Surrendering Information Through the Looking Glass: Transparency, Trust, and Protection

Kristen L. Walker

Trust and transparency influence consumer information exchanges, yet the understanding of how they shape marketing and public policy relating to privacy and security issues is not current with the digital and informational age. People face increasing complexity in online exchanges of information and lack the time, attention, and wherewithal to understand how to protect themselves. Society's reliance on technology results in individuals engaging in continuous partial attention and behaving as cognitive misers. The author explains the concept of surrendering to technology and presents a sharing–surrendering information matrix to address this phenomenon. The matrix clarifies the difference between surrendering versus sharing information online, leading to the proposition that current efforts to protect privacy and security, such as enhancing trust and transparency, lack legitimacy and will not be effective in the digital age. Surrendering information is a long-term societal and ethical issue for marketers and policy makers, requiring improvement(s) in verification mechanisms and increased educational efforts aimed at enhancing consumers' attention.

Keywords: information, trust, transparency, protection, privacy

The best victory is when the opponent surrenders of its own accord before there are any actual hostilities.... It is best to win without fighting.
—Sun Tzu

Exchanging Information on the Internet

The Internet has evolved and encroached on marketing with a vengeance. Originating as a method for communication and information, it has grown into a context for transactions, analyses, and multifaceted interactions. The digital age and the "Internet of Things" provide unique advantages through technology that enable consumers, organizations, and now machines to rapidly exchange information and acquire knowledge. Artificial intelligence and facial recognition software are becoming more conventional innovations used to facilitate exchanges. Information is a product and by-product of many of these innovative exchanges; a product that is gathered, stored, packaged, and sold. Firms purportedly use "big data" to personalize services and products as a means of improving customer satisfaction and increasing customer lifetime value, sometimes without much forethought. Society's increasing reliance on technology creates a data-rich environment that is inextricably intertwined with marketing and public policy issues of transparency, trust, and consumer protection.

The ease and convenience of exchanging information online often leaves consumers[1] with little choice but to participate, and little time to systematically process the short-term and/or long-term implications of this information exchange. The speed of innovation and adoption of new technology by consumers and organizations means that the use of data as a resource is exponentially increasing. American consumers face a data-rich environment with few modern legal or regulatory protections and rely on reactive measures to adapt to the new environment of limited privacy and security. Every day, consumers are interacting with technological devices, online platforms, and applications, exchanging personal information (e.g., location, health/medical data, relationships, preferences, behaviors) with a variety of third parties, often without clear knowledge of the identity of these parties. This socially transmitted data fosters uncertainty and places consumers at risk, making them vulnerable to third parties in information exchanges. Current methods of addressing privacy focus on controlling personal information and increasing transparency and trust. Yet in most instances, consumers are overloaded with digital information and lack the time and attention required to control their privacy, which hinders their ability to assess the trustworthiness of their online exchanges. This problem requires a shift in the basic

---

[1]This article focuses on consumers, yet many of the concepts (e.g., cybersecurity, liability) can be applied to organizations in the digital age.

assumptions of and solutions to privacy and security issues pertaining to marketing and public policy. The concepts developed herein around trust, technology, and transparency update and frame issues of privacy and security in the digital age, proposing a societal need for marketers and policy makers to increase consumer protection through regulation and education.

Policy makers and marketers often tout increasing trust and transparency as part of the solution to privacy issues. Yet the uncertainty that exists in online exchanges of information impedes trust; this uncertainty, accompanied by the ambiguity of transparency, is at the core of the privacy and security conundrum. The notion that information "consumes the attention of its recipients" (Simon 1971, p. 6) makes this issue especially concerning. In their discussion of relationship marketing and transparency, Murphy, Laczniak, and Wood (2007, p. 16) note that "a transparent firm does not give away trade secrets, but at the same time does not keep its stakeholders in the dark." The White House (2012, p. 1) Privacy Bill of Rights lists transparency as one of seven rights that apply to personal data, stating that "consumers have a right to easily understandable and accessible information about privacy and security practices." In May 2014, the Federal Trade Commission (FTC) issued a report, "Data Brokers: A Call for Transparency and Accountability," finding that data brokers operate without complete transparency and recommending that Congress enact legislation to improve knowledge and consumers' access to personal information held by companies (FTC 2014). Transparency in the digital age means that the rules, algorithms, and filters used to collect, store, and disseminate consumer information should be visible *and* understood by individuals and organizations. Yet requiring more data to be transparent will mean more information for consumers to process, further challenging their ability to make sound decisions and engage in protection behaviors.

In this article, I discuss the significance of technology in information exchanges and clarify the ambiguous nature of the concepts of trust and transparency. The lack of clarity around these concepts misleads consumers and influences exchanges of information online, encouraging the surrender to technology. New paradigms of privacy and security require a shift in consumer focus and attention. After proposing and describing the phenomenon of surrendering to technology, I present a 2 × 2 matrix of sharing versus surrendering information, define key constructs, and examine relevant literature. By doing so, this article will assist marketers and policy makers in understanding the nuances of trust, transparency, and protection behaviors in online exchanges of information and will clarify these nuances to protect and educate consumers about the long-term consequences that result when they willingly (and often unknowingly) surrender information. Current notions of prevention and protection may not be effective when people surrender information, underscoring societal and ethical concerns.

Surrendering to Technology

I postulate that surrendering to technology is a phenomenon whereby individuals in the digital age readily and willingly exchange information under conditions and in circumstances that they do not adequately understand. This advances current notions of privacy and security in marketing and public policy, demonstrating that there are significant challenges to trust and transparency as protection and/or prevention tools for consumers. In marketing, the term "surrender" has been used to describe competitive states and reaction (Kotler and Singh 2001), but it has not been used conceptually. Extant research has shown that surrender, as a concept, has been used primarily in sociology to describe epistemological views of knowledge and experience, to express methodological concerns for participants and respondents, or to address cultural issues (Postman 1992; Wolff 1976). In light of the phenomenon of surrendering to technology, it is critical for marketers and public policy makers to address the reality that "a wealth of information creates a poverty of attention" (Simon 1971, p. 6).

The concept of surrender generally implies submission. "Technology . . . is both friend and enemy" (Postman 1992, p. xii) and can lead to "the submission of all forms of cultural life to the sovereignty of technique and technology" (p. 52). I propose that surrendering to technology consists of overlapping constructs that delineate the challenges involved with exchanging information online (see Figure 1). These constructs are central to the changing nature of privacy and security issues in marketing and public policy. The four constructs identified are grounded in two general challenges: context (vulnerability, risk, and uncertainty) and complexity (continuous partial attention and cognitive miser behavior). In line with Chandler and Vargo's (2011, p. 38) views of markets and contexts, context is utilized in this article to frame challenges with online environments or "interactions or exchanges that we can 'see' and 'understand' [but] essentially . . . are continuous." Complexity frames the challenges individuals face when processing information in the digital age, emphasizing the need for public policy makers to focus on the problems created by surrendering to technology.

In online information exchanges, when individuals lack time or attention and are overloaded with information, they encounter contexts of uncertainty, vulnerability, and risk. The Internet of Things only magnifies this overload with the increasing yield of data, the rapid growth of data sources, and the persistent connections among consumers and firms (Brill 2014). In essence, the complexity in our informational age and speed of technological changes force some people to act without much forethought or reflection in their digital interactions. Thus, people engage in "continuous partial attention" (Stone 2007) and behave as cognitive misers (Fiske and Taylor 1991) (see Figure 1). The increasing capacity and interconnectedness of devices and data intensify the challenges for individuals and organizations.

Complexity Challenges: Lack of Time/Attention and Information Overload

When confronted with multiple devices and environments that are all connected to the Internet, people in the informational age exhibit continuous partial attention. In a *New York Times* article about the "age of interruption," Friedman (2006) notes that consumers in the digital age process information with continuous partial attention, multitasking with a variety of devices and activities. Continuous partial attention differs from multitasking by the type of motivation. Multitasking is "motivated by the desire to be more productive and efficient . . .,

Figure 1.   Challenges of Exchanging Information on the Internet
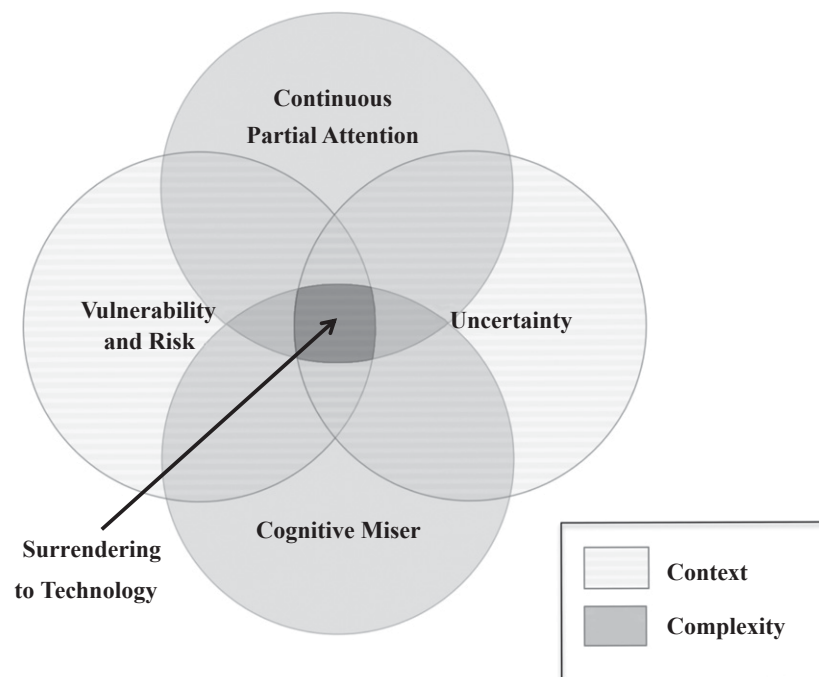
doing things that are automatic, that require very little cognitive processing." Continuous partial attention, in contrast, is "motivated by a desire to be a live node on the network . . ., scan[ning] for opportunity and optimiz[ing] for the best opportunities, activities, and contacts, in any given moment" in an "artificial sense of constant crisis" (Stone, personal website). This "distracted mental state" of continuous partial attention essentially means that people lack the time and, most importantly, the attention required to focus on the key details needed for their safety in exchanges of information online (Small and Vorgan 2008, p. 48). This significantly increases the risk, vulnerability, and uncertainty in online exchanges of information.

