J Bus Ethics (2016) 137:551–569
DOI 10.1007/s10551-015-2565-9

Understanding Privacy Online: Development of a Social Contract Approach to Privacy

Kirsten Martin

Received: 12 June 2014 / Accepted: 2 February 2015 / Published online: 19 February 2015

Abstract Recent scholarship in philosophy, law, and information systems suggests that respecting privacy entails understanding the implicit privacy norms about what, why, and to whom information is shared within specific relationships. These social contracts are important to understand if firms are to adequately manage the privacy expectations of stakeholders. This paper explores a social contract approach to developing, acknowledging, and protecting privacy norms within specific contexts. While privacy as a social contract—a mutually beneficial agreement within a community about sharing and using information—has been introduced theoretically and empirically, the full impact on firms of an alternative framework to respecting the privacy expectations of stakeholders has not been examined. The goal of this paper is to examine how privacy norms develop through social contract's narrative, to redescribe privacy violations given the social contract approach, and to critically examine the role of business as a contractor in developing privacy norms. A social contract narrative dealing specifically with issues of privacy is an important next step in exploring a social contract approach to privacy. Here, the narrative is used to explain to analyze the dynamic process of privacy norm generation within particular communities. Based on this narrative, individuals within a given community discriminately share information with a particular set of obligations in mind as to who has access to the information and how it will be used. Rather than giving away privacy, individuals discriminately share information within a particular community and with norms governing the use of their information. Similar to contractual business ethics' impact on global commerce in explaining how and why norms vary across global contexts, the social contract approach to privacy explains how and why norms vary across communities of actors. Focusing on agreements around privacy expectations shifts the responsibility of firms from adequate notification to the responsibility of firms as contractors to maintain a mutually beneficial and sustainable solution.

Keywords Privacy · Online · Social contract · Fair Information Practices · Internet · Technology

Consider three illustrative privacy issues online:

(1) Through 'Sponsored Stories,' Facebook users who clicked on 'like' buttons had pictures of themselves with an endorsement sent to their friends in a what looked like sponsored advertising (Kravets 2012).
(2) The travel site Orbitz tracks how users arrived at their site in order to prioritize search results: if a user arrived at Orbitz from a competitor's site, Orbitz may prioritize results based on price (Mattioli 2012). Similarly, Facebook mines users' browser history in order to target advertising.
(3) Verizon offers a service—Precision Market Insights—to business customers to mine Verizon's customer call and web browsing information in order to map where people are located and the types of services they purchase and use (Hill 2012). In an aptly titled article: "Verizon Very Excited That It Can Track Everything Phone Users Do And Sell That To Whomever Is Interested," Kashmir Hill outlines the service Verizon offers to business' to

K. Martin (✉)
Department of Strategic Management and Public Policy, George Washington University School of Business, 2201 G Street, NW Duquès Hall, Washington, DC 20052, USA
e-mail: martink@gwu.edu

Table 1 Ethical implications of privacy approaches

Privacy approach and JBE scholarship	Privacy defined as	Ethical implications
Access view Bonner (2007), Rowan (2000), Manning (1997), Miller and Weckert (2000), Brown (1996), Charters (2002), and Persson and Hansson (2003)	"right to be left along" (Peslak 2005, p. 329)	Respondents who disclose or give access to information are seen as *not* valuing privacy (e.g., Acquisti and Grossklags 2005). Since no privacy expectations exist after the disclosure of information, firms mistakenly believe or are told that no obligations to 'respect' privacy exist post-disclosure. Intrusions or violations of privacy are then 'justified: For example, monitoring of calls at work is seen as a violation but ethical (Persson and Hansson 2003)
Control/FIP Hsu and Kuo (2003), Angst (2009), Roman and Cuestas (2008), Lally (1996), Shaw (2003), and Alder et al. (2007)	"the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (Pollach 2005, p. 222)	Individuals are seen as controlling information through the informed consent within Fair Information Practices (FIPs). Individuals are responsible to understand the FIP of the firm through notice and choice. Firms have an incentive to only notify—no matter how outrageous the practice (Martin 2013)
Context-dependent norms (Privacy as a social contract) For example, Brown (1996), Cranford (1998), Introna and Pouloudi (1999), and Martin (2012)	"negotiated information norms within a particular community or situation" (Martin 2012, p. 520)	Information flow that is ethical meets privacy expectations by definition. For example, drug testing meets the requirements of contextual integrity, is ethical, and is not a privacy violation (Cranford 1998). Ethicists examine "what constitutes privacy concerns…and what they feel privacy is" (Kyo et al. 2007), and firms would be asked to take a more inductive approach to identifying privacy expectations

track their potential customers: "we [Verizon] understand what our customers' daily activity stream is…," and Verizon sells that activity stream to their commercial customers.

In each case, individuals willingly divulged information—clicked like, visited a travel site, watched a basketball game in a stadium—yet held different privacy expectations within the different contexts. For example, location information is expected to be used and tracked from a travel website (Martin and Shilton 2015); yet it is a surprise when information is used to track movement to and from a basketball game. Individuals share preferences with some friends—but not all. Users' different norms and expectations across contexts has been a source of frustration to firms and academics alike.

To explain variances in privacy expectations, previous work relies on a static, universal definition of privacy expectations and measures differences in individuals' concerns, attitudes, or valuations of privacy as illustrated in Table 1. In privacy scholarship, the access-view of privacy suggests that individuals have a reasonable expectation of privacy so long as they and their information are inaccessible or hidden (Warren and Brandeis 1890; Elgesem 1999; Persson and Hansson 2003; Schoeman 1984; Posner 1981). Online, the access-view would categorize the act of sharing information as necessarily giving up any expectation of privacy. When individuals use a phone, watch a basketball game, or click 'like,' individuals are seen as not having privacy expectations because all of the information was accessible. The question then becomes, 'why did the users divulge the information *at all?*'

Alternatively, the control-view of privacy (Westin 1967; Alder et al. 2007; Margulis 1977; Altman 1975; Moor 1997) suggests that relinquishing control of information to another party renders the individual without any reasonable expectation of privacy. Online, the control-view of privacy is regulated through adequate notice and choice in Fair Information Practices (FIPs; Bennett 1992; Ashworth and Free 2006; Peslak 2005; Culnan and Armstrong 1999; Bowie and Jamal 2006). FIPs allow for the contemporaneous disclosure of information and respect of privacy norms while online.[1] Although popular, notice and choice statements may be immaterial—or nonfactors—to

[1] See Federal Trade Commission (2012a, b) "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policymakers", Federal Trade Commission's Fair Information Practice Principles, and the White House's Consumer Data Privacy in a Networked World (February 2012).

assessments about the appropriateness and inappropriateness of the information transmitted within a particular context. In fact, each of the three examples was argued to comply with the written privacy notices, and users agreed to the notice upon engaging with the service; yet, all three examples caused privacy advocates to bring lawsuits or provided the impetus for articles exposing the firms' behavior. In other words, individuals, employees, users, and consumers make judgments about privacy expectations and violations regardless of the notice and choice policy in many situations.

Recent work on privacy suggests that privacy norms can be viewed as mutually beneficial and sustainable agreements within a community (Martin 2012) or as context-dependent norms (Nissenbaum 2004, 2009). These social contracts are the unstated agreements that individuals and groups make in contexts, communities, and relationships. Studies also substantiate the theory: 71 % of respondents would disclose within an established relationship (Louis Harris and Associates and Westin 1997; Culnan and Bies 2003), and individuals within a particular community, such as teams or young adults, develop substantive privacy norms not easily recognized or understood by outsiders (Martin 2012; Turow et al. 2009). In other words, individuals give access to information within a particular context with an understanding of the privacy rules that govern that context.

Understanding the factors that drive mutually beneficial and sustainable privacy norms within communities is important to firms in order to best meet the privacy expectations of stakeholders such as consumers, users, and employees.[2] Not only does meeting consumer privacy expectations increase purchase intentions and consumers' likelihood to transact with a firm (Cases et al. 2010; Eastlick et al. 2006), but meeting consumer privacy expectations also increases trust in a firm (McCole et al. 2010), while violating privacy expectations leads to adverse consumer reactions (Miyazaki 2009). Importantly for business ethicists, privacy violations are experienced as individual harms (Calo 2011) and as unfair acts (Ashworth and Free 2006).

While privacy as a social contract—a mutually beneficial agreement within a community about how information is used and shared—has been introduced theoretically (Culnan and Bies 2003) and empirically (Martin 2012), the full impact on firms of an alternative framework to respecting the privacy expectations of users, consumers, and employees has not been examined. Importantly for researchers and firms, questions remain about how to identify microsocial contract norms about privacy and what is taken into consideration in forming those privacy norms.

