so that they can show you advertisements that you will find relevant" (animate condition); the others were told: "computer programs scan your email to automatically generate advertisements that you will find relevant" (inanimate condition). As predicted, the practice was deemed more intrusive in the animate condition ($M_{animate}$ = 7.2 out of 9, SD = 1.98) relative to the inanimate condition ($M_{inanimate}$ = 6.3 SD = 2.4; $t(172) = 3.14$, $p < .01$).

5 However, the names of these technologies may be a countervailing force in terms of consumer acceptance: A "cookie" sounds innocuous; a "web bug" sounds invasive.

In sum, traditional communication norms suggest that consumers' acceptance of new surveillance technologies depends on the manner in which it is conducted. Surveillance technologies that are objectively equally intrusive (in that they collect the same information) may not necessarily be perceived as such.

Isolation Errors/Myopia

Now perhaps more than ever before, people are bombarded with frequent requests for information. However, each request is often for only a small piece of information – a phone number here, a log-in ID there. Small but frequent requests for personal information give rise to isolation errors – the failure to appreciate the broader impact of one's choices, also referred to as "myopia" (Herrnstein & Prelec, 1991; Kahneman & Lovallo, 1999; Read, Loewenstein, & Rabin, 1999). They are also likely to place the discloser in "low-level construal mode," known to lead individuals to downplay abstract, big-picture goals such as the desire for privacy (Liberman & Trope, 2003).

Consistent with these tendencies, when they are online people only narrowly consider the consequences of divulgence, leading to an underappreciation of the emergent properties of information sharing, namely that separate, seemingly innocuous facts can be aggregated to reveal new information. For example, social security numbers can be predicted by combining a person's date and place of birth (both commonly divulged on Facebook) with an algorithm of the pattern by which SSNs are generated (Acquisti & Gross, 2009); medical records can be tracked down simply by knowing a person's birth date and zip code (Tanner, 2014). And as noted earlier in the case of Target, personal information can be inferred by aggregating information on shopping habits. Moreover, the new permanence of (online) disclosure means that a person's digital footprint grows over time. In part because of myopia, people are often surprised to learn how much of their personal information can be found online (Duhigg, 2012).[6] Similarly, people often fail to appreciate that such information can later be used for purposes other than those initially intended. Potential employers find "dirt" on applicants by "Googling" them; much of what is found has been disclosed by the applicants themselves (Clark, 2006; Grasz, 2009).

Future research could test whether isolation errors affect people's willingness to share personal information. For example, online, people tend to act as if they are divulging to a narrow audience, which can result in embarrassment or worse. Facebook is rife with examples of sensitive disclosures clearly intended for a small audience, but visible to the discloser's entire network. One woman

6 Axciom, the consumer-data aggregator giant, is now letting people read the information it has on them. But ironically, to obtain your report, you have to provide the company with more personal data (your name, address, email address, and last four digits of your social security number). One commentator noted that this is like "the Transportation Security Administration offering to show you the naked photos it takes at the airport—as long as you first agree to pose for some more photos" (Lewis, 2013).

posted inflammatory comments about her boss, whom she forgot was part of her network. She was fired as a result (Moult, 2009). Facebook seems by design to foster a narrow consideration of audience, creating an illusion of intimacy: when a user posts information, his friend list is hidden from view. At the moment of divulgence, the user's broader network is out of sight and out of mind. The result: people behave as if they are sending letters, when instead they are sending postcards.

Present-Biased Preferences

Present-biased preferences refer to the tendency to overweight immediate costs and benefits and to take a much more evenhanded approach to delayed costs and benefits (Frederick, O'Donoghue, & Loewenstein, 2002; Laibson, 1997; Loewenstein & Elster, 1992; O'Donoghue & Rabin, 1999). Present-biased preferences give rise to a variety of self-control issues that are readily apparent in the privacy domain (Acquisti, 2004).

The overweighting of immediate benefits leads to pre-operation – people are proactive in realizing the immediate benefits of information revelation (Rabin & O'Donoghue, 2000). Pre-operation explains why people are willing to divulge sensitive information in exchange for very small, but immediate, rewards (Chellappa & Sin, 2002; Hann, Hui, Lee, & Png, 2002b; Spiekermann, Grossklags, & Berendt, 2001). For example, 71 percent of people revealed their computer password for a meager chocolate bar (BBC News, 2004), and 85 percent provided information to shopping websites for a chance at a small prize (Jupiter-Research, 2002).

The overweighting of immediate costs leads to procrastination – people postpone taking actions to protect their privacy (O'Donoghue & Rabin, 2001). Unlike in offline contexts, where implementing privacy-preserving measures can be as simple as drawing the blinds or lowering one's voice, doing so online often requires mastering complicated new technologies (Whitten & Tygar, 2005), a costly activity that lends itself to perpetual deferral. At the same time, by making it easy to divulge, online contexts reduce the procrastination to share. This helps to explain why information spreads so readily over the Internet. Whereas online it is possible to forward a message to hundreds with the simple click of a mouse, offline it would require considerable effort to distribute the message physically by mail.