When people are continuously partially attentive, this distracted state also means that they are more likely to behave as cognitive misers. Because they are short of time, individuals portraying cognitive miser behaviors tend to simplify and reduce the amount of information they use to make decisions and prioritize (Fiske and Taylor 1991). In a data-rich online environment in which uncertainty is prevalent, this scenario increases the vulnerability and risk to consumers.

People engage in continuous partial attention when they face an abundance of information, lacking the time and attention needed to make qualified decisions about protection. In addition, they face uncertainty in online environments, which results in a simplification of their information processing behavior (i.e., makes them cognitive misers). Prior research has extensively covered information processing and decision making. Information processing in psychology, economics, and marketing includes a variety of competing and complimentary concepts and theories, such as heuristics (Tversky and Kahneman 1974), the theory of bounded rationality (Simon 1972), the elaboration likelihood model

(Petty and Cacioppo 1986), or the MOA (motivation, opportunity, and ability) model (MacInnis, Moorman, and Jaworski 1991). These concepts all address how people process information, develop shortcuts, satisfice, create rules of behavior, and make decisions. To clarify, the complexity challenges as outlined in my conceptual framework do not focus on *how* consumers process information. What is relevant is that in the digital age, consumers are challenged to process an abundant amount of information in a short amount of time. They engage in continuous partial attention and act as cognitive misers, which means they surrender to technology, placing them at risk and making them vulnerable.

Contextual Challenges: Vulnerability, Risk, and Uncertainty

Protection implies vulnerability for participants in an exchange and is cause for ethical concern. Marketing and public policy issues of privacy and security involve the concepts of vulnerability and risk. Vulnerability refers to "a state of powerlessness aris[ing] from an imbalance in marketplace interactions or from the consumption of marketing messages and products," when the control is not in the hands of the individual or, in this case, the organization (Baker, Gentry, and Rittenberg 2005, p. 134). The concept of risk differs from vulnerability in that risk involves the quantification of susceptibility to harm, often based on the use of historical data, whereas vulnerability is the materialization of risk (Baker 2009). Exchanges of information online involve so many networks, cookies, application programming interfaces, and so on that even if consumers have an idea of with whom they are exchanging information, the other party's identity cannot easily be verified. Baker (2009, p. 118)

explains that vulnerability is the loss of security, not simply risk or the "probability that security will be lost." Yet in a digital world in which "clouds" store socially transmitted data and in which there is a lack of control over information dissemination, even when protection behaviors such as privacy settings are employed, there is no guarantee that consumers' privacy will not be breached and that company data will not be hacked. Interactions and exchanges in the digital age are rife with uncertainty and risk for consumers and liability issues for organizations.

Trust and transparency foster participation in online interactions and exchanges, reducing friction and allowing for convenience. Unfortunately, the regulatory and self-regulatory concepts of transparency are not clear enough to protect consumers in these exchanges. In addition, the assumption that giving consumers control over their information as a self-regulatory or regulatory solution ignores the complex aspect of data management processes for organizations and individuals. This complexity highlights important policy questions involving power versus process and knowledge versus access. If consumers are succumbing to technology, even with the regulatory and self-regulatory illusion of transparency, they have the right to understand that they are surrendering information and thus require protection.

Some scholars view the efficiency of interacting and acquiring knowledge on the Internet as leading to collaborations that benefit all by enhancing knowledge, and they assert that openness and transparency are ultimately societal benefits and social values (Westin 2003). Steele (2012, p. 57) states, "When we relate and share knowledge authentically, this places us in a state of grace, a state of 'win–win' harmony with others, and establishes trust among all." An opposite view is that we must address "cyber-utopianism," or the "naïve belief in the emancipatory nature of online communication that rests on a stubborn refusal to acknowledge its downside" (Morozov 2011, p. xiii). As Morozov (2011, p. 148) explains, "The Internet runs on trust, but its dependence on trust also opens up numerous vulnerabilities." This dual nature of the primary benefit of the Internet—to easily exchange information and acquire knowledge—highlights important questions for marketing and public policy about illusions of transparency and issues of privacy and security. Consumers are vulnerable in online exchanges because they face complexity and time constraints and engage in continuous partial attention; as a result, they simplify, behaving as cognitive misers. The notion that consumers not only may benefit from online interactions but also may be surrendering in these interactions highlights the necessity of marketing and public policy efforts to educate and protect consumers. Acknowledging that consumers surrender to technology will help clarify the ambiguous nature of the concepts of trust and transparency that mislead policy makers, consumers, and firms, thus influencing the protection and prevention mechanisms involved in interactions online.

Illusions of Trust, Transparency, and Protection

Storing client information in the cloud, using search history to serve consumers online behavioral advertisements or similar product offerings, promoting location-based dining choices, e-mailing promotional material, and other exchanges require consumer information. This information is gathered, stored, and disseminated in an instant through an array of smart devices. As of January 2014, Pew Research Center (2014) reported that more than half (58%) of Americans have a smartphone and 60% of Americans use their mobile devices to access the Internet. In November 2014, Pew Research Center reported that fewer than half of Americans (44%) are aware that the existence of a privacy policy does *not* mean that a firm keeps the information it gathers confidential (Smith 2014). The use of technology in the digital age is increasing at a faster pace than an understanding of the issues involved, leaving large amounts of data available for misuse and little time for regulation and self-regulation efforts to keep pace with the innovations.

In 1964, Marshall McLuhan wrote about the "electronic age" and the emergence of the television in his book *Understanding Media*. Although his focus at the time was television, he noted the connection between technology and the abundance of information.

> In this electronic age we see ourselves being translated more and more into the form of information, moving toward the technological extension of consciousness. The aspiration of our time for wholeness, empathy and depth of awareness is a natural adjunct of electric technology.... There is a deep faith to be found in this attitude—a faith that concerns the ultimate harmony of all being. (McLuhan 1964, p. 5)

Each year, the price of processors, bandwidth, and storage declines, reducing the cost to stream files on the Internet (Anderson 2009, p. 13). Consequently, online interactions have exploded, with information as a by-product. Information is an increasingly accessible and valuable resource "that is externally-based and dynamically determined in the context; that is they are resources that cannot be owned or controlled by a single actor" (Chandler and Vargo 2011, p. 38). This is significant because, as of mid-2013, "a full 90% of all the data in the world [had] been generated" (Dragland 2013). All parties benefit from online interactions and exchanges to some degree, but as these exchanges increase, consumers become resigned to the abundance of information exchanged, stored, and disseminated. It is evident that many consumers do not really know and understand when they are providing information or how information about them is packaged and sold, and even those that do are challenged by continual partial attention, leading to cognitive miser behavior.

The concept of transparency implies openness, knowledge, and verification without specificity of the context, time, or the number of parties involved, yet online information exchanges can involve an infinite number of parties. After the exchange of information occurs, much of the handling of the information is not seen, known, or evident to consumers. New technology gives consumers both a lot *of control* and a lot *to control*, but consumers and organizations often lack the capacity to manage either their information or the process of protecting the information they provide. This places them in a vulnerable position with regard to the information they exchange online and clarifies the significance of surrendering to technology for marketers and public policy makers. People may be resigning themselves to the new realities of technology, but this resignation is not necessarily a choice.

Consumers should be able to trust that other parties will handle their information ethically and should have a level of

control over this handling. How they can attain this control when so much uncertainty exists in the digital and informational age is an important question. Information exchanges between consumers and firms increasingly involve machines—information is no longer stored only on a piece of paper locked away in a file drawer in one physical location. Thus, trust is at the core of ethical relationship marketing. Murphy, Laczniak, and Wood (2007, p. 12) distinguish between authentic trust and "blind, simple or naïve trust," indicating that authentic trust "is given and reciprocated only after being carefully considered." In an examination of trust and performance in cooperative exchanges, Gundlach and Cannon (2009, p. 1) indicate that participants "offset the vulnerability of trust with verification strategies." The verification strategies that participants employ can help facilitate trust and enhance performance. Verifying information by monitoring resources and sharing information requires participants to either think carefully and process information to make decisions or avoid thinking and make decisions hastily, at times without regard or worry about potential harm.