This paper further develops a social contract approach to generating, acknowledging, and protecting privacy norms within specific contexts (Martin 2012). The goal of this paper is to examine how information norms develop through a social contract narrative, to reframe possible privacy violations of business given the social contract approach to privacy, and to critically examine the role of business as a contractor in developing privacy norms. The social contract approach "need not—and seldom does—eliminate all questions from a moral quandary. But it can provide logical vantage points from which to view an ethical quandary and, in turn, point towards a solution" (Donaldson and Dunfee 2003, p. 115).

Understanding the underpinnings of social contract privacy norms will allow researchers and practitioners to identify the factors driving privacy expectations. Based on this narrative, individuals within a given community discriminately share information with a particular set of obligations in mind as to who has access to the information and how it will be used. In other words, rather than giving away privacy, individuals discriminately share information within a particular community and with norms governing the use of their information. Most importantly for business and business ethics, privacy as a social contract shifts the focus from gaining the consent from the user, individual, employee, or consumer to the responsibilities of the firm as a contractor to maintain a mutually beneficial and sustainable solution. The beginning of this move can be seen in online sites and applications, such as diaspora,* TOR, DuckDuckGo, and YikYak, which place understanding and meeting the privacy expectations of users as part of their value proposition.

This paper proceeds as follows.

- First, the social contract approach to privacy is explored by connecting privacy scholarship with existing social contract theory within business ethics—namely, Integrative Social Contracts Theory (ISCT).
- Second, I examine the social contract narrative specifically around privacy; this social contract construct grounds microsocial contract privacy norms as the natural outgrowth of individuals living in a community. The narrative offered here suggests that individuals have an interest in *discriminately sharing information* within a particular community and helps explain the factors that contractors take into consideration in forming privacy expectations.
- Third, online privacy violations are redescribed given the social contract approach to privacy to better understand how seemingly disparate privacy violations (Solove 2006) are related through a social contract approach to privacy.

[2] In the words of social contract theorists, communities are best able to develop moral fabric supportive of efficiency and pre-existing community values (Donaldson and Dunfee 1999). I wish to thank Tom Donaldson for making this point.

- Fourth, I discuss the implications of the social contract approach to privacy and the social contract narrative for the alternative theories of privacy, which are neither descriptively valid nor prescriptively useful.
- Finally, I critically examine the role of business as a contractor in developing privacy norms and outline implications of a social contract approach to privacy on management research and practice in the implications and conclusion.

Privacy as a Social Contract

While a social contract approach to privacy has been suggested generally, here I examine what privacy as a social contract would entail within business ethics and ISCT before developing the social contract narrative.

Previous Links Between Privacy and Social Contract Theory

A growing body of theoretical scholarship has focused on privacy as contextually defined, where privacy norms are defined and examined within a specific set of relationships, situations, or contexts (Nissenbaum 2004, 2009; Solove 2006; Martin 2012; Stutzman and Hartzog 2012; Moor 1997; Jiang et al. 2002). Within these contextually defined privacy approaches, what is and is not private is dependent on relationships, actors, information, and context (Nissenbaum 2004, 2009; Solove 2006; Grimmelmann 2010; Tufekci 2008a, b; Sloan and Warner 2013). The rules used to develop privacy norms vary across contexts; therefore violations of privacy occur when these negotiated, context-dependent rules are broken.[3]

Contextually dependent or relationship-dependent approaches to privacy, where privacy rules are negotiated and evolve within particular contexts or relationships, mirror a social contract approach to norms (Martin 2012). For example, privacy as contextual integrity suggests that privacy is respected when an information exchange meets the privacy norms of a context or a community of actors. These norms include not only the type of information expected, but also who will be able to see and use the information as well as the transmission principles associated with the information (Nissenbaum 2009). Similarly, social contract theory suggests that behavior, such as economic transactions or exchanges of information (Martin 2012), that reside within a community and whose effects reside within the community's should be governed by the communities' locally negotiated norms.

Social Contract Theory in Business Ethics

Within business ethics, the conversation around social contract theory centers on Donaldson and Dunfee's ISCT (1994, 1995, 1999) and Heugens et al.'s Contractualist Business Ethics (2006).[4] While research has focused less on the application of ISCT and more on the philosophical underpinnings of ISCT (Heugens et al. 2006, p. 729), ISCT has been utilized to explore particular ethical issues previously (Dunfee 2006, p. 313) including financial reporting and governance (Campbell et al 2003), marketing (Dunfee et al. 1999), lying (Ross and Robertson 2000), deviance in organizations (Warren 2003), marketing credit to college students (Lucas 2001), and Internet adoption in the Arab world (Loch et al. 2003).

Of particular relevance to privacy, ISCT delineates two types of agreements, as cogently described by Donaldson and Dunfee (1999). First, a *macrosocial contract* sets up the space for individuals to develop rules of engagement—including privacy norms—within a particular community. Local communities are more than simply two-party relationships. A *community* is a "self-defined, self-circumscribed group of people who interact in the context of shared tasks, values, or goals and who are capable of establishing norms of ethical behavior for themselves" (Donaldson and Dunfee 1999, p. 262). Marriages, friends, teams, work groups, organizations, and organization–stakeholder relationships develop privacy norms particular to their community.

Second, contractors create and negotiate *microsocial contracts* within the community in order to resolve issues and place constraints on behavior. For example, Verizon's collection of phone record data—the metadata of every phone call including the caller, recipient, phone number, duration, and (possibly) the GPS location information, would be within a microsocial contract between contractors (users) and Verizon would be expected to respect those privacy expectations with their customers regardless of the

[3] This negotiation over privacy norms is not synonymous with privacy as a commodity (Smith et al. 2011), a privacy calculus (Culnan and Armstrong 1999; Dinev and Hart 2006), or a second exchange (Culnan and Bies 2003), all of which assume individuals *relinquish* privacy in order to gain something in return. In other words, individuals are seen as giving up some measure of privacy to benefit from a transaction (e.g., customizing products or using electronic health records or having books suggested online). In this paper, the negotiation is over the privacy norm function: actors within a context negotiate what the privacy rules will be while retaining every expectation of privacy. See also Martin (2013).

[4] A social contract approach has previously been applied to delineate norms across geographical boundaries (Donaldson and Dunfee 1995), distribute goods (Walzer 1983), assign property rights (Coase 1960), or develop a system of right and wrong (Dennett 1995, 2003). Here, the social contract approach is employed to understand how privacy norms are formed within particular communities.

substance of the notice in the user agreement. Similarly, Facebook users have expectations as to who sees their information and how it is used (Martin 2011) regardless of the privacy notices—including how user information is manipulated for experiments (Albergotti 2014b). Empirically, respondents within a particular community have a better understanding of the privacy norms than outsiders (Martin 2012).

ISCT allows for locally negotiated microsocial contracts as well as the universal principles that transcend communities. The communities are afforded the moral free space to generate community-specific moral rules consistent with their members' preference and experiences (Donaldson and Dunfee 1999, p. 83; Dunfee 2006, p. 315). However, these communities must abide by procedural *hypernorms* of consent—usually manifest through the right of contractors to have voice and to exit. Microsocial contracts are only legitimate if the agreements conform to the procedural hypernorms of consent, voice, and exit; and, microsocial contracts around privacy norms only bind contractors if the agreements are legitimate (Donaldson and Dunfee 1999).[5]

Allowing privacy rules to vary based on the community or relationship mirrors expectations of privacy in the world. Similar to contractual business ethics' impact on global commerce in explaining how and why norms may vary across global contexts (Donaldson and Dunfee 1994; Van Oosterhout and Heugens 2009), the social contract approach to privacy explains how and why norms may vary across communities of actors with important implications to research and practice.

Social Contract Narrative for Privacy

An important next step in exploring a social contract approach to privacy is the social contract narrative. The narrative can justify the moral rightness of a principle, explain the social and institutional fabric of a society (e.g., Nozick 1974), or explain the emergence, persistence, or stability of an extant social contract (Heugens et al. 2006). Here, a midlevel social contract narrative is used to explain and analyze the dynamic process of privacy norm generation within particular communities.[6] Table 2 illustrates the social contract narrative applied here.

The first step in walking through a social contract narrative is to specify an initial position. This position is a priori any agreement between parties and provides the setting for reasonable contracting where individuals are assumed to have (1) an initial state and (2) behavioral tendencies. This first step provides the setting to create an agreement and asks not only *what privacy norms would contractors agree to* but also *what do contractors take into consideration?* For firms and business ethicists, the output of this narrative will provide key facets of the microsocial contracts about privacy and the factors that contractors—such as users, consumers, and employees—take into considerations in developing privacy norms.