Several unique characteristics of online divulgence exacerbate the pernicious effects of present-biased preferences. First, the costs of online divulgence are often delayed; negative consequences – such as receiving spam email or, in the extreme, falling victim to identity theft – typically do not occur immediately after the disclosure episode but instead after considerable time has elapsed. Present-biased preferences lead individuals to favor the immediate gratification of divulgence despite its negative consequences because the latter are usually delayed and hence easily "written off." Unfortunately, however, when the future comes, people sometimes find themselves regretting their earlier

disclosures. Secondly, the influence of present-biased preferences is heightened by the murky relationship between disclosure and its consequences. Disclosure is immediately rewarding psychologically, and often also economically, as when a consumer provides personal data in exchange for a discount. By contrast, the undesirable consequences of information sharing, such as identity theft, are difficult to attribute to a single disclosure episode. Both the coupling of disclosure to its benefits and the decoupling from its harms tend to aggravate the effects of present-biased preferences.

Together, these characteristics can account for consumers' great unwillingness to pay for privacy enhancing technologies. Whether it be time (in the case of privacy-enhancing web browsers such as DuckDuckGo, Tor, and PrivacyBird) or money (Tsai et al., 2011), the costs of adopting these technologies are immediate, and the benefits are delayed and amorphous.

Projection Bias

Projection bias refers to the misguided belief that future tastes will resemble current ones (Loewenstein, O'Donoghue, & Rabin, 2000). This bias suggests that people fail to appreciate that their valuation of privacy is likely to change over time and is readily apparent in the behavior of college students who post sensitive personal information only to regret it later, such as when seeking employment (Clark, 2006; Grasz, 2009) or when their parents join Facebook (myparentsjoinedFacebook.com). Projection bias, along with the heightened permanence of online information sharing, implies a systematic predisposition to overdisclose. A decision *not* to disclose is reversible, while the same cannot be said for a decision to disclose.

Overoptimism

People are generally overly optimistic about their likelihood of engaging in positive behaviors, such as donating to charity, exercising, or losing weight (Armor & Taylor, 2002; DellaVigna & Malmendier, 2006; Epley & Dunning, 2000; Weinstein, 1980). Applied to privacy, overoptimism suggests that people are likely to believe erroneously that they are invulnerable to privacy violations, which helps to explain why they fail to take privacy-protective actions. Consistent with this conjecture, 56 percent of respondents in a large survey were overly optimistic about their likelihood of avoiding identity theft (Romanosky, Sharp, & Acquisti, 2010).

Summary of Part 2

BDT principles account for the seemingly illogical decisions consumers make with respect to their online privacy. Privacy decision making is easily influenced by nonnormative factors, suggesting that people are vulnerable to making disclosure decisions that they later stand to regret.

Part 3: Broad Topics for Future Research

In Parts 1 and 2, I discussed how BDT principles can account for the privacy paradox and, more broadly, for the seemingly self-destructive choices consumers make with respect to the management of their personal data. Throughout, I have also highlighted opportunities for future research to further understand how consumers navigate the new complexities of information sharing in the digital age. In particular, I have identified areas for future research on digital advertising, a key marketing function that is affected by the shift toward openness. But BDT still has much to contribute. To conclude, I outline several other broad topics for future research.

A natural next step after having gained an understanding of consumers' online behavior with respect to their privacy is to develop ways to deal with personal information that are beneficial to firms and consumers alike. Several privacy advocates have recently proposed information provision as a means of helping people to make disclosure decisions that are in their best interest. Grimmelmann (2009, p. 1205), for example, argues that "teens and college students would be better off with a better understanding of the ways that persistent postings can return to haunt them." Similarly, one of the central tenets of the Federal Trade Commission's (2012) guidelines for consumer protection is information provision. These approaches imply that as long as people are aware of the costs and benefits of their online activities, they will be able to manage their personal data in a self-interested way. However, this approach is likely to be severely limited because biases in decision making tend to persist even when individuals are fully aware of their influence (Fischhoff, 1982; O'Donoghue & Rabin, 1999). On the other hand, recent research has shown that BDT principles can help people make better decisions (Loewenstein, John, & Volpp, 2013; Thaler & Benartzi, 2004; Volpp et al., 2008). In the following subsections, I outline two possible approaches to help people align their disclosure decisions with their own interests. These and similar ideas could be developed in future work.

Cue Realignment

Aligning contextual cues with the dangers of disclosure may improve privacy decision making. For example, privacy-preserving software could display behaviorally informed stimuli, such as a set of watchful eyes to signal dangerous websites. The feeling of being watched makes people self-conscious (Duval & Wicklund, 1972, p. 121) and could thus curb disclosure. Legal scholar Ryan Calo aptly notes that anthropomorphic design, "a form of 'visceral notice' – in the sense that the technique directly conveys the reality that user information is being collected, used, and often shared – could help shore up a failing regime of textual notice visceral notice that lines up our experience with actual information practice" (Calo, 2010, p. 848).