The complexity and continuous evolution of technological advances in the informational age emphasizes exchanges of information. When individuals surrender to technology, mechanisms such as trust, transparency, and protection may not help them carefully consider their options when exchanging information. The surrendering-to-technology framework emphasizes the need to examine the illusions associated with trust, transparency, and protection. Surrendering is rarely the optimal choice in an exchange unless all parties are aware of and understand the agreement. Technology is best used to help people, to empower them to make informed choices, and to enable them to maneuver through complicated processes. When consumers surrender to technology in online information exchanges, they are also apt to surrender information. To delineate how individuals cope with the complexity and uncertainty in online information exchanges, I distinguish sharing information from surrendering information with two propositions. First, surrendering to technology threatens the careful consideration and verification strategies by consumers; thus, they exhibit *faith*, rather than *trust*, in the information exchange. Next, building on previous privacy research and the concept of surrendering to technology, I posit that many consumers are passive in protecting themselves in their exchanges of information online. This dynamic of faith in online information exchanges and passive protection behavior frames surrendering information as a critical societal issue for marketers and public policy makers.

The Sharing–Surrendering Information Matrix

I use two constructs best suited to shift the paradigms associated with transparency, trust, and protection and distinguish sharing information from surrendering information: (1) *trust/faith*, based on the level of certainty in information exchanges, and (2) *active/passive protection*, influenced by challenges with information processing and attention. The resulting 2 × 2 matrix (see Figure 2) highlights the complexity of transparency (what is known, seen, and evident) in information exchanges. It clarifies that while transparency is used to help foster trust, the uncertainty and challenge for individuals to process increasingly more information leads

to consumer vulnerability. Uniting these constructs forms the sharing–surrendering information matrix (SSIM) shown in Figure 2. Next, the four quadrants of the matrix are outlined, followed by detailed explanations of the trust/faith and active/ passive constructs.

The SSIM addresses "roles of mutual benefits, mutual commitments, trust, and social and information linkages" that are necessary to understand in the increasing information and digital age (Day and Montgomery 1999, p. 3). As consumers share more information, firms and third parties will continue to collect and store data. The motive and intent of this collection is not evident at the outset of these exchanges. In ethical relationship marketing, transparency in interactions is exemplified by virtues of fairness, integrity, respect, and empathy (Murphy, Laczniak, and Wood 2007). Yet with so much complexity in the use, storage, and dissemination of consumer information exchanged online, one or more of these virtues can be compromised. Although consumers seemingly provide information for an immediate purpose (e.g., purchase, search, social), that purpose is most often perceived as short term. The ease of storing and sharing digital information, combined with the current challenge of verifying the pertinent details of what happens with the information in these exchanges and the lack of cognitive consideration by many consumers, are significant problems. The inadvertent impact is that people are surrendering information for the long run even if they believe they have shared the information conditionally. Individuals exchange information at one point in time that may be used in the future without their knowledge or control of that use.

Reciprocity is an important aspect of fairness in exchanges, even those concerned with sharing information on the Internet. If there is mutual benefit for both parties in the exchange of information, then both parties are more likely to be satisfied. Some marketing academics, especially in public policy, have found that marketers may benefit at a cost to the consumer (e.g., Caudill and Murphy 2000). The SSIM portrays the exchange of information online defined by the level of certainty. More certainty in an exchange depicts trust when information provided is considered *shared*, whereas less certainty depicts faith when information is *surrendered* or at risk of being taken, used, or stored without the knowledge of the other party.

Because an exchange of information on the Internet involves many parties (i.e., the website, the individual, and third parties) and the motives of these parties are not always evident, the SSIM also takes into account the nature of the protection behaviors enacted. Active protection behavior means that the party sharing the information online (dis)allows others to access the information without his or her explicit permission—(s)he places conditions on the exchange (i.e., uses privacy settings). In contrast, passive protection behaviors describe when the party sharing the information allows anyone access to his or her information or provides information unconditionally (willingly or unwillingly).

The four quadrants are conditional share, unconditional share, conditional surrender, and unconditional surrender. From a marketing and public policy perspective, the significance of the SSIM is where surrendering occurs—on the faith side of the trust–faith continuum, at which point transparency is promoted by industry and policy makers—yet in the digital age, people are likely to be continually partially attentive and

Figure 2.   The Sharing–Surrendering Information Matrix (SSIM)
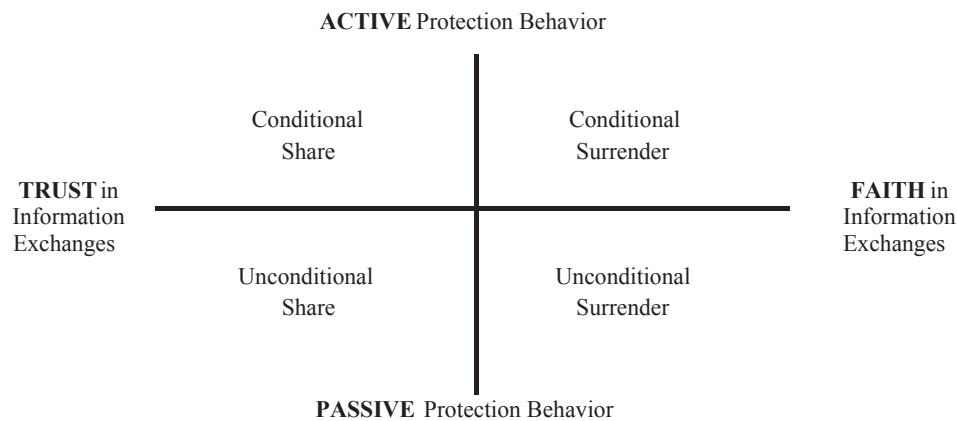
behave as cognitive misers. This means that consumers cannot or do not engage in protection behaviors or verify with certainty the complexities of the information exchange needed to employ active protection behaviors. In these cases, the participants are surrendering information, either conditionally (active protection) or unconditionally (passive protection). Examples of each quadrant are provided next.

Conditional Share

When consumers trust an exchange on the Internet and engage in active protection, they share information yet place conditions on the information they provide. This conditional sharing describes a mutually beneficial (i.e., reciprocal) exchange, the ideal and utopian view of exchanges on the Internet. This mutually beneficial exchange is facilitated by trust between both parties. Complete certainty for this trust is realistically impossible to achieve, yet this quadrant illustrates the most certainty. An example of conditional share is as follows:

> A consumer on a social media website posts a status update indicating his presence at an event. The consumer would prefer that certain friends or followers not know that he is present at the event. The consumer places restrictions on the post through the privacy settings, disabling certain people from seeing his post. The consumer willingly shares information but implements protection behaviors, trusting that the social media site's privacy settings will work. The consumer has the ability to verify his privacy settings to test and determine whether these friends will be able to view the post, now and in the future. The consumer is also able to view any and all parties who receive his information from the initial social media site, whether shared, stored, bought, or sold.

Unconditional Share

If the parties exhibit trust in an exchange and are passive in their privacy protection, this means they are surrendering information to others, described as unconditional sharing. An example of unconditional share is as follows:

> A consumer purchases a new application for her smart device that one of her friends told her about. As part of the process to set up the new app, the consumer is asked to read the privacy policy and

agree to the terms of service. The consumer is in a hurry and checks the box indicating that she has read and agrees to the terms. The consumer is passive in her protection behavior, and because her friend has the app, she trusts that the app will not harm her and poses no actual threat. There is no easy verification method to determine the veracity of this agreement in the short or long run. The consumer is not able to view any and all parties who receive her information from the initial company, whether shared, stored, bought, or sold.

Conditional Surrender

When parties in an exchange exhibit faith in an exchange of information on the Internet and are active in their privacy protection (placing conditions on the exchange), they are actively allowing others some access, described as conditional surrender. An example of conditional surrender is as follows:

> A high school student agrees to go to prom with another student. Before the prom, she sends her date a suggestive, scantily clad picture of herself. She knows the dangers of texting a picture of this sort and understands that she should not post this type of picture on social media, because it is only meant for her date. She chooses to send it through a social media platform/application on which the image "disappears" after a few seconds. Although the platform/app informs her when her image has been "copied," her date has another platform/app that allows him to take a screenshot of the image without informing her. She has faith both in her platform/app and that her date will not use the picture in a damaging manner. The following day, she sees her picture posted on her date's social media site with the hashtag "#mysurething4prom." She also was not able to view any and all parties who had the potential to receive her information from the initial site, whether they shared, stored, bought, or sold her information.

Unconditional Surrender

Finally, and most concerning, there are instances in which parties have faith in an exchange of information on the Internet and are passive in their privacy protection, demonstrating unconditional surrender. An example of unconditional surrender is as follows:

A person visits an office building in a major U.S. city. As part of the entry policy to the building, the visitor must show his driver's license. The visitor is not informed and has no idea that the security team at the building runs his license number through complex software that provides the security personnel a brief history of personal information, including social media posts, to determine his level of threat. The visitor has faith that his license will be used only to assess the risk of gaining access to the building. As a result, visitors are completely passive in their protection behaviors. The visitor is not able to view any and all parties who may have access to this surrendered information.

The examples only provide a glimpse into the complexity of trust, transparency, and protection in online information exchanges. What follows is a detailed examination of the literature used to develop each construct. While previous research helps explain what consumers have done and perceived with regard to their information exchanges, the matrix provides a macro perspective. This will enable marketers and policy makers to consider which quadrant consumers are currently in and how to move them to less vulnerable quadrants. It also stresses the ethical necessity involved with regulatory and self-regulatory issues of consumer information exchanges and questions whose responsibility it is to encourage active protection strategies.