Initial Position

For an initial state, one would need to imagine a world where individuals have no communication or interaction with others and are in a state where information can easily remain inaccessible. Individuals in this initial state would live and work by themselves and maintain their living environment independently. Privacy, in such a world, only requires that individuals keep a solitary existence and not give access to their information to anyone. In this position, the individual is able to maintain privacy by remaining alone and hidden. This initial state would constitute a scattering of recluses.

In fact, this initial state remains a theme throughout privacy scholarship in that individuals continue to have an interest in being inaccessible to others by remaining isolated both physically and psychologically. The right to be left alone (Warren and Brandeis 1890) preserves liberty and autonomy as individuals are free to "develop personalities, goals, ideas, and the right to determine to whom their thoughts, emotions, sentiments, and tangible products are communicated" (Bloustein 1964, p. 18). Such a state of solitary inaccessibility corresponds to defining privacy as the ability to restrict access to personal information (e.g., Allen 1988) or as protection from information gathering (Tavani and Moor 2001). Privacy as restricted access prevents people from knowing certain things and implies entering the public sphere to require giving up a measure of privacy (Alfino and Mayes 2006). According to the

[5] All members, even dissenting members, are obligated to abide by the authentic microsocial contracts based not only on their explicit or implicit consent when entering the community (Dunfee et al. 1999) but also out of obligations of fairness (Phillips 1997). Contractors are beholden to each other given the terms of these microsocial contracts and obligated as a community to uphold the procedural hypernorms of consent, exit, and voice (Donaldson and Dunfee 1999). For example, illegitimate microsocial contracts would not be binding, e.g., a microsocial contract that includes reading the personal email of everyone of a particular age or gender or race. Such a microsocial contract would violate the hypernorm of nondiscrimination and would render the microsocial contract illegitimate. I wish to thank Tom Donaldson for this example.

[6] From an initial position, the narrative results in an agreement that includes only those social constraints to human action that have normative appeal—agreements that "reasonable agents could, and arguably would, agree to if they had the choice" (Heugens et al. 2003, p. 11). The narrative illustrates the internal morality of contracting by walking through a precontractual state and demonstrating how cooperation works (Van Oosterhout et al. 2006).

Table 2 Social contract narrative for expectations of privacy

Components of social contract narrative		
Input	Narrative	Output
As applied to privacy as a social contract		
Initial, precontractual state: inaccessibility; scattering of recluses.	Narrative: Individuals discriminately sharing and knowing information to preserve an ideal sphere.	Microsocial contracts: the normative, institutional, social constraints on how information flows.
Characteristics of reasonable agents: to form relationships and coordinate activities (Dennett 1995; De Waal and De Waal 1997)	Reasons and interests that go into agreement: (1) Preserve liberty and autonomy as individuals are free to "develop personalities, goals, ideas, and the right to determine to whom their thoughts, emotions, sentiments, and tangible products are communicated" (Bloustein 1964, p. 18) (2) Share information for intimacy (Elgesem 1996, p. 51), in order to have relationships (Fried 1968), and to converse and trade information (Singleton 1998) friendship, intimacy, and trust (Fried 1968) and preserves important human relationships (Nissenbaum 2004)	Framework: *what* information is shared with *whom* and *how* is it used?
Social contract requirements voice, exit, consent. → Sustainable, mutually beneficial agreements		
Implications for business ethics		
Expecting individuals to keep information inaccessible is unsustainable and unrealistic. Users, consumers, and employees need a way to share relevant information to form relationships and coordinate activities	Strong privacy norms and expectations are necessary to preserve liberty and autonomy, to develop personalities, and to develop different relationships. Work in business ethics and management seeking to *justify* privacy helps support the narrative	Firm would need to support stakeholders in maintaining their microsocial contracts around privacy
Social contract requirements notice and choice may fulfill social contract procedural minimums of consent; the "right to be forgotten" may fulfill exit requirements		

restricted-access view of privacy in this original state, individuals either share information and make it public or do not share information and keep it private.

Behavioral Tendencies

Such a state of inaccessibility is not sustainable as we may minimally assume individuals have a behavioral tendency to form relationships and coordinate activities (Dennett 1995; De Waal and De Waal 1997). In other words, we do not have the behavioral tendencies to live as a scattering of recluses. These tendencies are so strong and integral to being human that a state of perfect inaccessibility—or a completely solitary existence where a person and their information is kept inaccessible from others—is considered an extreme form of punishment today: solitary confinement (Tufekci 2008a, b). Defining privacy as a state of inaccessibility is neither practical nor desirable and, ironically, renders privacy as a form of punishment.

As individuals naturally come together to form relationships, they share information. Human beings enjoy the freedom to converse and trade information about one another and have an interest in collecting information as well as sharing information. Throughout privacy scholarship, a need to share information for intimacy (Elgesem 1996, p. 51), in order to have relationships (Fried 1968), and to converse and trade information (Singleton 1998) pervades justifications for privacy norms. Because the original state of inaccessibility is inefficient for economic and social actors (Posner 1981), information sharing becomes necessary for relationships.[7]

Furthermore, *discriminately sharing* information affords people the important power to determine both how close they are to others and the nature of their relationships. Information sharing is not only necessary to form relationships and trade, but *discriminately* sharing allows individuals to differentiate between relationships. Maintaining more than one relationship becomes more complicated as individuals interact with different types of people from different contexts or communities. Individuals share different types and amounts of information in order to negotiate the boundary conditions of relationships (Samarajiva 1997). "The sort of relationship that people have to one another involves…a conception of the kind and degree of knowledge concerning one another which it is appropriate for them to have" (Rachels 1975, p. 294). Different relationships require different information-sharing rules, and controlling who has access to

[7] Sociologist Gerstein notes that individuals take on two roles in any relationship—observer and participant—and mere observation is not sufficient to form intimate relationships. Instead, individuals must participate by sharing information in order to form relationships.

personal information is necessary for friendship, intimacy, and trust (Fried 1968) and preserves important human relationships (Nissenbaum 2004). As noted by technology scholar James Moor, "different people may be given different levels of access for different kinds of information at different times" (1997, p. 414).

Outcome: Framework for Privacy as a Social Contract

The social contract narrative illustrates the natural evolution of social contract norms around privacy. Based on this narrative, individuals within a given community discriminately share information with a particular set of obligations in mind as to who has access to the information and how it will be used (Nissenbaum 2004, 2009; Martin 2012; Sloan and Warner 2014). Based on the social contract narrative, a framework for microsocial contract privacy norms centers on (1) the type of information, (2) who has access to information, and (3) how the information is used within a given community as explored below.

First, an ideal sphere lies around every individual where trespasses can be seen as an insult to one's honor (Simmel 1906, p. 321). Protecting that space can help create a background for a self-creative enterprise (Bennett 1992). Privacy law scholar Julie Cohen refers to this inviolate space as the privacy of the home that affords "freedom of movement that is both literal and metaphorical" (Cohen 2008, p. 195). This tension between the need to maintain the ideal sphere around ourselves and the need to disclose information for relationships and communities is sustained through negotiated norms around *the type of information*. Users on a site, such as Facebook or diaspora,* have an expectation about the type of information collected—such as GPS or browsing history or demographics.

Importantly, people retain the desire to limit *who has access to information*. In other words, information known to one person does not necessarily mean the information is meant for *all* people. Sharing is not all or nothing but 'optimal' depending on maturity and scope of relationship and the role of the individual (Brin 1999). Determining who receives which piece of information keeps people from being "misrepresented and judged out of context" (Rosen 2001, p. 21). Trying out different jokes, behaviors, or personas with friends helps people to develop as individuals; but those same jokes, behaviors, or personas could be damaging with a different population. Individuals are constantly deciding how to present themselves at varying personal and social levels through agreements about confidentiality (Stutzman and Hartzog 2012), while retaining a desire for seclusion and a fear of intrusion (Bambauer 2012). Online individuals need to discriminately share information within a relationship without fear of these behaviors or information being broadcast broadly—or sold to data aggregators or retained for years. In casual language, individuals talk about expectations of *confidentiality* to signify the rules about which actors can know particular information.

Finally, when individuals do reveal information to an actor, rules and obligations govern not only who else should receive the information but also *how the information is used* (Hartzog 2011). These social contracts around what, to whom, and for what purpose information flows are the governing rules about privacy for a given community. The purpose(s) of the community within which the information is shared dictates the valid uses of the information gathered or disclosed. Tracking GPS location data by an application is valid when the application is for directions or tracking your cycling route, but not valid when the application is to simulate a flashlight. When people attempt to assign property rights to control information, they attempt to control how information is later used.