Cooling-Off Periods

Much as mandatory waiting periods for obtaining handguns are designed to prevent violence, cooling off periods may help people to avoid making disclosure decisions that they later stand to regret. On his blog, Thaler has written about the (currently fictional) "Civility Check" software "designed to prevent our hot-headed selves from causing unnecessary email disasters" (Thaler, 2009). Upon detecting inflammatory language (with the help of actual software like Tone Check; Wawro, 2008), the program could direct offending email to a temporary folder – a type of email purgatory. The email would be sent only upon confirmation by the user after several hours have passed, when he or she has presumably calmed down. Since this blog entry was written, a phone app called Drunk Text Savior has emerged, which scans text messages for cues of inebriation before they are sent. If detected, the program displays: "WARNING! You May Be Drunk! You have some warning signs in your text. Possibly too many drinks. Are you sure you want to send this text?"

Conflicting motivations are likely to pose a key barrier to implementing these types of interventions. Many online companies have strong interests in making information open and easily accessible and therefore are not motivated to increase consumers' privacy protection unless consumers demand it or it is required by law. Given our apathetic, often conflicting, attitudes toward privacy, it is unlikely that consumer demand for privacy protection will force companies to instate it. Government intervention may be necessary to regulate and protect consumers' privacy in the face of these forces. Yet there is still much to understand with respect to consumer behavior and online privacy, far beyond what can be understood through a BDT lens alone. To conclude, I highlight broad topics that are ripe for collaboration across different sub-disciplines within marketing and beyond.

Economic Benefits versus Consumer Satisfaction

Future research is needed to understand how marketers balance the economic benefits of obtaining and using consumers' personal data against consumers' often seemingly irrational responses. Understanding such trade-offs is integral to the success of a host of marketing functions, including pricing. The new availability of consumer data enables ever-finer price discrimination. The ride-sharing service Uber, for example, frequently implements surge pricing whereby the customer is informed that prices have increased due to high demand and is offered a new price (a multiple of the standard price). I have often wondered whether Uber uses my history of accepting or rejecting offers of various multiples to customize my prices. Even information that we leak through our online behavior could be rich pricing inputs for firms. For example, if you conduct several web searches for a specific flight, you may be signaling to the airline that you are eager to buy and hence willing to pay a premium. Although from a standard economics perspective price discrimination is beneficial both

to firms (because it enables the highest rents to be extracted) and consumers (because it puts products into the hands of the people who value them most), the psychology of the matter is that it is perceived as unfair (Kahneman, Knetsch, & Thaler, 1986). How to balance the huge marketing opportunities of personal data against the desire to maximize customer satisfaction is an important topic for future research.

Interaction with Other Consumer Psychological Insights

This chapter has treated BDT principles as main effects, but there is still much to understand about how they interact with other psychological factors to explain consumers' online behavior with respect to their privacy. For example, common biases operate differently under the influence of different emotions (Lerner, Kassam, Li, & Valdesolo, 2015). Now more than ever before, through video and multimedia applications, the Internet is equipped to spark emotional reactions. This example points to the need to integrate the BDT perspective with other insights from psychology to form a unified framework for understanding consumer privacy. Such a framework would be helpful in understanding and predicting the impact of new Internet technologies that have yet to emerge in the constantly evolving online world.

Acknowledgments

I thank David John, Cait Lamberton, George Loewenstein, Michael Norton, and Evan Robinson for helpful comments on earlier versions of this chapter.

References

Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. Paper presented at the Proceedings of the ACM Conference on Electronic Commerce (EC'04).

Acquisti, Adjerid, & Brandimarte, L. (2013). Gone in 60 seconds: The limits of privacy, transparency, and control. *IEEE*, *13*, 72–74.

Acquisti, A., & Gross, R. (2009). Predicting social security numbers from public data. *Proceedings of the National Academy of Sciences*, *106*(27), 10975–10980.

Acquisti, A., John, L. K., & Loewenstein, G. (2012). The impact of relative standards on the propensity to disclose. *Journal of Marketing Research, April*, 160–174.

Acquisti, A., John, L. K., & Loewenstein, G. (2013). What is privacy worth? *Journal of Legal Studies*, *42*(2), 249–274.

Acquisti, A., & Varian, H. (2002). Conditioning prices on purchase history. *Marketing Science*, *24*(3), 367–381.

Adjerid, I., Acquisti, A., Brandimarte, L., & Loewenstein, G. (2013). Sleights of Privacy: Framing, disclosures, and the limits of transparency. In *Proceedings of the*

Ninth Symposium on Usable Privacy and Security, 9. New York: Association for Computing Machinery.

Alter, A. L., & Oppenheimer, D. M. (2009). Suppressing secrecy through metacognitive ease: Cognitive fluency encourages self-disclosure. *Psychological Science, 20* (11), 1414–1420.

Altman, I. (1975). *The Environment and Social Behavior.* Monterey, CA: Brooks/Cole.

Angwin, J. (2014). *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance.* New York: Henry Holt, Times Books.