Complexity and Uncertainty in Information Exchanges: Trust or Faith

For some, trust is touted as a solution to privacy concerns and consumer doubt. Firms are encouraged to strengthen the trust with their consumers and vendors to "boost e-commerce" (Luo 2002, p. 112). TRUSTe (2014, p. 11), a third-party verification service, concludes in its 2014 Consumer Confidence Privacy Report that "businesses need to do more to build online trust." In Federal Trade Commissioner Julie Brill's (2014) speech, titled "The Internet of Things: Building Trust and Maximizing Benefits Through Consumer Control," she states, "Now is the time to ask how companies can provide this burgeoning connectivity—and its considerable benefits—without compromising consumers' privacy or losing their trust" (p. 3). Trust is important, but without certainty of all the details in an exchange, trust is elusive, and transparency is nonexistent (i.e., the exchange is opaque). Providing *all* the information is not enough to move consumers from surrendering information to sharing information. The next section discusses what it means to share or surrender information, based on the level of certainty that exists in the exchange.

Transparency and Trust: Sharing Information

Trust acts as a catalyst for exchanges between buyers and sellers (Pavlou 2003). In an examination of the theory of exchanges in marketing, Houston and Gassenheimer (1987) describe the goal of marketing involving trust. "The goal of marketing is still the development of trust between exchange partners that leads to a long-term relationship" (p. 10). They examine reciprocity in social interactions and the social distance between exchange partners. Relevant to trust as a process is their recognition that exchanges that "have not been fully consummated can occur in a state of total uncertainty …

because this state is what leads to the establishment of trust" (p. 11). The process of an exchange is thus facilitated by trust, even when and if uncertainty exists. Reciprocation of acceptable terms in a mutual exchange can benefit the relationship and, thus, the outcomes. Key to this exchange is how reciprocation of terms works when consumers surrender to technology. If they rely on trust to facilitate processes, and the issue of trust is already confounding, then the increasing uncertainty that exists in online exchanges when individuals are continuously distracted poses a problem for consumers. How do we operationalize transparency to assist consumers and foster trust rather than overwhelm consumers and engender faith?

Zucker (1986) points out that trust is implicit in all forms of exchanges and not easily measured. "Trust is so closely related to basic norms of behavior and social customs that most actors take it for granted until it is violated" (p. 3). On the Internet, this behavioral norm is magnified as a result of continuous changes in technology that challenge common understandings and the fluidity of the context and situation. For example, Zucker discusses the background expectations as standardized sets involving signals and coding rules. These rules develop "reciprocity of perspectives" with individuals or firms making use of similar social cues and facts in an exchange (p. 8). On the Internet, the social cues and facts in the exchange of information are constantly in flux. Therefore, the signals and coding rules necessary as the foundation for trust mean that exchanging information online involves a high degree of uncertainty. In essence, "trust is a defining feature of most economic and social interactions in which uncertainty is present" (Pavlou 2003, p. 106). In the digital age, signals may provide clues to consumers to pay attention and be less miserly with their cognitive resources.

The implied intent of the availability of information on the Internet is cooperation and exchange. Consumers use a variety of services and applications, and many of these are without overt costs. This exchange is much like a conversation, though technology allows for variable time frames (real time or delayed) and contexts (mobile, e-mail, or apps). Consumers use applications to manage their daily lives and firms use applications and programs to manage their business activities. The problem is that exchanging information on the Internet seldom occurs in what technology experts refer to as a "walled garden," or a completely defined and closed environment on the Internet. More problematic is that exchanges of information on the Internet rarely occur in a simple, dyadic relationship between one party and another. Conversations and interactions online are often a complex network (web) of information and algorithms. This complexity challenges consumers' ability to verify their trust. Yet in many cases, the required knowledge for the foundation of trust is almost impossible to obtain by the average consumer. In 1996, the Director of the Electronic Frontier Federation stated that the "lack of trust is a significant impediment to electronic commerce" (Anthes 1996, p. 72). This observation is compounded by the fact that the exchange of information between parties on the Internet is not always fair, meaning that information cannot and is not always verified or verifiable. Using "transparency" as a catchall phrase is not the answer. Instead, technology and transparency should be used to provide the key details consumers need in a user-friendly

manner. Food pyramids, financial risk segments, and other simple organization strategies for complex information are some examples of successful strategies employed.

Transparency and Faith: Surrendering Information

Transparency is a way to enhance trust, but the following subsection describes faith as differing from trust and what that means for online information exchanges. When it is difficult to "believe that one can know quickly what one's experience means," this describes a lack of certainty and connotes faith (Wolff 1976, p. 20). Uncertainty may be measured when confidence is vested in a relationship with little or no evidence. This serves to support the position that trusting with a high level of uncertainty is, in actuality, faith. When faith is used in an information exchange, it portrays surrendering information, rather than sharing information.

Morgan and Hunt (1994) address the issue of uncertainty in relationships that involve commitment and trust and theorize that a successful process of relationship marketing requires commitment and trust. They delve into ethical considerations of trust by conceptualizing trust as "existing when one party has confidence in an exchange partner's reliability and integrity" (p. 23). This highlights the benefit of trust as a lubricant in exchanges, facilitating easier and faster decision making. "Trust decreases a partner's decision-making uncertainty because the partner has confidence that the trustworthy party can be relied on" (p. 26). Morgan and Hunt argue that trust is a process with uncertainty embedded, while the actual decision making is the result of the process.

Gundlach and Cannon (2009) illustrate the confounding aspects of trust or the "dilemma of trust" for firms and apply the notion of truth and proof by operationalizing a "trust but verify" concept (p. 5). In their study of performance implications of cooperative exchanges, they show that trust enhances performance related benefits, in support of the notion of trust as facilitator. They assert that "trust can enhance relationship quality and facilitate performance in exchange" (p. 1). Even so, they describe a "dilemma of trust," because it not only "empower[s] a relationship, . . . [it] also creates conditions of vulnerability" (p. 2). Gundlach and Cannon propose that information produced in the process of trusting in relationships is utilized in the "trust but verify" concept describing the effective use of information in exchange. Their findings demonstrate that trust and verification strategies involve gathering and using information in an exchange and that when participants in the exchange share information, it reduces uncertainty and helps productivity. This implies that there are challenges with verification strategies when there are high degrees of uncertainty, when parties do not share information, or when they share false information. Their study focuses on cooperative exchanges, in which both parties share information to enhance the performance of each. It is critical to learn how these exchanges occur in the Internet of Things. Understanding the nature of cooperation when consumers may be engaging in continuous partial attention and acting as cognitive misers is essential for marketers and policy makers to move consumers toward certainty and trust and encourage sharing rather than surrendering information.

A *Consumer Reports* WebWatch report titled "Leap of Faith: Using the Internet Despite the Dangers" indicates that "trusting the information online is a key to the users' faith in any site" (Derakhshani and Bloom 2005, p. 23). This report details a variety of online categories (identity theft, e-commerce, financial sites, news sites, blogs, and search engines) in which consumers remain skeptical about privacy and protection even though they have built a level of trust over time and through interactions. The study finds that consumers often make a "leap of faith" when interacting online, yet the authors use the term loosely and only tangentially refer to issues of credibility and surety. The process of trust is intangible, complex, and confounding with challenges of certainty and verifiability, leading to ethical questions and implications. Marketers recognize that trust during an exchange facilitates decision making and is useful in commitment and relationships, but determining whether there are levels of trust or outcomes due to trust (the result of an interaction or several interactions) is challenging. Therefore, the result of interactions with limited certainty describes *faith* rather than trust, which is critical to addressing issues of consumer vulnerability and assurance. The SSIM distinguishes trust from faith on the basis of the level of certainty, or knowledge and belief based on evidence, existing in an information exchange (see Figure 2).

When there is a lack of certainty in that exchange, the other party is relegated to faith that the exchange will cause no harm now or in the future. That faith in the exchange and the resulting unpredictability means that information is being surrendered—consumers (and perhaps firms) are captive. Surrendering implies a lack of control, a lack of knowledge or attention to details, or a lack of certainty, which has implications for social responsibility between parties online and ethical behavior by firms, consumers, and government.

Regulation and Protection Behaviors: Active or Passive

Marketing research and knowledge has long been useful in consumer protection strategies and research. Andrews (2001) provides a framework describing how marketing knowledge has influenced public policy on consumer protection and details how marketing has made many theoretical contributions to consumer protection policy (in Bloom and Gundlach 2001). The goal of much of the multidisciplinary research on consumers and privacy is to understand an individual's privacy protection behaviors. Jones (1991) provides an overview of public concern for privacy, the origins of privacy rights, privacy protection, and industry self-regulation. Before the Internet and social networking sites were prevalent, Jones called for "balancing the needs of record keepers for information against the interest of consumers in protecting their privacy" (p. 145). Part of balancing those needs is disclosure, or what the White House, the FTC, and self-regulatory agencies refer to as transparency. In his 1962 Consumers' Bill of Rights, President John F. Kennedy indicated that consumers have the right to be informed, or the "right to know" (Kennedy 1962). Today's technology allows for easy access to knowledge but does not make the transparency and certainty necessary for consumers' right to know easy to acquire. Nonetheless, websites and social networking sites are required to provide details to consumers in a variety of ways (e.g., privacy policies, terms of service, opt-in/opt-out messages)

as to how their information from an exchange will be used, stored, and/or disseminated.