These facets of privacy norms—the what, who, and how—can be seen as working in concert within a given relationship. Within a community or context, for every given set of data, there exists a rule about who should be privy to that information and the purpose for that information. Similarly, for every given set of individuals, there exists a set of information that is expected to be shared and why. Key to these agreements is how the main components work together (see Nissenbaum 2009). Within privacy as a social contract, "who, what, and how" would identify a particular micro privacy norm in a community.

From an original and unsustainable state of inaccessibility, individuals have a need to *discriminately share information* in order to socialize, create relationships, form groups, and trade. Individuals have a desire—and a reasonable expectation—to be able to live within communities while maintaining a sense of self. Just as communities acknowledge freedom of movement simultaneous to a protection from assault, individuals and society have an interest of interacting in a community through sharing information while preserving space to develop themselves, their relationships, and their communities.

(Re)conceptualizing Privacy Online

The social contract approach used here is a multilevel, contextually rich framework allowing for specific contractors within a contracting community the moral free space to develop authentic and legitimate privacy norms and expectations. And the social contract narrative is an important step to understand the factors individuals take into consideration when negotiating privacy microsocial contract norms. Alternative approaches to privacy have

been attractive because respecting and violating privacy are clearly defined and easy to measure—privacy is violated when information is either not controlled or no longer inaccessible. Privacy as a social contract offers a more nuanced, context-dependent understanding of privacy while not venturing into the territory of relativism. To explain, common privacy violations are redescribed below given the social contract approach to privacy and outlined in Tables 3 and 4.

Reframing Privacy Violations

Violation #1: Procedural Hypernorms

First, hypernorms can be violated by not adequately addressing the procedural and structural requirements for a legitimate social contract. Microsocial contracts rely upon procedural norms of adequate voice, exit, and informed consent (Dunfee 2006), and the current focus online on adequate notice and choice seeks to uphold minimal precepts of social contract's procedural norms of exit, consent, and voice. Online privacy notices, authentic consent, and an ability to switch websites would address the procedural hypernorms required in the macrosocial contract.

For example, researchers continually find violations to procedural hypernorms online. Notices are unrealistically time consuming (McDonald and Cranor 2008) and not always targeted toward consumers (Cranor et al. 2014). Empirical studies have shown that notices are difficult if not impossible to find by users (Leon et al. 2012) and include misleading information (Leon et al. 2010). Respondents do not understand notices to the point where users are misled by icons and notices (Ur et al. 2012). And respondents have been found to assume their privacy expectations are included in the notice (Martin 2014) or that the advertising icon does more to protect their privacy than in actuality (Leon et al. 2012).

Privacy as a social contract would suggest that focusing on informed consent and the contractors' right of exit and voice are important, but not the only tactics to respect privacy expectations. The procedural norms of consent, exit, and voice are required for the micro-privacy social contracts to be legitimate and to bind the members of the community.[8] However, much of the proverbial 'heavy lifting' around privacy expectations is done within the community in identifying and negotiating context-specific privacy norms around who, what, and why information is shared.

Violation #2: Microsocial Contracts

In addition, a violation of privacy would also include when information is tracked, disseminated, or used against the agreement of the actors within the community through a breach of microsocial contracts. Given the framework of micro privacy norms above, privacy violations occur when the recipient of information—an organization, a user, or the primary website—changes *who* is included in receiving information, *what* information is shared, and *how* the information is used.

Change What Information is Shared Individuals retain a desire to keep certain information inaccessible even within defined relationships, yet new pieces of information become available with advances in technology. In regards to online surveillance, GPS data is now available from mobile devices and tracked in addition to a user's IP address or a unique user identifier. A study of 101 popular applications found that 47 transmitted phone location and 56 transmitted a unique phone identifier to a third-party data aggregator (Thurm and Kane 2010). In addition, websites can identify and capture how individuals travel to a website, where they click on a page, and where they travel after the visit in addition to purchases and searches while on the site. For example, Facebook began collecting and using user browsing history—users' online activities outside the context of Facebook—in order to target advertising (Albergotti 2014a). A recent study found that 31 % of applications gather information outside their purpose and without a valid use ("Backgrounder" 2014). Collecting new information within an existing relationship may constitute a privacy violation.

Change Who Receives the Information Individuals regularly give access to information to some people or some organizations while keeping the same information from others. For example, Facebook's Beacon program took information about an individual's browsing and buying habits with an online retailer, such as Amazon.com, and sent alerts automatically to a new group of individuals—the Facebook user's friends. The information disclosed to Amazon.com (and others) was leaked to Facebook friends, thereby changing the actors who received the information. When a fitness application, Moves (https://www.moves-app.com), was acquired by Facebook, a new actor (Facebook) suddenly had access to the app's user information—much to their surprise (Wagner 2014). Similarly, tagging photographs online allows new individuals to know about offline activities: by posting a picture and linking it to a subject's name, offline activities are suddenly available to individuals not present at the event. Users do not relinquish information to an undefined group

[8] I wish to thank Gaston de los Reyes for making this important point on the role of the procedural hypernorms of exit, voice, and consent.

Table 3 Reframing privacy violations

Tenet of social contracts	Commonly seen as: privacy as…	Violations	As addressed in market
Procedural contract norms			
Voice Informed consent Exit	FIP—notice and choice	Website does not notify users of third-party tracking Initially, Facebook users had difficulty deleting their accounts thereby removing the option to 'exit'	Better designed notices such as P3P (Cranor 2012) that allows for consumer-friendly interface based on machine-language notice
Microcontract norms			
Change who receives the information	Confidentiality	Facebook's Beacon program captured information about individual's browsing and buying habits with an online retailer, e.g., Amazon.com, and sent alerts automatically to a new group of individuals—the Facebook user's friends For example, when a fitness application, Moves (https://www.moves-app.com), was acquired by Facebook, a new actor (Facebook) suddenly had access to the app's user information—much to their surprise (Wagner 2014)	TOR is free anonymizing software to securely route traffic Diaspora* social network does not sell access to third parties Encryption in user communication in WhatsApp (Greenberg 2014)
Change what information is shared	Secrecy	GPS data is now regularly available from mobile devices and tracked in addition to IP addresses and a unique user identifier For example, Facebook began collecting and using user browsing history—online activities outside the context of Facebook—in order to target advertising (Albergotti 2014a). And, a recent study found that 31 % of applications gather information outside their purpose and without a valid use ("Backgrounder" 2014)	Diaspora* social network allows users to remain anonymous Whisper application does not track users (Dwoskin 2014)
Change how information is used	Control/ property	A user's online activity may be passed to a website such as Orbitz and used to prioritize search results For example, Facebook manipulated the newsfeeds of 700,000 to render the feed more positive or negative and to measure the effect on users' postings of those manipulations	Diaspora* social network allows users to retain rights over their data
Integrity of community (e.g., moral free space Donaldson and Dunfee 1994)			
Interference with the norms within a community by outsiders	Decisional privacy	Legislative, substantive norms imposed from outside the community. For example, Do Not Track at the browser level Regulation of substantive social contracts within communities	Snapchat's approach to native advertising to not interfere with users' conversations (Shields 2014)

of actors. Rather, individuals knowingly disclose information to a particular set of actors within a community.

Change How the Information is Used Individuals have an interest in how their information is used within a community, and a line of scholarship has evolved to equate privacy with the degree of control over personal information. While problems abound with conceptualizing privacy as solely an intellectual property issue (Bambauer 2012), the underlying premise that individuals have an interest in how their information is used is sound and remains a strong focus in privacy framed as a property right and the FIPs prevalent in business.

For example, information given to a medical professional is to be used for medical diagnosis or for furthering the medical field through research. If the medical professional were to sell that information to a pharmaceutical company for marketing purposes or use that information to sell the patient a car, the professional would breach the terms of use within the social contract. Online, a user's travel history may be known to a website such as Orbitz and can be used to analyze how individuals came to find Orbitz for future Orbitz marketing or advertisements.