Ariely, D., Loewenstein, G., & Prelec, D. (2003). Coherent arbitrariness: Stable demand curves without stable preferences. *Quarterly Journal of Economics, 118*, 73–106.

Armor, D. A., & Taylor, C. R. (2002). When predictions fail: The dilemma of unrealistic optimism. In T. Gilovich, D. Griffin, & D. Kahneman (eds.), *Heuristics and Biases: The Psychology of Intuitive Judgment.* Cambridge: Cambridge University Press.

Asch, S. E. (1956). Studies of independence and conformity: A minority of one against a unanimous majority. *Psychological Monographs, 70*(9), 118.

Asch, S. E. (1959). A perspective on social psychology. In S. Koch (ed.), *Psychology: A Study of Science* (vol. 3, pp. 363–383). New York: McGraw-Hill.

Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly, 30*(1), 18–28.

Bankston, K. (2009). Facebook's new privacy changes: The good, the bad, and the ugly. Retrieved from www.eff.org/deeplinks/2009/12/Facebooks-new-privacy-changes-good-bad-and-ugly.

BBCNews (2004). Passwords revealed by sweet deal. Retrieved from http://news.bbc.co.uk/2/hi/technology/3639679.stm.

BBCNews (2009). Facebook faces criticism on privacy change. Retrieved from http://news.bbc.co.uk/2/hi/technology/8405334.stm.

Berscheid, E. (1977). Privacy: A hidden variable in experimental social psychology. *Journal of Social Issues, 33*(3), 85–101.

Bicchieri, C. (2006). *The Grammar of Society: The Nature and Dynamics of Social Norms.* Cambridge: Cambridge University Press.

Brandimarte, L., Acquisti, A., & Gino, F. (n.d.). Baring out with iron hands: Can disclosing make us harsher? Working Paper.

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2012). Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science* (August), 340–347.

Brandimarte, L., Vosgerau, J., & Acquisti, A. (n.d.). Neither forgiven nor forgotten – moral acts depreciate over time, immoral acts do not. Working Paper.

Brickman, P., Coates, D., & Janoff-Bulman, R. (1978). Lottery winners and accident victims: Is happiness relative? *Journal of Personality and Social Psychology, 36*(8), 917–927.

Brunk, B. D. (2002). Understanding the privacy space. *First Monday*, 7.

Calo, R. (2010). People can be so fake: A new dimension to privacy and technology scholarship. *Penn State Law Review, 114*(3), 809–855.

Chellappa, R., & Sin, R. (2002). *Personalization versus Privacy: New Exchange Relationships on the Web*. Los Angeles: Marshall School of Business, University of Southern California.

Cialdini, R. B., Vincent, J. E., Lewis, S. K., Catalan, J., Wheeler, D., & Darby, B. L. (1975). Reciprocal concessions procedure for inducing compliance: The door-in the face technique. *Journal of Personality and Social Psychology*, *31*, 206–215.

Clark, A. S. (2006). Employers look at Facebook, too: Companies turn to online profiles to see what applicants are really like. Retrieved from www.cbsnews.com/stories/2006/06/20/eveningnews/main1734920.shtml.

Collins, N. L., & Miller, L. C. (1994). Self-disclosure and liking: A meta-analytic review. *Psychological Bulletin*, *116*(3), 457–475.

ConsumersUnion.org. (2008). Americans extremely concerned about Internet privacy. Retrieved from www.consumersunion.org/pub/core_telecom_and_utilities/006189.html.

Conway, L. (2008). Virgin Atlantic sacks 13 staff for calling its flyers "chavs." *The Independent*, November 1. Retrieved from www.independent.co.uk/news/uk/home-news/virgin-atlantic-sacks-13-staff-for-calling-its-flyers-chavs-982192.html.

Cooper, H. (2010). Administration to seek balance in airport screening. Retrieved from www.nytimes.com/2010/11/23/us/23tsa.html.

Cozby, P. C. (1972). Self-disclosure, reciprocity, and liking. *Sociometry*, *35*(1), 151–160.

Cranor, L. (2002). Web Privacy with P3P. Sebastopol, CA: O'Reilly & Associates.

Cryder, C. E., Loewenstein, G., & Scheines, R. The donor is in the details. *Organizational Behavior and Human Decision Processes*, *120*(1), 15–23.

Culnan, M. J., Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, *10*(1), 104–115.

DellaVigna, S., & Malmendier, U. (2006). Paying not to go to the gym. *American Economic Review*, *96*(3), 694–719.

Denham, E. (2009). *Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. under the Personal Information Protection and Electronic Documents Act*. Ottawa: Privacy Commissioner of Canada.

Devenow, A., & Welch, I. (1996). Rational herding in financial economics. *European Economic Review*, *40*, 603–615.

Duhigg, C. (2012). How companies learn your secrets. *New York Times Magazine*, February 16. Retrieved from www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

Duval, S., & Wicklund, R. A. (1972). *A Theory of Objective Self-Awareness*. New York: Academic Press.