Protection behaviors are outlined here as two general states: active and passive. Active protection is when people place conditions on their information exchange, permitting or consenting to details of the exchange. Passive protection refers to the lack of conditions placed on an information exchange, when individuals behave as cognitive misers and do not pay attention to details and therefore simplify, or when they are unaware of the details of the exchange. Some researchers have taken a public policy stance on protection and consumerism (Aaker and Day 1971; Barksdale and Darden 1972; Cohen 1975; Foxman and Kilcoyne 1993; Roselius 1971), and some have examined information and education around consumer protection (Caudill and Murphy 2000; Cunningham and Cunningham 1976; Dommeyer and Gross 2003; Petty 2000; Stern 1967). Murphy and Wilkie (1990, p. 2) examined the "vague mandate" of the FTC and the regulatory efforts to provide "our nation with a marketplace that is both efficient and fair, for both consumers and firms." In general, consumer protection movements have focused on consumers in relation to product development and product information, but technological changes and the evolution of the Internet have focused dialogue and research on the collection and exchange of consumer information (Brill 2014; Goodwin 1991; Milne 2000; Nowak and Phelps 1995; Sachs 2009).

The issue of protection is increasingly critical because consumer privacy in online environments is often compromised or violated during information exchanges, whether information is given voluntarily or gathered without consumer knowledge (Milne 2000). The FTC realizes its future challenge to protect consumers' "personally identifiable and non-public information" in the online environment (FTC 2011, p. v). A 2012 White House report on consumer digital data privacy, protection, and trust makes it clear that "privacy protections are critical to maintaining consumer trust in networked technologies" (The White House 2012, p. i). Yet in reality, consumers are continuously partially attentive—they demonstrate cognitive miser behaviors and do not actively engage in protecting their information online, notwithstanding their concern for privacy.

The history of examining consumer behaviors to safeguard privacy and the need for consumers to take action to protect themselves includes control strategies such as Do Not Call lists and Opt-In Opt-Out information practices. In a study examining the antecedents of online protection behaviors, Milne and Rohm (2000, p. 229) find that "while consumers are becoming more cognizant of the dangers in providing information to online marketers without sufficient assurance, they still put themselves at risk by not taking technical precautions or fully understanding how a Web site might collect information." Regulatory challenges include helping firms and consumers protect financial data, ensuring general data transparency, providing notice and choice for consumers regarding their personal data, and removing identification elements from individual data (Brill 2013). Commissioner Brill (2013, p. 10) recommends a solution called "Reclaim Your Name" to "empower the consumer to find out how brokers are collecting and using data." Industry efforts over more than a decade have included concepts of permission marketing in which marketing strategies are designed to be anticipatory, personal, and relevant, with the permission of the consumer (Godin 1999). Nonetheless, attempts to enhance consumer protection behaviors require people to engage in active information processing in order to engage in protection behaviors. This is obviously a challenge when consumers are surrendering to technology.

In 2012, recognizing the risks inherent in information exchanges online, the White House introduced a Consumer Privacy Bill of Rights, building on John F. Kennedy's 1962 Consumer Bill of Rights. The report by the White House (2012) makes it clear that "the Consumer Privacy Bill of Rights provides general principles that afford companies discretion in how they implement them" and states that the goal is to allow for flexibility and innovation derived from consumer input (p. 2). It is evident that, on the surface, most of these rights (individual control, transparency, respect for context, security, access and accuracy, focused collection, and accountability) are prescriptive and meant to be flexible "rather than requiring companies to adhere to a single, rigid set of requirements" (p. 2). Indeed, the only overt rights provided to consumers are the right to exercise control over the personal data provided to companies and the right to access information and correct it for accuracy. Most of the privacy rights, such as transparency, respect for context, security, focused collection, and accountability place the onus of responsibility with consumer information on those gathering, storing, and disseminating information. However, the nature of exchanging information on the Internet between and among an abundant number of third parties is an important practical and ethical question for marketers and policy makers.

Furthermore, consumers have little time to exercise control, process, or place conditions on the extensive amount of information exchanged and often lack the effort required to benefit from these rights. It would be challenging to use technology to help move consumers from passive acquiescence to active protection; it is more probable that technology could be used to help marketers and policy makers operationalize these rights to address ethical concerns involved with surrendering information. Marketers and policy makers cannot simply provide more information through transparency but must simplify the protection efforts creating user-friendly regulatory and self-regulatory missives, educating consumers to avoid surrendering information.

Passive Protection Behavior: Unconditional Exchange of Information

Information available through transparency is useful when consumers are actively concerned and/or active in their protection behavior. Protection is not automatic: it requires consumers exposed to the information to decide whether to take action. If consumers do not find or read the information a company provides about privacy, they are not exposed to it. Many studies have addressed consumer knowledge of privacy related information, as I discuss next.

In a direct marketing study, Dommeyer and Gross (2003) build on a large body of research on privacy concern and consumer characteristics (Foxman and Kilcoyne 1993; Goodwin 1991; Milne 2000; Nowak and Phelps 1992, 1995; Petty 2000) to examine consumer knowledge of privacy-related

laws and practices and consumer awareness of strategies available to protect their privacy. Their findings show that consumers are not very knowledgeable about consumer privacy but are aware of privacy-protection strategies in a direct marketing setting, leading to the obvious conclusion that privacy controls need to be easy for consumers to implement. Although the authors conducted this study before the intense growth of the Internet as a context and tool for organizations and consumers, it provides evidence of passive privacy protection behavior. Simply having privacy knowledge does not ensure an active form of privacy protection by consumers, and surrendering to technology almost forces passivity. When purchasing a song online, most of the time people have to click only once if their payment information is provided (and often online businesses require payment information to have an account). Many consumers and organizations either are unaware of the conditions that exist to protect them on the Internet or are aware and simply do not use them much, if at all, as a result of their continuous partial attention. Even when individuals do place conditions on their information exchanges, the uncertainty and complexity in the environment makes employing protection behaviors challenging.

Other types of passive protection behaviors surround the use of privacy policies. As defined by the Electronic Privacy Information Center (EPIC), "[Online privacy] policies are disclaimers produced by a Web site, that become waivers once the users accept them. By accepting the terms of the policy (the conditions), the user volunteers to relinquish some known right or privilege they may have" (EPIC 2014, p. 9). Rifon, LaRose, and Choi (2005, p. 359) note, "Privacy policies are intended to provide information to consumers so that the consumer can control participation in the process." For the policy to be informative enough so that users can understand and accept the terms, it is vital that the policies be read and understood. However, EPIC (2014) also notes that privacy policies are difficult for users to find and read, and their online nature allows them to be changed or altered with no clear sign of how this fluidity of the policies influences consumers' trust and privacy behaviors. In this manner, consumer awareness of a privacy policy, or even consumer reading of the privacy policy, is also considered a passive form of privacy protection, one in which individuals make routine decisions that do not require a great deal of thought or involvement. When consumers are challenged to process the details of their exchange, they are unconditionally providing information (see Figure 2).

Milne and Culnan (2004) examine online privacy notices and their relationship to trust (operationalized as trust in the online privacy notice) to determine whether and why consumers read them. They find that reading online privacy notices relates to privacy concern, understanding of the notices, and trust in the actual online notice. Privacy notices are supposed to "reduce the risks of disclosing personal information online" (Milne and Culnan 2004, p. 15). The reduction of risks is a gain or loss decision for consumers, yet it is clear that consumers are unaware of the long-term risks and potential loss with regard to the information they share online. Indeed, in cases of sharing information, consumers treat privacy policies and terms of service agreements as barriers to the actual service or good they are attempting to access online (Luo 2002). Although efforts have been made

to make privacy notices user friendly (e.g. financial industry privacy forms), current privacy notices are incredibly detailed legalese designed to indemnify the firm, not protect the consumer. As research has shown, consumers often ignore these terms and policies, placing few if any conditions on the exchange, thus only passively protecting themselves. Thus, they provide information unconditionally.

As the use of the Internet has increased and the World Wide Web has moved from being solely informational to transactional, consumers' privacy and information about them has become a mounting concern for public policy researchers and government agencies alike. For example, Sheehan and Hoy (2000) investigate influences on consumer privacy online by utilizing the results of an FTC e-mail survey of U.S. online consumers. Their analysis finds that consumers are concerned about the relationships between entities and online users and the exchange of their personal information for compensation. Although consumers may be concerned, this does not mean that they will process all of the information and/or take the steps to actively protect themselves. They may believe that there is no point in doing so. More protections have been afforded younger generations, in the form of the 1998 Children's Online Privacy Protection Act, because youth are using the Internet in ways unfamiliar to older people (Prensky 2001).

> Millennials are different from past generations. . . . This group has been empowered by social networking and other forms of convenient, computer-enabled, and mobile communication capabilities. . . . They can "filter," timeslice, commoditize their attention, and synthesize information, yet they also have little regard for their own or other's online privacy. (McHaney 2011, p. xvii)

Marketers and policy makers have taken steps to protect young people online, yet youth are not the only consumers exchanging information online. Frequent breaches of information (e.g., Edward Snowden's breach of the National Security Agency) or hacking events affecting organizations such as Sony, the Federal Office of Personnel Management, Target, Heartbleed, and Twitter make it evident to consumers and firms that concern is warranted. In some cases, such incidents seem to have increased active protection behaviors online, influencing users to place conditions on the information exchange.

Active Protection Behavior: Conditional Exchange of Information

Milne (2000, p. 2) presents a general privacy research framework based on the influences on marketers and consumers that shape the information strategies both use to interact with each other. The resulting "Marketer-Consumer Information Interaction" framework provides a useful foundation for understanding privacy issues as well as how both marketers and consumers are influenced by technology and context, yet these interactions involving information only show two parties (the marketer and the consumer) in one type of information exchange (the provision and use of information) on the Internet.