Table 4 Analyzing privacy violations online using examples

	Before design change: Implicit privacy norms	Design change	Post-design change: Privacy violation
Sponsored Stories			
What information	The Facebook user's approval of an article, story, or advertisement	Facebook users who clicked on 'like' buttons had pictures of themselves with an endorsement sent to their friends in a sponsored story	Same
Who receives information	The 'liked' article, story, or advertisement		Facebook user's friends
How information is used	To tally the popularity of an article, story, or advertisement on a third-party site		To market the article, story, or product to Facebook friends using relationship advertising
Orbitz			
What information	Website browsing history and Orbitz purchase history	Orbitz tracks how users arrived at their site in order to prioritize search results	Same. Internet browsing history might be new for some
Who receives information	Orbitz		Same
How information is used	Remember recent searches, targeted advertising for travel locations, possible add-ons for travel locations. Possibly for Orbitz marketing purposes		To modify search results based on the likelihood that the user is price sensitive
Verizon			
What information	Call history, browsing history, GPS/location of consumer	Verizon offers Precision Market Insights to mine Verizon's customer call and browsing information and map where people are located and what types of services they purchase and use	Same
Who receives information	Verizon		Third party, business customers interested in tracking the location and purchase tendencies of their customers
How information is used	Billing, tracking for 911 calls		For example, sports venue could identify which people watching the game are likely to leave via different routes or purchase paraphernalia by matching spectators to Verizon's records

However, using an individual's online history to change query results uses the known information in a novel way. Research has shown users have privacy expectations around both the type of information access as well as how the information is used using mobile apps (Shilton and Martin 2013) and online (Martin 2014). Further, when respondents are shown the information that was collected and aggregated about them online, respondents care about the scope of use of even innocuous information online (Cranor et al. 2014).

An infamous example of the misuse of legitimately acquired information is the use of Facebook users' data and the users themselves in an experiment (Albergotti 2014b; Meyer 2014). Facebook manipulated the newsfeeds of 700,000 users to be more positive or negative and then measured the effect on users' subsequent postings. The postings were in the hands of a valid actor (Facebook and the recipients of the post), but Facebook used the information in a novel way thereby violating the microsocial contract in the Facebook community around the expected use of information.

Violation #3: Community or Contextual Integrity (Nissenbaum 2009)

Social contract theory suggests a third level of privacy violations in protecting the integrity *of the boundaries* of the contracting community and their moral free space. In other words, viewing privacy norms as a social contract highlights the moral importance in protecting the boundaries of the context in Nissenbaum's Privacy as Contextual Integrity (2004, 2009) or moral free space of the communities. Within social contract theory, society has an obligation to *not* develop and impose substantive norms on the moral free space of the contractors. If outsiders to a contracting community make substantive demands on the content and flow of information, such outsiders would be breaching the integrity of that moral free space. In fact, such a privacy intrusion or violation is also referred to as a violation of *decisional privacy* (Allen 1999) or passive privacy (Floridi 2006) where the interference in autonomy is considered a privacy violation. Broad regulations aimed at too high a level may impose a standardized set of

privacy norms across communities. For example, the browser-level Do Not Track designation may not apply to particular contexts and would interfere with the ability to develop microsocial contracts within particular communities.

Discussion

Privacy as a social contract constitutes a shift from viewing sharing information online as dispositive of relinquishing reasonable expectations of privacy to viewing sharing information online as a necessary part of strong community and individual autonomy. As such, the use of a social contract approach to privacy sheds light on weaknesses in the traditional restricted access and control definitions of privacy and also extends the important work within privacy on privacy as contextual integrity (Nissenbaum 2009).

Correcting Previous Views of Privacy

The access-view of privacy, where privacy is maintained only by remaining inaccessible to others, requires individuals to relinquish privacy when interacting within their community. Yet, research has shown users have privacy expectations around both the type of information revealed as well as how the information is used when online (Martin 2014) or when using mobile apps (Martin and Shilton, 2015). Respondents care about the scope of use of even innocuous information online (Leon et al. 2013), view tracking and online behavioral advertising as creepy (Ur et al. 2012), and wish to not be tracked when online (McDonald and Cranor 2010). *Privacy as a social contract allows for the fact that individuals disclose information without relinquishing privacy.*

Privacy as a social contract provides guidance post-disclosure and allows for the interest of individuals both to share information while having privacy expectations around how information is used and who has access within a community. For example, Facebook tracking users' web browser history, experimenting with users' newsfeed, and gaining access to user data of an acquired application concerned previously disclosed information that was, for the access-view of privacy, considered 'public." Facebook's violations are not captured with the access-view of privacy but are explained with privacy as a social contract as a breach of microsocial contract norms and as explored in Table 3 above.

The control-view of privacy, most often operationalized through adequate notification and consumer choice, assumes that individuals maintain control over their information by reading a privacy notice and choosing the website whose privacy practices most closely match their preferences. Yet considerable agreement exists that notice and choice has failed to govern privacy effectively online (Martin 2013; Nissenbaum 2011; Calo 2012; Solove 2013). Consumers fall victim to becoming a 'captive audience' without functional opt-out mechanisms thereby making notice and choice less meaningful (Popescu and Barah 2013). Perhaps most damning, 91 % of respondents feel as though they have lost control of their data (Madden et al. 2014). In fact, the infamous Facebook experiment conformed to the broad statements in Facebook's privacy policy (Elder 2014).

Not only are the access-view and control-view of privacy lacking in descriptive validity, the views of privacy may guide firms in the wrong direction to meet privacy expectations of users. Currently, the only affirmative responsibility of firms online is adequate notification (Calo 2012; Beales and Eisenach 2013). Firms online are not responsible for their specific privacy practices—only in communicating their tactics to consumers. In focusing on disclosure as the main responsibility of the firm, firms become free to implement questionable privacy practices so long as the practices are accurately reported. However, the social contract narrative suggests that individuals have an interest in discriminately sharing information with limits as to who knows and how it is used, thus changing how managers and management researchers would frame privacy violations and judge privacy expectations.

Extending Privacy as Contextual Integrity

The social contract approach to privacy also extends context-dependent theories of privacy, such as privacy as contextual integrity (Nissenbaum 2009). Privacy as a social contract offers a mechanism to judge privacy norms and, in doing so, addresses charges of relativism endemic to contextually dependent theories of privacy. First, locally negotiated social contracts are always beholden to procedural universal principles to remain legitimate (Van Oosterhout et al. 2006). Therefore, microsocial contract privacy norms must also abide by the universal and thin second order norms such as the rights of consent, voice, and exit (Donaldson and Dunfee 1995; Dunfee 2006; Heugens et al. 2006). As such, contracting has an internal morality without the need for external substantive guidance—for some (Van Oosterhout et al. 2006).[9]

[9] In fact, rather than substantive macro norms to guide thick micro privacy norms, Walzer positions minimal, thin guiding principles as a product of repeated social contract norms. According to Walzer, "moral terms have minimal and maximal meanings (1994, p. 2) where minimalist meanings are embedded in the maximal morality and designate "some reiterated features of particularly thick of maximal moralities" (Walzer 1994, p. 10). This minimalism is "reasonable enough and universal enough, has no imperial

In addition, locally negotiated privacy norms, i.e., microsocial contracts, can be analyzed through both actual and hypothetical social contracts to address "norms of decency, etiquette, sociability, convention, and morality" (Nissenbaum 2004; see also, Tavani 2008; Dunfee 2006). While privacy as contextual integrity (Nissenbaum 2004, 2009) focuses on the *actual* negotiated privacy norms, a social contract approach adds a possible additional layer of analysis in the form of the *hypothetical* social contract which would have moral weight. We could ask, what privacy norms would reasonable individuals agree to, given minimal social contract standards of consent, voice, and exit?

These hypothetical microsocial contracts should leverage existing empirical work on privacy expectations, interests, and preferences. For example, we can ask, "would users of Facebook expect their browsing histories to be used for targeted advertising?" regardless of what practices were communicated in the privacy policy (Albergotti 2014a). Considering the fact that 80 % of respondents are concerned third parties accessing data they share (Madden et al. 2014), we would be able to presume Facebook users would be concerned with third parties accessing their data.

Finally, locally negotiated privacy norms must meet the interests of the contractors to discriminately share information as illustrated within the narrative above. Similarly, Helen Nissenbaum highlights the important purpose of the community in guiding appropriate privacy norms. Nissenbaum further suggests judging privacy norms based on, first, the promotion of goods and values within the context and, second, meeting "fundamental social, political, and moral values" (2009, p. 128). Within social contract theory, the criterion of mutually beneficial and sustainable local norms (Van Oosterhout et al. 2006) also suggests a required fit within the community's goals or purpose is an important factor to consider in judging privacy norms. Similarly, one of the two key assumptions in the construction of the macrosocial contract and the moral free space within a community by Donaldson and Dunfee (1999) is the need for a moral fabric supportive of (1) efficiency and (2) preexisting core values of the community.