Epley, N., & Dunning, D. (2000). Feeling "holier than thou": Are self-serving assessments produced by errors in self- or social prediction? *Journal of Personality and Social Psychology*, *79*(6), 861–875.

Evangelista, B. (2010). Canada's privacy commissioner launches new Facebook probe. sfgate. Retrieved from www.sfgate.com/cgi-bin/blogs/techchron/detail?entry_id=56175.

Federal Trade Commission (2000). *Privacy Online: Fair Information Practices in the Electronic Marketplace*. Washington, DC: Federal Trade Commission.

Federal Trade Commission (2006). *The Identity Theft Report*. Washington, DC: Federal Trade Commission.

Federal Trade Commission (2012). *Protecting Consumer Privacy in an Era of Rapid Change*. Retrieved from ftc.gov/os/2012/03/120326privacy report.pdf.

Fehr, E., & Gaechter, S. (2002). Altruistic punishment in humans. *Nature*, *415*, 137–140.

Fischhoff, B. (1982). Debiasing. In D. Kahneman, P. Slovic & A. Tversky (eds.), *Judgment under Uncertainty: Heuristics and Biases* (pp. 422–444). Cambridge: Cambridge University Press.

Fox, C. R., & Tversky, A. (1995). Ambiguity aversion and comparative ignorance. *Quarterly Journal of Economics*, *110*(3), 585–603.

Frederick, S., & Loewenstein, G. (1999). Hedonic adaptation. In D. Kahneman & E. Diener (eds.), *Well-being: The Foundations of Hedonic Psychology* (pp. 302–329). New York: Russell Sage Foundation.

Frederick, S., O'Donoghue, T., & Loewenstein, G. (2002). Time discounting and time preference: A critical review. *Journal of Economic Literature*, *40*(2), 351.

Freedman, Jonathan L., & Fraser, Scott C. (1966). Compliance without pressure: The foot-in the door technique. *Journal of Personality and Social Psychology*, *4*(2), 195–202.

Frey, J. H. (1986). An experiment with a confidentiality reminder in a telephone survey. *Public Opinion Quarterly*, *50*, 267–269.

Gilbert, F. (2008). Beacons, bugs, and pixel tags: Do you comply with the FTC behavioral marketing principles and foreign law requirements? *Journal of Internet Law*, *11*(11), 3–10.

Goldfarb, A., & Tucker, C. (2011a). Shifts in privacy concerns. Available at SSRN: http://ssrn.com/abstract=1976321 or http://dx.doi.org/10.2139/ssrn.1976321.

Goldfarb, A., & Tucker, C. (2011b). Privacy regulation and online advertising. *Management Science*, *57*(1), 57–71.

Goldfarb, A., & Tucker, C. (2011c). Online display advertising: Targeting and obtrusiveness. *Marketing Science*, *30*, 389–404.

Grasz, J. (2009). 45% employers use Facebook-Twitter to screen job candidates. *Oregon Business Report* (August). Retrieved from http://oregonbusinessreport.com/2009/08/45-employers-use-Facebook-twitter-to-screen-job-candidates/.

Grice, Paul (1975). Logic and conversation. In P. Cole & J. Morgan (eds.), *Syntax and Semantics* (vol. 3: Speech Acts, pp. 41–58). New York: Academic Press.

Grimmelmann, J. (2009). Saving Facebook. *Iowa Law Review*, *94*, 1137–1206.

Hann, I.-H., Hui, K.-L., Lee, T. S., & Png, I. P. L. (2002a). The value of online privacy: Evidence from the USA and Singapore. Paper presented at the Twenty-Third International Conference on Information Systems, Barcelona.

Hann, I.-H., Hui, K.-L., Lee, T. S., & Png, I. P. L. (2002b). Online information privacy: Measuring the cost-benefit trade-off. Paper presented at the Twenty-Third International Conference on Information Systems, Barcelona.

Henslin, J. M. (1967). Craps and magic. *American Journal of Sociology*, *73*(3), 316–330.

Herrnstein, R. J., & Prelec, D. (1991). Melioration: A theory of distributed choice. *Journal of Economic Perspectives*, *5*(3), 137–156.

Hill, K. (2012). How Target figured out a teen girl was pregnant before her father did. Forbes.com, February 16. Retrieved from www.forbes.com/sites/kashmirhill/2012/02/16/howtarget-figured-out-a-teen-girl-was-pregnant-before-her-father-did/.

Hsee, C., Loewenstein, G., Blount, S., & Bazerman, M. (1999). Preference reversals between joint and separate evaluations: A review and theoretical analysis. *Psychological Bulletin*, *125*(5), 576–590.

Ivory, M. Y., & Hearst, M. A. (2002a). Improving web site design. *IEEE Internet Computing*, *6*(2, Special Issue on Usability and the Web), 56–63.

Ivory, M. Y., & Hearst, M. A. (2002b). Statistical profiles of highly rated web sites. Paper presented at the Conference on Human Factors in Computing Systems, Minneapolis.

Ivory, M. Y., Sinha, R. R., & Hearst, M. A. (2001). Empirically validated web page design metrics. Paper presented at the Conference on Human Factors in Computing Systems, Seattle.