> Marketers can use information to profile and personalize communications, which may result in more or less privacy. Consumers can follow safe (or unsafe) information practices and

employ (or not employ) technology to safeguard their information exchanges (Milne 2000, p. 3).

The evolution of technology has shifted this traditional view of information interactions. A dyadic view of the exchange does not take into account the increased number of third parties or the degrees of sharing and use over time. Information is not only shared by consumers with marketers and vice versa but also shared with third parties, fourth parties, and at times sold by a network of data brokers, invisible to the consumer, thus complicating the interaction and challenging the intent of transparency.

In 2013, Pew Research Center reported that 86% of adult Internet users occasionally take steps to remove or mask their digital footprints online, yet 68% also believe that current laws do not protect consumers enough on the Internet (Rainie, Smith, and Duggan 2013). Furthermore, half of Internet users report that they are worried about their personal information that is available online. The report concludes that "people would like control over their information," yet this control would be exercised after they provide the information. Notably, users who report that they use strategies to be less visible online were not asked about their use of privacy settings but were asked whether they cleared their browser history, deleted or edited information posted in the past, used a fake name, and other strategies employed to hide online.

The Pew report also notes that the concern for personal information available online increased by 33% since 2009. The report finds that "privacy is not an all-or-nothing proposition for Internet users" (p. 18) and attempts to differentiate concern from protection strategy. The active protection behaviors respondents take show that they are active in terms of protection strategies, yet these strategies are not necessarily associated with the sites directly. It is clear that some consumers are increasingly active in attempting to protect their information by deciding to take some kind of action, such as creating fictitious names/aliases when interacting online. However, some of their active protection behaviors may actually be reducing the ultimate credibility and certainty in current and future information exchanges. Many consumers are not using the protective tools that marketers and policy makers provide and instead are creating ways to simplify processing information.

Studies in computer technology and communication have examined consumer use and awareness of privacy settings (Fogel and Nehmad 2009; Stutzman, Gross, and Acquisti 2012). Findings from these disciplines have used Facebook as a domain for study and show that although people know about privacy settings on Facebook, they do not spend a great deal of time using the settings to protect themselves. Building on these findings, Debatin et al. (2009) discover that a majority of Facebook users understand what privacy settings entail and make use of them, but how that "use" is interpreted is unclear. Notably, Fogel and Nehmad (2009) find that social networking site users in general tend to have more risk-taking attitudes than those who are not on social networking sites. Thus, consumers are providing more information and using privacy settings, but how active they are in such use is not obvious. The use of privacy settings does demonstrate some level of active protection behavior, but using default privacy settings would be a level of privacy protection more passive in the continuum of protection behavior.

A longitudinal study of Facebook users provides an "unprecedented view of the long term evolution of privacy and disclosure behavior on a social network site" (Stutzman, Gross, and Acquisti 2012, p. 8). The authors examine privacy behavior on Facebook from 2005 through 2011, reporting that although privacy behaviors over time actually increased, people were also providing more personal information. This finding is perplexing. Active protection behaviors may actually sustain more faith in the exchange. Regardless of the effectiveness of protection behaviors, the SSIM describes that employing more protection behaviors means active protection, while employing fewer or no protection behaviors refers to passive protection.

The process of acquiring information for purchase decisions has always been of concern for marketers, but protection behaviors are also the result of acquiring information. Extant research findings illustrate the differences along the continuum and highlight the challenging roles for firms and consumers with the rapid pace of technology. Economists often view consumer information search as a cost–benefit proposition of searching for information, in which the cost to find information is offset by the benefits (Stigler 1961 in Beales, Craswell, and Salop 1981). Policy makers have "typically adopted the view that consumers will seek 'objective' information if the government acts to make it available" (Beales, Craswell, and Salop 1981, p. 11). Yet, as discussed previously, when too much information is available and consumers are unwilling or unmotivated to process this information, they surrender to technology, which leads to critical consumer protection issues.

Conclusions

If we're going to be connected, we need to be protected.
—President Barack Obama, January 12, 2015

The significance of this article is the assertion that the increasing use and reliance on technology is leading people to surrender much of their information online without consideration of the long-term effects. With the little time consumers have to devote the requisite attention to protect their privacy, the uncertainty created by unknown third parties involved in exchanges of information, and the constant change in technology, individuals (and organizations) face risk and vulnerability. This is a societal concern.

U.S. society has made it clear that the act of surrendering requires rules and guidelines. Article 2 of the U.S. military code of conduct clearly states, "I will never surrender of my own free will. If in command I will never surrender the members of my command while they still have the means to resist." Furthermore, Article 4 reads, "If I become a prisoner of war, I will keep faith with my fellow prisoners. I will give no information or take part in any action which might be harmful to my comrades." As a society, we clearly position surrendering as an undesirable scenario. Why then are we allowing our citizens to surrender so much information? The exchange, storage, and dissemination of consumer information in the digital age create ethical issues for marketers, policy makers, and society.

The phenomenon of surrendering to technology, along with the SSIM matrix, provides a much-needed macro perspective

of consumers and their online information exchanges to frame trust, transparency, and protection strategies for marketers and policy makers. Surrendering to technology means that consumers are not always investing the time and attention needed to process the abundance of information required to make informed decisions about information exchanges online, and they often act with continuous partial attention. This is a public policy issue that is currently and primarily addressed with efforts of regulation (e.g., legal action, fines) and self-regulation (e.g., training, certification[s], terms and conditions), yet these efforts are reactive, at best. I have demonstrated that transparency does not always mean clarity, nor does it necessarily enhance certainty. The goal of the SSIM is to move people from surrendering to technology to sharing with technology. Policies that (perhaps ironically) utilize technology to increase attention and allow for more clarity in information exchanges are imperative.

The SSIM not only sheds light on the vague aspects of trust and transparency but also demonstrates the paradigm shift required by firms, individuals, and government when it comes to trust and protection. Recognizing that consumers are exchanging information without conditions (i.e., reading the notifications, often without understanding the conditions) means that they are not only surrendering to technology but also surrendering information. There is a need to "allocate [consumer] attention efficiently among the overabundance of information sources that might consume [their attention]" (Simon 1971, p. 7). As Federal Trade Commissioner Brill strongly recommends, perhaps technology is not only the problem but also the solution to improving the certainty in online information exchanges and providing consumers the tools to recognize whether they are resisting or submitting when they exchange information online.

Transparency, as it is presently conceptualized, only offers consumers the illusion of control over their information—control that consumers do not always embrace. The storage capacities available, the myriad of third parties involved in exchanges of information, and the speed of technological change is outpacing self-regulatory and regulatory protection strategies, compounding the risk of unknown long-term consequences. This risk is also important for firms, as Awad and Krishnan (2006) find a "personalization privacy paradox" in which consumers who want more information transparency are less willing to be profiled for use in personalization in online advertising (p. 13). The authors also find that an "effective use of consumer information is a critical success factor for firms online" (p. 24). Ultimately, many consumers do not pay attention to the details of an information exchange even when firms have the intent of transparency. They may believe they are sharing information conditionally, when in fact they could be surrendering their information unconditionally.

Applying the SSIM: Verification and Education

The reality of social marketing is that consumers may not always want to, know how to, or care to protect themselves. The shift to "Web 3.0" postures to have a stronger consumer, human-centered focus, "where profitability is balanced with corporate responsibility" (Kotler, Kartajaya, and Setiawan

2010, p. 6). This values-driven goal for marketers means that it is imperative for them to embrace the social and societal responsibility associated with the concept of surrendering to technology and to encourage sharing rather than surrendering information.

Marketers and organizations should use the SSIM to enhance transparency and foster trust in a user-friendly fashion in two areas: verification and education. These should be utilized to increase the likelihood that consumers will begin sharing information—that is, to move consumers from the unconditional and surrender quadrants to the conditional and share quadrants. The goal of the SSIM is to make consumer interactions and exchanges online more transparent at a macro level. Marketers and public policy makers can also use the SSIM to inform consumers, in a clear and concise manner, of the level of risk and vulnerability they face in information exchanges.

Faith → Trust: Enhancing Verification

Regulatory and self-regulatory organizations can utilize the SSIM to develop default conditions for consumers, thus ensuring that consumers will not unconditionally surrender information and limit the spread of this information to unknown third parties. As previous research has shown, trust and transparency work best when certainty is assured. Verification strategies can be improved through the application in regulatory and self-regulatory efforts of what Rothschild (1999, p. 25) refers to as the "tripartite classification of education, marketing, and law," with an update to include technology. Regulatory efforts alone cannot offset the dilemma of surrendering to technology, and because "education can teach and create awareness about existing benefits but cannot deliver them," education alone is not enough (Rothschild 1999, p. 25). Regulatory policies and/or legislation should create defaults that take into account the reality that many consumers are surrendering information and that firms may be on an ethical slippery slope by encouraging this surrender. Legislation and public policy (keeping pace with technological changes) should ensure corporate and social responsibility with consumer information, allow for verification to protect consumers, and ultimately prevent ethical lapses by individuals and organizations.