Footnote 9 continued
tendencies; it doesn't aspire to global rule, it leaves room" (Walzer 1994, p. 64). It is less the product of persuasion than of mutual recognition across spaces (Walzer 1994, p. 17). We can think of the content of macrosocial contracts as the result of a numberless accumulation of psychological contracts that individuals have socially constructed over time (Thompson and Hart 2006, p. 233).

Implications and Conclusion

In relying on notice and choice to assuage privacy concerns, a firm's only role in respecting privacy expectations online was to ensure a user was adequately notified and the consent of the user was acquired. This gives firms the perverse incentive to construct elaborately vague privacy notices, left unread and misunderstood by users, only to gain users' consent. With individuals and consumers rendering privacy judgments regardless of the explicit privacy notices, the prominent tool available for businesses to manage privacy expectations is rendered ineffective.

Within a social contract approach to privacy, the focus shifts from firms gaining consent to the role and responsibilities of businesses as contractors in communities. From the narrative above, rules around discriminately sharing information take into consideration the possible benefits to the individual (such as better relationships, trading for goods and services, employment, etc.) as well as the benefits to the contracting community (such as a banking system, a functioning workplace, a credit system, a marketplace, etc.) while also balancing the expected harms. Understanding this privacy analysis will help firms better meet the privacy expectations of their stakeholders. Importantly for researchers and firms, questions remain about how to identify microsocial contract norms about privacy and what is taken into consideration in forming those privacy norms.

The implications to privacy research and practice based on social contract concepts are examined below and outlined in Table 5.

Implications for Research

Both the restricted-access and control approaches may be considered universal principles or 'strong' definitions of privacy where the definition of what it means to respect privacy—remaining inaccessible or adhering to notice statements—is universally known and applicable. This is problematic in that performing research on privacy becomes an exercise in testing an individual's belief in a predefined and arbitrary conception of privacy. For example, it has become almost cliché to declare young adults to have diminished or no privacy expectations, yet, when examined closely, young adults are found to have privacy norms that differ from older adults while retaining strong expectations of privacy (Hoofnagle et al. 2010). Similarly, individuals who do not agree with the analyst's definition of privacy are presumed to not find privacy important (e.g., Acquisti and Grossklags 2005) or to be unethical (Winter et al. 2004). Instead, researchers and organizations should ask *what are the privacy expectations of the users, customers, or employees in this situation?* rather than *do users,*

Table 5 Implications to research and practice

Social contract concept	Within a social contract approach to privacy	Previous alternative	Implications for practice	Implications for research
Contracting community focus	Privacy norms are developed within a particular community of actors. That community is circumscribed by a common set of goals, purpose, and value system	Privacy concerns and expectations are uniform and universally known as either the degree information is inaccessible or controlled	Tactics to address online privacy expectations should be dependent on the context of the exchange	For privacy research, survey questions should be tailored to a particular context or community rather than remain general. More inductive research is needed to identify the expectations in a particular community rather than test for conformity to the access-view or control-view of privacy
Microcontract norms	Individuals have a continuing interest in discriminately sharing information about *who* has access for *what* information and *how* it is used	The decision to share information is framed dispositive of relinquishing a reasonable expectation of privacy Privacy vacuums or areas where no privacy expectations are reasonable (e.g., public space, online, etc.)	Users do not relinquish information without an expectation about how that information will be used within that context No area exists where "anything goes"	More work would need to examine the privacy expectations of users with disclosed information. Researchers and organizations should ask *what are the privacy expectations of the users, customers, or employees in this situation?* Rather than *do users customers, or employees have any reasonable expectation of privacy here?*
Role of contractors	Actors, such as firms, within a community have a responsibility to uphold and develop privacy expectations Expectations can be dynamic and change over time requiring constant re-negotiation and attention to expectations of stakeholders (consumers, users, employees)	The responsibility for the handoff of information is placed primarily on the consumer Privacy expectations are set with notice when users hand off information	In the case of privacy online, the relationship between the website and the user becomes critical to upholding privacy expectations Firms are responsible for managing the privacy expectations regardless of notice	More longitudinal studies to help firms identify whether and how privacy expectations change over time and with new innovations. Research should focus on the responsibility of all contractors—including websites and online actors tracking information

customers, or employees have any reasonable expectation of privacy here?

Scholarship that operationalizes relinquishing privacy as when users provide information misses the expectations consumers have even once they provide information—even innocuous information (Leon et al. 2013). In other words, researchers will observe a respondent who is willing to purchase something online and equate that behavior with a demonstration that he/she is less concerned about privacy. When asked, as shown above in the studies, respondents go online *and* have expectations of privacy.

A social contract approach would be particularly well suited to the stakeholders and issues of organizations and managers. However, little empirical work has been done to test a social contract approach to privacy, since social contract approaches, in general, remain empirically challenged (Dunfee 2006; Glac and Kim 2009; Van Oosterhout et al. 2006; Soule 2002). This is due to the fact that allowing for locally defined norms renders contextual approaches to privacy difficult to test empirically. The identification of the relevant community and local authentic norms is "partially if not entirely" an empirical task (Husted 1999). Additional inductive research to identify the particular privacy norms within a community or context would help organizations meet privacy expectations of users, employees, and customers.

Implications for Practice

Responsibility of Firms

Current approaches to online privacy place the onus on the consumer to *understand* and *acknowledge* the privacy notices or to choose wisely where and when they give access to their information. In other words, the responsibility for the handoff of information is placed primarily on the consumer. Once privacy is viewed as the social contract between parties about the type and flow of information within a given community, privacy becomes attached primarily to a relationship rather than to a piece of data or location.

In the case of privacy online, the relationship between the website and the user becomes critical to upholding

privacy expectations. All contractors—users and organizations—have a right and an obligation as both the recipient of information and as the disseminator of information to abide by the particular privacy norms within that community or to voice objection. Primary websites have the knowledge, access, and incentives to become more responsible regarding their users' overall privacy experience online.

As noted by Dunfee Dunfee et al. (1999, p. 32) and Van Oosterhout and Heugens (2009, p. 731), merely enjoying the benefits of the community, engaging in transaction within the community, and reaping the benefits of the structure offered by the microsocial contracts within the community entails a reciprocal obligation to uphold and develop the authentic norms of the community. Firms reaping the benefits of users, consumers, and employees from their disclosures of information have an obligation to respect the privacy norms within their community. For example, Facebook partners with many retail, gaming, search, and news sites to allow a Facebook login on these third-party sites. However, Facebook negotiated that these partners are not permitted to transfer any information to AdNetworks or data brokers based on their Facebook users' login. In addition, Facebook also uses technology to detect attempts to scrape, or copy, their members' profiles thereby taking responsibility to manage their users' online experience. However, Facebook's purchase of the fitness app Move, and attempt to access Move's user data (Wagner 2014), calls into question whether Facebook prioritizes the role and responsibility of the website's relationship with users or, instead, prioritizes Facebook's needs.

"Anything Goes" Fallacy (Nissenbaum 2004)

According to the narrative offered, the decision to share information is not dispositive of relinquishing a reasonable expectation of privacy. Instead, individuals have an interest in discriminately sharing information. For privacy research, more work would need to examine the privacy expectations of users with disclosed information. Both the traditional control and restricted-access approach to privacy approaches treat the act of sharing information as dispositive of relinquishing an expectation of privacy: individuals either share information and lose a right to privacy or do not share information and retain a reasonable expectation of privacy. The narrative offered here suggests shifting the conversation to view individuals as always having an interest in discriminately sharing information. The question for firms becomes how to support individuals discriminately sharing information within a particular context or community. For example, selling behavioral information may be appropriate for retail websites but not for financial services, as MasterCard and Visa learned when they approached companies with selling personalized information (Steel 2011).

For privacy as a social contract, no area exists where "anything goes" (Nissenbaum 2004). Any community has prevailing privacy norms and associated reasonable expectations of privacy that are the product of either explicit or implicit negotiations. Rather than create the false possibility of a region where anything goes online, a social contract approach to privacy suggests that information is always governed by the norms of a particular community.

Privacy as a social contract—or a mutually beneficial agreement within a community about how information is used and shared—suggests that tactics to address online privacy expectations should be dependent on the context of the exchange. This diverges from tactics that seek to address privacy issues online as if privacy concerns and expectations are uniform. For example, a banking website will have different privacy norms from a retail website. Similarly, a gaming website might have more in common with a social networking site than a retail site. The purpose of the website will influence the privacy expectations for the users and empirical studies may be required to identify the microsocial contract norms around privacy—as has been called for in scholarship (Dunfee 2006).