Jenni, K. E., & Loewenstein, G. (1997). Explaining the "identifiable victim effect." *Journal of Risk and Uncertainty*, *14*, 235–257.

Jesdanun, A. (2006). Facebook offers new privacy options. Associated Press.

John, L. K., Acquisti, A., & Loewenstein, G. (2008). Inconsistent preferences for privacy. Paper presented at Behavioral Decision Research in Management Conference, Rady School of Management, University of California, San Diego.

John, L. K., Acquisti, A., & Loewenstein, G. (2011). Strangers on a plane: Context-dependent willingness to divulge sensitive information, *Journal of Consumer Research*, *37*, 858–873.

John, L. K., Loewenstein, G., Acquisti, A., & Vosgerau, J. (n.d.). The Psychology of randomized response techniques and why they backfire. Working Paper.

John, L. K., Loewenstein, G., & Rick, S. (2014). Cheating more for less: Upward social comparisons motivate the poorly compensated to cheat. *Organizational Behavior and Human Decision Processes*, *123*, 101–109.

Jourard, S. N. (1959). Self-disclosure and other-cathexis. *Journal of Abnormal and Social Psychology*, *59*, 428–431.

Jourard, S. N. (1966). Some psychological aspects of privacy. *Law and Contemporary Problems*, *31*(2), 307–318.

Jupiter Research. (2002). Seventy percent of US consumers worry about online privacy, but few take protective action. Retrieved from www.prnewswire.com/news-releases/70-of-us-consumers-worry-about-online-privacy-but-few-take-protective-action-reports-jupiter-media-metrix-77697202.html.

Kahneman, D., Knetsch, J., & Thaler, R. (1986). Fairness as a constraint on profit seeking: Entitlements in the market. *American Economic Review*, *76*(4), 728–741.

Kahneman, D., Knetsch, J., & Thaler, R. (1990). Experimental test of the endowment effect and the Coase Theorem. *Journal of Political Economy*, *98*(6), 1325–1348.

Kahneman, D., & Lovallo, D. (1999). Timid choices and bold forecasts: A cognitive perspective on risk taking. *Management Science*, *39*(1), 17–31.

Kahneman, D., & Miller, D. T. (1986). Norm theory: Comparing reality to its alternatives. *Psychological Review*, *93*, 136–153.

Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision making under risk. *Econometrica*, *47*, 263–291.

Laibson, D. (1997). Golden eggs and hyperbolic discounting. *Quarterly Journal of Economics*, *112*(2), 443–478.

Lambrecht, A., & Tucker, C. (2013). When does retargeting work? Information specificity in online advertising. *Journal of Marketing Research*, *50*(5), 561–576.

Langer, E. (1975). The illusion of control. *Journal of Personality and Social Psychology*, *32*(2), 328.

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues*, *33*(3), 22–24.

Lerner, J. S., Kassam, K., Li, Y., & Valdesolo, P. (2015). Emotion and decision making. *Annual Review of Psychology*, *66*, 799–823.

Lewis, A. (2003). Please, tell us more. *Wall Street Journal*. Retrieved from www.wsj.com/articles/SB10001424127887324123004579057350800192892.

Liberman, N., & Trope, Y. (2003). Temporal construal theory of intertemporal judgment and decision. In G. Loewenstein, D. Read, & R. Baumeister (eds.), *Time and Choice: Economic and Psychological Perspectives on Intertemporal Choice*. New York: Sage.

Lichtenstein, S., & Slovic, P. (2006). *The Construction of Preference*. New York: Cambridge University Press.

Loewenstein, G., & Elster, J. (eds.). (1992). *Choice over Time*. New York: Russell Sage Foundation.

Loewenstein, G., John, L. K., & Volpp, K. (2013). Protecting people from themselves: Using decision errors to help people help themselves (and others). In E. Shafir (ed.), *The Behavioral Foundations of Public Policy* (pp. 361–379). Princeton, NJ, and Oxford: Princeton University Press.

Loewenstein, G., & O'Donoghue, T. (2005). *Animal Spirits: Affective and Deliberative Processes in Economic Behavior*. Pittsburgh, PA: Carnegie Mellon University.

Loewenstein, G., O'Donoghue, T., & Rabin, M. (2003). Projection bias in predicting future utility. *Quarterly Journal of Economics*, *118*(4), 1209–1248.

Loewenstein, G., & Prelec, D. (1993). Preferences for sequences of outcomes. *Psychological Review*, *100*(1), 91–108.

Loewenstein, G., Thompson, L., & Bazerman, M. H. (1989). Social utility and decision making in interpersonal contexts. *Journal of Personality and Social Psychology*, *57*, 426–441.

Lohr, S. (2010). Library of Congress will save tweets. *New York Times*, April 15, B2.

Mallon, H. W. (2014). Hiding in plain sight: Privacy on the Internet. Retrieved from http://helenwmallon.com/hiding-in-plain-sight-privacy-on-the-internet/.