Passive → Active Protection: Authentic Education

Marketers and policy makers can use education to inform and persuade people (1) that they are surrendering to technology, (2) how to avoid surrendering information, and (3) how to use other people's information ethically. Education should be utilized to enhance verification mechanisms, to increase knowledge that surrendering is an issue, and to create effective safety warnings to better prepare consumers to protect themselves. Surrendering information to technology requires "authentic education" in which marketers, consumers, and regulators collaborate with one another to encourage information sharing and discourage surrendering (Freire 1993, p. 74). The SSIM can be used to enhance prevention and promotion regarding the phenomenon of surrendering information to technology—it can increase awareness and distinction between trust and faith and encourage consumers to move from surrendering to sharing information.

SSIM Goal Flow: Sharing Information with Conditions

As noted previously, from a marketing and public policy perspective, the challenges identified in the matrix are present when individuals surrender to technology and when they exchange information unconditionally. Technology should be appropriated to increase the ease of access to verify where and how information is spread and used to encourage people to protect themselves through interactivity (e.g., "gamification"). In all, regulation, education, and technology should be used to improve verification and enhance trust, thus encouraging information sharing (vs. surrendering) and fostering proactive (vs. reactive) protection behaviors.

Next, I explain how these behaviors are specific to each quadrant, with the goal for marketers and public policy makers to encourage ethical and responsible online information exchanges, even with the challenges and realities associated with surrendering to technology. Trust and transparency cannot be relied on at face value to solve issues of privacy and security. The SSIM goal flow acknowledges that society faces an information blitz and focuses on guiding/directing consumers from faith to trust and from passive to active protection behaviors.

Conditional Share

In this quadrant, people are employing protection strategies (placing conditions on the information exchange) and verifying some or all of the information they exchange. This is the ideal quadrant for information exchanges online and should be the goal for marketers and public policy makers. With conditional share, people are willingly and knowingly exchanging information—they are paying attention, trusting in the exchange, and actively protecting themselves.

Unconditional Share

In this quadrant, people are employing few or no protection strategies, yet they are verifying some or all of the information they exchange. Marketers and public policy makers should focus on the ease of verification mechanisms and need for protection strategies through regulation and education, using technology to assist in the implementation of both.

Conditional Surrender

In this quadrant, people are employing some protection strategies but are not verifying much, if any, of the information they exchange. Marketers and public policy makers should acknowledge that there is faith in the exchange and should focus on gaining these users' attention through education and improving the ease of verification mechanisms and protection strategies through regulation and education, using technology to assist in the implementation.

Unconditional Surrender

This is the most concerning quadrant for marketers and public policy makers because it poses the largest ethical and societal challenge. Individuals exhibit only faith in the exchange and employ few or no protection strategies, not verifying much, if any, of the information they exchange. In addition, the surrendering-to-technology concept posits that this is the quadrant in which most consumers find themselves when exchanging information online. Marketers and public policy makers should focus on gaining these users' attention through

education and improving the ease of verification mechanisms and protection strategies through regulation and education, using technology to assist in the implementation. Web 3.0 demonstrates the imperative to move consumers from faith to trust in online information exchanges and to encourage conditions on these exchanges.

Implications: Sharing *with* or Surrendering *to* What and *for* How Long

Both the concept of surrendering to technology and the SSIM have several applications and implications for future empirical studies, consumers, marketers, and regulatory agencies. Use of the SSIM may involve identifying consumers (perhaps even through self-identification, for consumer educational purposes) and firms in each quadrant and generating potential strategies to move them to other quadrants. Another use of the SSIM includes applying it to various contexts of information exchange to determine whether certain populations or target markets are sharing or surrendering information. The SSIM can also be used in the application of protection strategies to employ for each quadrant. Although the verification and education strategies may vary by industry and sector, the goal flow of the SSIM is from surrender to share and from unconditional to conditional. Finally, the matrix can be utilized to try to understand the paradox of convenience and dissonance (cost–benefit) for consumers and marketers in their information exchanges. In general, the SSIM should be useful for guiding further research examining whether and how consumers are surrendering information to technology. This is an important societal and ethical issue for marketers and policy makers as the nature and pace of technology improves artificial intelligence and machine-to-machine interactions.

The Internet of Things will create a web of problems if marketers and policy makers do not keep pace. The subtle differences between trust and faith can be used in studies examining whether an individual or firm is actually displaying trust or faith and, if so, how the level of certainty varies, or how much certainty is necessary for a default level of trust that allows for sharing rather than surrendering. Acknowledging realities in active-passive protection will continue to help privacy researchers and practitioners identify which types of protection strategies are best to employ, as well as the pertinent details to present. The SSIM also provides government and policy researchers an evaluative instrument for existing recommended and employed protection strategies. Currently, private and public firms are predominantly focused on the short-term implications of online information exchange. Surrendering information to technology is a long-term ethical problem for individuals and society as a whole, but it can be mediated if marketing and public policy makers implement authentic education and effective regulation to increase attention and reduce uncertainty.

References

Aaker, David A. and George S. Day (1971), *Consumerism*. New York: Simon and Schuster.

Anderson, Chris (2009), *Free: The Future of a Radical Price*. New York: Random House.

Andrews, Craig (2001), "The Use of Marketing Knowledge in Formulating and Enforcing Consumer Protection Policy," in

Handbook of Marketing and Society, Paul N. Bloom and Gregory T. Gundlach, eds. Thousand Oaks, CA: Sage Publications, 1–33.

Anthes, Gary H. (1996), "In Web E-Trust: Label Will Certify Sites for Security and Privacy," *Computerworld*, 30 (47), 71–72.

Awad, Naveen Farag and M.S. Krishnan (2006), "The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization," *Management Information Systems Quarterly*, 30 (1), 13–28.

Baker, Stacey Menzel (2009), "Vulnerability and Resilience in Natural Disasters: A Marketing and Public Policy Perspective," *Journal of Public Policy & Marketing*, 28 (Spring), 114–23.

———, James W. Gentry, and T.L. Rittenburg (2005), "Building Understanding of the Domain of Consumer Vulnerability," *Journal of Macromarketing*, 25 (2), 128–39.

Barksdale, Hiram C. and William R. Darden (1972), "Consumer Attitudes Toward Marketing and Consumerism," *Journal of Marketing*, 36 (October), 28–35.

Beales, Howard, Richard Craswell, and Steven C. Salop (1981), "Efficient Regulation of Consumer Information," *Journal of Law & Economics*, 24 (3), 491–539.

Bloom, Paul N. and Gregory T. Gundlach, eds. (2001), *Handbook of Marketing and Society*. Thousand Oaks, CA: Sage Publications.

Brill, Julie (2013), "Reclaim Your Name," keynote address at the 23rd Computers Freedom and Privacy Conference, Washington, DC.

——— (2014), "The Internet of Things: Building Trust and Maximizing Benefits Through Consumer Control," keynote address at Fordham University School of Law Center on Law and Information Policy Conference "What Is Your Car Saying to Your Shoes? Assessing the Internet of Things," (March 14), [available at https://www.ftc.gov/public-statements/2014/03/internet-things-building-trust-maximizing-benefits-through-consumer].

Caudill, Eve M. and Patrick E. Murphy (2000), "Consumer Online Privacy: Legal and Ethical Issues," *Journal of Public Policy & Marketing*, 19 (Spring), 7–19.

Chandler, Jennifer D. and Stephen L. Vargo (2011), "Contextualization and Value-in-Context: How Context Frames Exchange," *Marketing Theory*, 11 (1), 35–49.

Cohen, Dorothy (1975), "Remedies for Consumer Protection: Prevention, Restitution or Punishment," *Journal of Marketing*, 39 (October), 24–31.

Cunningham, William H. and Isabella C. Cunningham (1976), "Consumer Protection: More Information or More Regulation?" *Journal of Marketing*, 40 (April), 63–68.

Day, George S. and David B. Montgomery (1999), "Charting New Directions for Marketing," *Journal of Marketing*, 63 (October), 3–13.

Debatin, Bernhard, Jennette P. Lovejoy, Ann-Kathrin Horn, and Brittany Hughes (2009), "Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences," *Journal of Computer-Mediated Communication*, 15, 83–108.

Derakhshani, Delara and Ellen Bloom (2005), "Leap of Faith: Using the Internet Despite the Dangers," research report, Princeton Survey Research Associates International, (October 26), (accessed March 4, 2016), [available at http://consumersunion.org/research/leap-of-faith-using-the-internet-despite-the-dangers/].

Direct Marketing Association (2014), "Direct Marketing Association's Guidelines for Ethical Business Practice," online handout, (accessed December 5, 2014), [available at http://thedma.org/wp-content/uploads/DMA_Guidelines_January_2014.pdf].

Dommeyer, Curt J. and Barbara L. Gross (2003), "What Consumers Know and What They Do: An Investigation of Consumer Knowledge, Awareness, and Use of Privacy Protection Strategies," *Journal of Interactive Marketing*, 17 (2), 34–51.

Dragland, Âse (2013), "Big Data – for Better or Worse," SINTEF, (May 22), (accessed March 4, 2016), [available at https://www.sintef.no/en/news/big-data–for-better-or-worse/].

EPIC (2014), "Social Networking Privacy Report," (accessed May 24, 2014), [available at http://epic.org/privacy/socialnet/].

Fiske, Susan T. and Shelley E. Taylor (1991), *Social Cognition*, 2nd ed. New York: McGraw-Hill.

Fogel, Joshua and Elham Nehmad (2009), "Internet Social Network Communities: Risk Taking, Trust, and Privacy Concerns," *Computers in Human Behavior*, 25 (1), 153–60.

Foxman, Ellen R. and Paula Kilcoyne (1993), "Information Technology, Marketing Practice, and Consumer Privacy: Ethical Issues," *Journal of Public Policy & Marketing*, 12 (Spring), 106–19.