Privacy as a Competitive Advantage

The development of mutually beneficial privacy norms by contractors is a competitive advantage within communities. In order to keep people actively participating in relationships and trade within a particular community, privacy rules develop around who is privy to which piece of information and the obligations associated with knowing that piece of information. Sociologist Schwartz notes that privacy rules are necessary within any stable social system as he suggests that privacy agreements should be viewed as an index of solidarity (1968). In other words, strong privacy norms make strong communities.

The larger community also benefits from individuals retaining 'a backstage' or a private self (Goffman 1959; Nissenbaum 2004) while also sharing information.[10] Communities—including those of a firm—benefit when websites and users, husbands and wives, work groups, or teams develop their particular privacy expectations and norms. In fact, "part of what makes a society a good place to live is the extent to which it allows people freedom from

[10] Similarly, Dunbar (1998) proposes that gossip, people-curiosity and small talk, all of which are seemingly nonfunctional and are often popularly understood as mere distraction or deviation, are in essence the human version of social grooming in primates: an activity that is essential to forging bonds, affirming relationships, displaying bonds, and asserting and learning about hierarchies and alliances. See Tufekci (2008a, b): "Grooming, Gossip, Facebook and Myspace."

intrusiveness of others" (Regan 2011). As Priscilla Regan notes, "on a societal level, people require a measure of understanding of how they relate to others that permits the development of a sense of self and connectedness to others within the society of which they are a part." Without rules governing how information should move within a given community or relationship, individuals withdraw (Schwartz 1968). This approach is Deweyan in acknowledging that both individuals and society benefit from particular protection of privacy rather than positioning the interests of parties as opposing forces (see also Nissenbaum 2004; Regan 2011; Solove 2006).

On a smaller scale, this competitive advantage can be seen in the introduction of privacy-aware products and services. For example, DuckDuckGo is "the search engine that doesn't track you" (www.duckduckgo.com). Diaspora* (www.diasporafoundation.org) is a decentralized social network that differentiates based on freedom and privacy: users access diaspora* through user-supported servers (or pods), using pseudonyms, and with full rights over the use of their data.[11] In addition, Whisper, an app that allows users to share thoughts anonymously, was caught tracking users (Dwoskin 2014); yet a competitor, Secrets, noted their business model does not include developing relationships with media outlets and therefore will not have the incentive to monetize tracking of users. Similarly, Snapchat attempted to distance themselves from other social media services by not using native advertising: instead ads are "compartmentalized" and not based on collected user data (Shields 2014). Table 3 includes the examples of the products and services in the market seeking to responsibly contract in their community by engineering privacy into their product—as has been called for in research (Mayer and Narayanan 2013) and public policy (Ohlhausen 2014).

Limitations and Concerns

Because privacy norms may be locally defined within a particular community, charges of relativism are endemic to a social contract approach. The lack of substantive principles to guide the development of local norms leave some to find a lack of moral authority (Wempe 2005; Soule 2002; Dunfee 2006) and allow "morally rogue agreements" (Soule 2002). Locally developed privacy norms can be perceived as losing moral authority because the norms are tied to practice or convention (Nissenbaum 2004). Van Oosterhout et al. (2006) refer to this assumption as the 'contractualist fallacy,' or the "erroneous assumption that the contractualist argumentative structure uniquely determines a single set of action-guiding norms" (p. 522).

However, other approaches to social contracts do not view contracting as "a morally neutral idea" (Van Oosterhout et al. 2006, p. 528). In fact, the social contract narrative illustrates what Van Oosterhout et al. (2006) refer to as 'the internal morality of contracting' by walking through a 'precontractual state of nature without cooperation and demonstrate how cooperation works." Therefore, substantive privacy principles are not needed, according to Nissenbaum (2004), Van Oosterhout et al. (2006), and Van Oosterhout and Heugens (2009), in order to have moral gravity. The internal morality defines a moral threshold for microsocial contracting that enables us to filter out contracts and practices incompatible with the moral import of contracting (Van Oosterhout et al. 2006). Instead, contractualists "focus on the reasonable and normative foundations of contractual schemes" (Van Oosterhout et al. 2006, p. 521). The goal of the contractualist endeavor is not to identify the single right answer, but to identify legitimate and authentic agreements.

In addition, the demarcation where one community starts and another stops is not clear at times. In fact, a social contract approach to privacy introduces the possibility of conflicting norms of privacy and overlapping communities similar to other social contract theories. Overlapping spaces and conflicting norms/duties are endemic limitations for social contract approaches (Phillips and Johnson-Cramer 2006). Future research on privacy as a social contact would need to take such overlapping communities into consideration.

The evolution of thick privacy norms may be seen as a problem for some, since a social contract approach to privacy leads to an increase in stability and a tendency toward the status quo. Social contract approaches can be viewed as lacking a mechanism for revising micro norms (Phillips and Johnson-Cramer 2006) or, as Nissenbaum notes in reference to privacy as contextual integrity, a tendency toward conservatism (Nissenbaum 2004). Changes are initially resisted as "entrenched normative framework represents a settled rationale" (Nissenbaum 2004, p. 127).

Yet for Michael Walzer, agreements "change over time as a result of internal tension and external example; hence they are always subject to dispute" (Walzer 1994, p. 27). In fact, others see social contract approaches to include dynamism as an asset rather than a hindrance and position the norm of forgiveness as critical to sustainable solutions (Van Oosterhout et al. 2006). Most clearly, Daniel Dennett suggests an evolutionary story with a mutation arising "instead of persisting in the myopically selfish policies of mutual defection and distrust that had reigned heretofore, these particular lucky competitors hit upon a new idea:

[11] These attributes also make diaspora* attractive to terrorist groups such as IS (aka ISIL or ISIS)—the decentralized nature of the infrastructure makes banishing a terrorist group almost impossible (Lee 2014).

cooperation for mutual benefit" (Dennett 1995, p. 454). All social contract theorists "agree in seeing morality to be, in one way or another, an emergent product of a major innovation in perspective." Where Rawls sees a stable agreement that cannot be upset in the form of reflective equilibrium, such stability creates problems for Phillips and Johnson-Cramer in their analysis of ISCT within business ethics (2006); and Dennett never commits to such stability and talks of evolutionary nature. Importantly here, both assumptions of stability and dynamism are possible within the arguments herein, however Dennett's assumption about human behavioral tendencies are more in line with the social contract narrative above.

Conclusion

This paper examined how privacy norms develop through a social contract narrative in order to reframe possible privacy violations given the social contract approach to privacy and critically examine the role of business as a contractor in developing privacy norms. These social contracts are important to understand if firms are going to adequately manage the privacy expectations of stakeholders. Most importantly, focusing on the microsocial contracts around privacy expectations shifts the responsibility of firms from adequate notification and gaining consent of the individuals to the responsibilities of the firm as a contractor to maintain a mutually beneficial and sustainable solution. The social contract approach to privacy has important practical implications for firms struggling to identify the privacy expectations of stakeholders.

Acknowledgments This material is based on work supported by the National Science Foundation under Grant No. 1311823. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation. I wish to thank Tom Donaldson and Gaston de los Reyes Jr. for their comments on the paper. The usual disclaimer applies.

References

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in decision making. *IEEE Security and Privacy, 3*(1), 26–33.

Albergotti, R. (2014a, June 12). Facebook to target ads based on web browsing. *Wall Street Journal*. http://online.wsj.com/articles/facebook-to-give-advertisers-data-about-users-web-browsing-1402561120.

Albergotti, R. (2014b, July 2). Facebook experiments had few limits. *Wall Street Journal*. http://online.wsj.com/articles/facebook-experiments-had-few-limits-1404344378.

Alder, S. G., Schminke, M., & Noel, T. W. (2007). The impact of individual ethics on reactions to potentially invasive HR practices. *Journal of Business Ethics, 75*(2), 201–214.

Alfino, M., & Mayes, R. (2006). *Limits of some formal approaches to risk: Directions for future research*. Delft: Delft University of Technology.

Allen, A. (1988). *Uneasy access: Privacy for women in a free society*. Totowa, NJ: Rowman and Littlefield.

Allen, A. (1999). Lying to protect privacy. *Villanova Law Review, 44*(161), 1–21.

Altman, I. (1975). *The environment and social behavior*. Monterey, CA: Brooks/Cole Publishing Company.

Angst, C. (2009). Protect my privacy or support the common-good? Ethical questions about electronic health information exchanges. *Journal of Business Ethics, 90*, 169–178.

Ashworth, L., & Free, C. (2006). Marketing dataveillance and digital privacy: Using theories of justice to understand consumers' online privacy concerns. *Journal of Business Ethics, 67*(2), 107–123.