Margulis, S. T. (2003). On the status and contribution of Westin's and Altman's theories of privacy. *Journal of Social Issues*, *59*(2), 411–429.

Marthews, Alex, & Tucker, Catherine. (2014). Government surveillance and Internet search behavior. Available at SSRN: http://ssrn.com/abstract=2412564.

Mayer-Schoenberger, V. (2011). *Delete: The Virtue of Forgetting in the Digital Age*. Princeton, NJ: Princeton University Press.

McDonald, A. D., & Cranor, L. F. (2008). The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society*, *4*(22), 543–568.

Mikulincer, M., & Nachson, O. (1991). Attachment styles and patterns of self-disclosure. *Journal of Personality and Social Psychology*, *61*(2), 321–331.

Moult, J. (2009). Woman "sacked" on Facebook for complaining about her boss after forgetting she had added him as a friend. Mail Online, August 14. Retrieved from www.dailymail.co.uk/news/article-1206491/Woman-sacked-Facebook-boss-insult-forgetting-added-friend.html.

Nisbett, R. E., & Ross, L. (1980). *Human Inference: Strategies and Shortcomings of Social Judgment*. New Jersey: Prentice Hall.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, *79*(1), 119–157.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, *41*(1), 100–126.

Nussbaum, Emily (2007). Say everything. *New York Magazine*, February 12. Retrieved from http://nymag.com/news/features/27341/.

O'Connell, H. (2009). What does Facebook's privacy transition mean for you? Retrieved from http://dotrights.org/what-does-Facebooks-privacy-transition-mean-you.

O'Donoghue, T., & Rabin, M. (1999). Doing it now or later. *American Economic Review*, *89*(1), 103–124.

O'Donoghue, T., & Rabin, M. (2001). Choice and Procrastination. *Quarterly Journal of Economics*, *116*(1), 121–160.

Organization for Economic Cooperation and Development (1980). OECD guidelines on the protection of privacy and transborder flows of personal data, 23. Retrieved from www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyand transborderflowsofpersonaldata.htm#memorandum.

Parr, B. (2006). Students against Facebook News Feed (official petition to Facebook). Retrieved from www.Facebook.com/group.php?gid=2208288769.

Peer, E., Acquisti, A., & Loewenstein, G. (n.d.). The impact of reversibility on the decision to disclose personal information. Working Paper.

Pennebaker, J. (1984). Confiding in others and illness rate among spouses of suicide and accidental-death victims. *Journal of Abnormal Psychology*, *93*(4), 473–476.

Pennebaker, J. W., Kiecolt-Glaser, J. K., & Glaser, R. (1988). Disclosure of traumas and immune function: Health implications for psychotherapy. *Journal of Consulting and Clinical Psychology*, *56*(2), 239–245.

Png, I. P. L. (2007). *On the Value of Privacy from Telemarketing: Evidence from the "Do Not Call" Registry*. Singapore: National University of Singapore.

Rabin, M., & O'Donoghue, T. (2000). The economics of immediate gratification. *Journal of Behavioral Decision Making*, *13*, 233–250.

Read, D., Loewenstein, G., & Rabin, M. (1999). Choice bracketing. *Journal of Risk and Uncertainty*, *19*(1–3), 171–197.

Reis, H. T., & Shaver, P. (1988). Intimacy as an interpersonal process. In S. Duck (ed.), *Handbook of Personal Relationships* (pp. 367–389). Chichester, England: Wiley.

Riis, J., Loewenstein, G., Baron, J., Jepson, C., Fagerlin, A., & Ubel, P. (2005). Ignorance of hedonic adaptation to hemodialysis: A study using ecological momentary assessment. *Journal of Experimental Psychology: General*, *134*(1), 3–9.

Romanosky, S., & Acquisti, A. (2009). Privacy costs and personal data protection: Economic and legal perspectives. *Berkeley Technology Law Journal*, *24*(3), 1061–1101.

Romanosky, S., Sharp, R., & Acquisti, A. (2010). Data breaches and identity theft: When is mandatory disclosure optimal? Presentation for the Ninth Workshop on the Economics of Information Security (WEIS), June 7, Arlington, VA.

Rosen, J. (2010). The web means the end of forgetting. *New York Times Magazine*, July 21. Retrieved from www.nytimes.com/2010/07/25/magazine/25privacyt2.html?pagewanted=all&_r=0.

Schelling, T. C. (1968). The life you save may be your own. In S. Chase (ed.), *Problems in Public Expenditure Analysis* (pp. 113–146). Washington, DC: Brookings Institute.

Sedikides, C., Campbell, W. K., Reeder, G. D., & Elliot, A. J. (1999). The relationship closeness induction task. *Representative Research in Social Psychology, 23*, 1–4.

Singer, E., Hippler, H.-J., & Schwarz, N. (1992). Confidentiality assurances in surveys: Reassurance or threat? *International Journal of Public Opinion Research, 4*, 256–268.

Singer, E., von Thurn, D. R., & Miller, E. R. (1995). Confidentiality assurances and response: A quantitative review of the experimental literature. *Public Opinion Quarterly, 59*, 66–77.