Freire, Paulo (1993), *Pedagogy of the Oppressed*. New York: The Continuum Publishing Company.

Friedman, Thomas (2006), "The Age of Interruption," *New York Times*, (July 6), (accessed March 16, 2016), [available at http://www.nytimes.com/2006/07/05/opinion/05friedman.html].

FTC (2011), "FTC Performance and Accountability Report Fiscal Year 2011," press release, (November 17), (accessed March 11, 2016), [available at https://www.ftc.gov/sites/default/files/documents/reports_annual/performance-and-accountability-report/2011parreport.pdf].

——— (2014), "Data Brokers: A Call for Transparency and Accountability," FTC Report, (May), [available at http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf].

Godin, Seth (1999), *Permission Marketing: Turning Strangers into Friends and Friends into Customers*. New York: Simon and Schuster.

Goodwin, Cathy (1991), "Privacy: Recognition of a Consumer Right," *Journal of Public Policy & Marketing*, 10 (Spring), 149–66.

Gundlach, Gregory T. and Joseph Cannon (2009), "'Trust but Verify'? The Performance Implications of Verification Strategies in Trusting Relationships," *Journal of the Academy of Marketing Science*, 38, 399–417.

Houston, Franklin S. and Jule B. Gassenheimer (1987), "Marketing and Exchange," *Journal of Marketing*, 51 (October), 3–18.

Jones, Mary Gardiner (1991), "Privacy: A Significant Marketing Issue for the 1990s," *Journal of Public Policy & Marketing*, 10 (Spring), 133–48.

Kennedy, John F. (1962), "Special Message to the Congress on Protecting Consumer Interest," speech, (March 15), (accessed March 4, 2016), [available at http://www.jfklibrary.org/Asset-Viewer/Archives/JFKPOF-037-028.aspx].

Kotler, Philip, Hermawan Kartajaya, and Iwan Setiawan (2010), *Marketing 3.0: From Products to Customers to the Human Spirit*. Hoboken, NJ: John Wiley & Sons.

——— and Ravi Singh (2001), "Marketing Warfare in the 1980s," in *Marketing: Critical Perspectives on Business and Management*, Vol. 3. New York: Taylor & Francis, 411–28.

Luo, Xueming (2002), "Trust Production and Privacy Concerns on the Internet: A Framework Based on Relationship Marketing and Social Exchange Theory," *Industrial Marketing Management*, 31 (2), 111–18.

MacInnis, Deborah J., Christine Moorman, and Bernard J. Jaworski (1991), "Enhancing and Measuring Consumers' Motivation, Opportunity, and Ability to Process Brand Information from Ads," *Journal of Marketing*, 55 (October), 32–53.

McHaney, Roger (2011), *The New Digital Shoreline: How Web 2.0 and Millennials are Revolutionizing Higher Education*. Sterling, VA: Stylus Publishing.

McLuhan, Marshall (1964), *Understanding Media: The Extensions of Man*. New York: Dresden.

Milne, George R. (2000), "Privacy and Ethical Issues in Database/Interactive Marketing and Public Policy: A Research Framework and Overview of the Special Issue," *Journal of Public Policy & Marketing*, 19 (Spring), 1–6.

——— and Mary J. Culnan (2004), "Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices," *Journal of Interactive Marketing*, 18 (3), 15–29.

——— and Andrew J. Rohm (2000), "Consumer Privacy and Name Removal Across Direct Marketing Channels: Exploring Opt-In and Opt-Out Alternatives," *Journal of Public Policy & Marketing*, 19 (Fall), 238–49.

Morgan, Robert and Shelby D. Hunt (1994), "The Commitment-Trust Theory of Relationship Marketing," *Journal of Marketing*, 58 (July), 20–38.

Morozov, Evgeny (2011), *The Net Delusion: The Dark Side of Internet Freedom*. New York: PublicAffairs.

Murphy, Patrick E., Gene Laczniak, and G. Wood (2007), "An Ethical Basis for Relationship Marketing: A Virtue Ethics Perspective," *European Journal of Marketing*, 41 (1/2), 37–57.

——— and William L. Wilkie (1990), *Marketing and Advertising Regulation: The Federal Trade Commission in the 1990s*. South Bend, IN: University of Notre Dame Press.

Nowak, Glen J. and Joseph E. Phelps (1992), "Understanding Privacy Concerns: An Assessment of Consumers' Information-Related Knowledge and Beliefs," *Journal of Direct Marketing*, 6 (November), 28–39.

——— and ——— (1995), "Direct Marketing and the Use of Individual-Level Consumer Information: Determining How and When 'Privacy' Matters," *Journal of Direct Marketing*, 9 (3), 46–60.

Pavlou, Paul A. (2003), "Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model," *International Journal of Electronic Commerce*, 7 (3), 101–34.

Petty, Richard E. and John T. Cacioppo (1986), *The Elaboration Likelihood Model of Persuasion*. New York: Springer.

Petty, Ross D. (2000), "Marketing Without Consent: Consumer Choice and Cost, Privacy, and Public Policy," *Journal of Public Policy & Marketing*, 19 (Spring), 42–53.

Pew Research Center (2014), "Internet Project Survey: Mobile Technology Fact Sheet," (accessed January 3, 2015), [available at http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/].

Postman, Neil (1992), *Technopoly: The Surrender of Culture to Technology*. New York: Vintage Books.

Prensky, Marc (2001), "Digital Natives, Digital Immigrants Part 1," *On the Horizon*, 9 (5), 1–6.

Rainie, Lee, Aaron Smith, and Maeve Duggan (2013), "Coming and Going on Facebook," research report, Pew Research Center, (February 5), (accessed March 4, 2016), [available at http://www.pewinternet.org/2013/02/05/coming-and-going-on-facebook].

Rifon, Nora J., Robert LaRose, and Sejung Marina Choi (2005), "Your Privacy Is Sealed: Effects of Web Privacy Seals on Trust and Personal Disclosures," *Journal of Consumer Affairs*, 39 (2), 339–62.

Roselius, Ted (1971), "Consumer Rankings of Risk Reduction Methods," *Journal of Marketing*, 35 (January), 56–61.

Rothschild, Michael L. (1999), "Carrots, Sticks, and Promises: A Conceptual Framework for the Management of Public Health and Social Issue Behaviors," *Journal of Marketing*, 63 (October), 24–37.

Sachs, Benjamin R. (2009), "Consumerism and Information Privacy: How Upton Sinclair Can Again Save Us from Ourselves," *Virginia Law Review*, 95 (March), 205–52.

Sheehan, Kim Bartel and Mariea Grubbs Hoy (2000), "Dimensions of Privacy Concern Among Online Consumers," *Journal of Public Policy & Marketing*, 19 (Spring), 62–73.

Simon, Herbert A. (1971), "Designing Organizations for an Information-Rich World," *Computers, Communication, and the Public Interest*, Martin Greenberger, ed. Baltimore: Johns Hopkins University Press, 37–72.

——— (1972), "Theories of Bounded Rationality," *Decision and Organization*, 1 (1), 161–76.

Small, G. and G. Vorgan (2008), "Meet Your iBrain," *Scientific American Mind*, 19 (5), 42–49.

Smith, Aaron (2014), "What Internet Users Know about Technology and the Web," research report, Pew Research Center, (November 25), (accessed March 4, 2016), [available at http://www.pewinternet.org/files/2014/11/PI_Web-IQ_112514_PDF.pdf].

Steele, Robert David (2012), *The Open-Source Everything Manifesto: Transparency, Truth, and Trust*. Berkeley, CA: North Atlantic Books.

Stern, Louis L. (1967), "Consumer Protection via Increased Information," *Journal of Marketing*, 31 (April), 48–52.

Stigler, George J. (1961), "The Economics of Information," *Journal of Political Economy*, 69 (3), 213–25.

Stone, Linda (2007), "The Harvard Business Review List of Breakthrough Ideas for 2007: Living with Continuous Partial Attention," *Harvard Business Review*, 85 (2), 28–29.

———, "Continuous Partial Attention," lindastone.net, (accessed July 2, 2015), [available at http://lindastone.net/qa/continuous-partial-attention].

Stutzman, Fred, Ralph Gross, and Alessandro Acquisti (2012), "Silent Listeners: The Evolution of Privacy and Disclosure on Facebook," *Journal of Privacy and Confidentiality*, 4 (2), 7–41.

TRUSTe (2014), "U.S. Consumer Confidence Privacy Report: Consumer Opinion and Business Impact," research report, (accessed March 4, 2016), [available at http://www.theagitator.net/wp-content/uploads/012714_ConsumerConfidenceReport_US1.pdf].

Tversky, Amos and Daniel Kahneman (1974), "Judgment Under Uncertainty: Heuristics and Biases," *Science*, 185 (4157), 1124–31.

Westin, Alan F. (2003), "Social and Political Dimensions of Privacy," *Journal of Social Issues*, 59 (2), 431–53.

The White House (2012), "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy," (February), (accessed March 3, 2016), [available at http://www.whitehouse.gov/sites/default/files/privacy-final.pdf].

Wolff, Kurt H. (1976), *Surrender and Catch: Experience and Inquiry Today*, Vol. 1. Dordrecht, The Netherlands: D. Reidel Publishing.

Zucker, Lynne G. (1986), "Production of Trust: Institutional Sources of Economic Structure, 1840–1920," *Research in Organizational Behavior*, 8, 53–111.