Slovic, P. (1995). The construction of preference. *American Psychologist, 50*(5), 364–371.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly, 20*(2), 167–196.

Smyth, J. M. (1998). Written emotional expression: Effect sizes, outcome types, and moderating variables. *Journal of Consulting and Clinical Psychology, 66*, 174–184.

Solove, D. (2007). *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet.* New Haven, CT: Yale University Press.

Spera, S. P., Buhrfeind, E. D., & Pennebaker, J. W. (1994). Expressive writing and coping with job loss. *Academy of Management Journal, 37*, 722–733.

Spiekermann, S., Grossklags, J., & Berendt, B. (2001). E-privacy in 2nd generation E commerce: Privacy preferences versus actual behavior. Paper presented at the Conference on Electronic Commerce, Association for Computing Machinery, Tampa, FL.

Stalder, F. (2002). The failure of privacy enhancing technologies (PETs) and the voiding of privacy. *Sociological Research Online, 7*(2). Retrieved from www.socresonline.org.uk/7/2/stalder.html.

Tamir, D. I., & Mitchell, J. P. (2012). Disclosing information about the self is intrinsically rewarding. *Proceedings of the National Academy of Sciences, 109*(21), 8038–8043.

Tanner, A., (2014). *What Stays in Vegas: The World of Personal Data – Lifeblood of Big Business – and the End of Privacy as We Know It.* New York: PublicAffairs.

Tate, R. (2009). Facebook's great betrayal. Retrieved from http://gawker.com/5426176/Facebooksgreat-betrayal.

Thaler, R. (2009). Civility check has been here all along. Retrieved from http://nudges.wordpress.com/a-civility-check-has-been-here-all-along/.

Thaler, R., & Benartzi, S. (2004). Save more tomorrow: Using behavioral economics to increase employee saving. *Journal of Political Economy, 112*(1), S164–S187.

Tourangeau, R., & Yan, T. (2007). Sensitive questions in surveys. *Psychological Bulletin, 133*(5), 859–883.

Tsai, J. Y., Engelman, S., Cranor, L., & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research, 22*(2), 254–268.

Tucker, C. (2014). Social networks, personalized advertising, and privacy controls. NET Institute Working Paper No. 10–07; MIT Sloan Research Paper No. 4851–10. Available at SSRN: http://ssrn.com/abstract=1694319.

Tufecki, 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.

Tversky, A., & Kahneman, D. (1974). The framing of decisions and the psychology of choice. *Science*, *211*(4481), 453–458.

Tversky, A., & Kahneman, D. (1991). Loss aversion in riskless choice: A reference dependent model. *Quarterly Journal of Economics*, *106*(4), 1039–1061.

Tversky, A., Slovic, P., & Kahneman, D. (1990). The causes of preference reversal. *American Economic Review*, *80*(1), 204–217.

Tybout, Alice M., Sternthal, Brian, & Calder, Bobby J. (1983). Information availability as a determinant of multiple request effectiveness. *Journal of Marketing Research*, *20*(August), 280–290.

Van Baaren, R., Horgan, T., Chartrand, T. L., & Dijkmans, M. (2004). The forest, the trees, and the chameleon: Context dependency and nonconscious mimicry. *Journal of Personality and Social Psychology*, *86*, 453–459.

Volpp, K., John, L., Troxel, A. B., Norton, L., Fassbender, J., & Loewenstein, G. (2008). Financial incentive-based approaches for weight loss: A randomized trial. *Journal of the American Medical Association*, *300*(22), 2631–2637.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, *4* (5), 193–220.

Wathieu, L., & Friedman, A. 2009. An empirical approach to understanding privacy concerns. ESMT Working Paper 09–001, ESMT European School of Management and Technology, Berlin.

Wawro, A. (2008). ToneCheck email plugin is like spellcheck for your emotions. *PC World Communications*. Retrieved from http://tech.ca.msn.com/pcworld-article.aspx?cp-documentid=27941607.

Weinstein, N. (1980). Unrealistic optimism about future life events. *Journal of Personality and Social Psychology*, *39*(5), 806–820.

Westin, A. F. (1991). *Harris-Equifax Consumer Privacy Survey 1991*. Atlanta, GA: Equifax, Inc.

White, T. B., Zahay, D. L., Thorbjorsen, H., & Shavitt, S. (2008). Getting too personal: Reactance to highly personalized email solicitations. *Marketing Letters*, *19*, 39–50.

Whitten, A., & Tygar, J. D. (2005). Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In L. Cranor & G. Simson (eds.), *Security and Usability: Designing Secure Systems that People Can Use* (pp. 679–702). Sebastopol, CA: O'Reilly and Associates.

Whitty, M. T., & Joinson, A. N. (2009). *Truth, Lies, and Trust on the Internet*. New York: Routledge.

Zuckerberg, M. (2006). An open letter from Mark Zuckerberg. Retrieved from http://blog.Facebook.com/blog.php?post=2208562130.