Backgrounder. (2014, September 10). *Results of the 2014 global privacy enforcement network Sweep—September 10, 2014*. Retrieved November 18, 2014, from https://www.priv.gc.ca/media/nr-c/2014/bg_140910_e.asp.

Bambauer, J. (2012). The new intrusion. *Notre Dame Law Review, 88*, 205.

Beales, H., & Eisenach, J. A. (2013). Putting consumers first: A functionality-based approach to onlineprivacy. *Available at SSRN* http://ssrn.com/abstract=2211540.

Bennett, C. (1992). *Regulating privacy*. Ithaca, NY: Cornell University Press.

Bloustein, E. J. (1964). Privacy as an aspect of human dignity: An answer to Dean Prosser. *New York University Law Review, 39*, 962.

Bonner, W. (2007). Locating a space for ethics to appear in decision-making: Privacy as an exemplar. *Journal of Business Ethics, 70*(3), 221–234.

Bowie, N. E., & Jamal, K. (2006). Privacy rights on the internet: Self-regulation or government regulation? *Business Ethics Quarterly, 16*(3), 323–342.

Brin, D. (1999). *The transparent society: Will technology force us to choose between privacy and freedom?*. New York: Basic Books.

Brown, W. S. (1996). Technology, workplace privacy and personhood. *Journal of Business Ethics, 15*(11), 1237–1248.

Calo, M. R. (2011). The boundaries of privacy harm. *Indiana Law Journal, 86*, 1131.

Calo, R. (2012). Against notice skepticism in privacy (and elsewhere). *Notre Dame Law Review*, *87*.

Campbell, D., Craven, B., & Shrives, P. (2003). Voluntary social reporting in three FTSE sectors: a comment on perception and legitimacy. *Accounting, Auditing & Accountability Journal*, *16*(4), 558–581.

Cases, A.-S., Fournier, C., Dubois, P.-L., & Tanner, J. F., Jr. (2010). Web Site spill over to email campaigns the role of privacy, trust and shoppers' attitudes. *Journal of Business Research, 63*(9–10), 993–999.

Charters, D. (2002). Electronic monitoring and privacy issues in business-marketing: The ethics of the DoubleClick experience. *Journal of Business Ethics, 35*(4), 243–254.

Coase, R. H. (1960). The problem of social cost. *Journal of Law and Economics, 3*, 1–44.

Cohen, J. E. (2008). Privacy, visibility, transparency, and exposure. *University of Chicago Law Review, 75*(1), 181–201.

Cranford, M. (1998). Drug testing and the right to privacy: Arguing the ethics of workplace drug testing. *Journal of Business Ethics, 17*(16), 1805–1815.

Cranor, L. F. (2012). Necessary but not sufficient: Standardized mechanisms for privacy notice and choice. *Journal on Telecommunications and High Technology Law, 10*, 273.

Cranor, L. F., Hoke, C., Leon, P. G., & Au, A. (2014). Are they worth reading? An in-depth analysis of online advertising companies' privacy policies. 2014 TPRC

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

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues, 59*(2), 323–342.

De Waal, F. B. M., & De Waal, F. B. M. (1997). *Good natured*: *The origins of right and wrong in humans and other animals* (No. 87). Cambridge, MA: Harvard University Press.

Dennett, D. C. (1995). *Darwin's dangerous idea*: *Evolution and the meanings of life* (No. 39). New York: Simon and Schuster.

Dennett, D. C. (2003). *Freedom evolves*. New York: Viking Books.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for E-commerce transactions. *Information Systems Research, 17*(1), 61–80.

Donaldson, T., & Dunfee, T. W. (1994). Towards a unified conception of business ethics: Integrative social contracts theory. *Academy of Management Review, 19*, 252–284.

Donaldson, T., & Dunfee, T. W. (1995). Integrative social contracts theory. *Economics and Philosophy, 11*, 85–111.

Donaldson, T., & Dunfee, T. W. (1999). *Ties that bind: A social contracts approach to business ethics*. Cambridge, MA: Harvard Business Press.

Donaldson, T., & Dunfee, T. W. (2003). Social contracts. In P. Heugens, et al. (Eds.), *The social institutions of capitalism: Evolution and design of social contracts*. Cheltenham: Edward Elgar Publishing Ltd.

Dunbar, R. (1998). *Grooming, gossip, and the evolution of language*. Cambridge, MA: Harvard University Press.

Dunfee, T. W. (2006). A critical perspective of integrative social contracts theory: Recurring criticisms and next generation research topics. *Journal of Business Ethics, 68*(3), 303–328.

Dunfee, T. W., Smith, C. N., & Ross, W. T. (1999). Social contracts and marketing ethics. *Journal of Marketing, 63*(3), 14–32.

Dwoskin, E. (2014, November 13). Anonymous messaging app Secret distances itself from Whisper. *Wall Street Journal*. http://blogs.wsj.com/digits/2014/11/13/anonymous-messaging-app-secret-distances-itself-from-whisper/.

Eastlick, M. A., Lotz, S. L., & Warrington, P. (2006). Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, commitment. *Journal of Business Research, 59*(8), 877–886.

Elder, J. (2014, June 30). What Facebook's own rules say about its news-feed experiment. *Wall Street Journal*. http://blogs.wsj.com/digits/2014/06/30/what-facebooks-own-rules-say-about-its-news-feed-experiment/.

Elgesem, D. (1996). Privacy, respect for persons, and risk. In C. Ess (Ed.), *Philosophical perspectives on computer-mediated communication*. Albany, NY: SUNY.

Elgesem, D. (1999). The structure of rights in Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data. *Ethics and Information Technology, 1*(4), 283–293.

Federal Trade Commission. (2012a, March 26). Protecting consumer privacy in an era of rapid change. In *FTC report*. http://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers.

Federal Trade Commission. (2012b, November 23). Fair information practice principles. In *FTC report*. http://www.gov/reports/privacy3/fairinfo.shtm.

Floridi, L. (2006). Information ethics, its nature and scope. *Computers and Society, 36*(3), 21–36.

Fried, C. (1968). Privacy. *The Yale Law Journal, 77*(3), 475–493.

Glac, K., & Kim, T. W. (2009). The 'I' in ISCT: Normative and empirical facets of integration. *Journal of Business Ethics, 88*(4), 693–705.

Goffman, E. (1959). *The presentation of self in everyday life*. New York: Doubleday.

Greenberg, A. (2014, November 18). Whatsapp just switched on end-to-end encryption for hundreds of millions of users. Retrieved November 20, 2014, from http://www.wired.com/2014/11/whatsapp-encrypted-messaging/.

Grimmelmann, J. (2010). Privacy as product safety. *Widener Law Journal, 19*, 793.

Hartzog, W. (2011). Chain-Link Confidentiality. *Georgia Law Review*, *46*, 657.

Heugens, P., van Oosterhout, H., & Kaptein, M. (2006). Foundations and applications for contractualist business ethics. *Journal of Business Ethics, 68*, 211–228.

Heugens, P., van Oosterhout, H., & Vromen, J. J. (Eds.). (2003). *The social institutions of capitalism: evolution and design of social contracts*. Northhampton: Edward Elgar Publishing.

Hill, K. (2012, October 27). Verizon very excited that it can track everything phone users do and sell that to whoever is interested. *Forbes.* http://www.forbes.com/sites/kashmirhill/2012/10/17/verizon-very-excited-that-it-can-track-everything-phone-users-do-and-sell-that-to-whoever-is-interested/.

Hoofnagle, C. J., King, J., Li, S., & Turow, J. (2010). How different are young adults from older adults when it comes to information privacy attitude and policies? http://www.ftc.gov/os/comments/privacyroundtable/544506-00125.pdf.

Hsu, M.-H., & Kuo, F.-Y. (2003). The effect of organization-based self-esteem and deindividuation in protecting personal information privacy. *Journal of Business Ethics, 42*(4), 305–320.

Husted, B. W. (1999). A critique of the empirical methods of integrative social contracts theory. *Journal of Business Ethics, 20*(3), 227–235.

Introna, L., & Pouloudi, A. (1999). Privacy in the information age: Stakeholders, interests and values. *Journal of Business Ethics, 22*(1), 27–38.

Jiang, X., Hong, J. I., & Landay, J. A. (2002). Approximate information flows: Socially-based modeling of privacy in ubiquitous computing. *Proceedings of Ubicomp, 2002*, 176–193.

Kravets, D. (2012, August 18). Judge rejects Facebook 'Sponsored Stories' lawsuit settlement. *Wired.* http://www.wired.com/threatlevel/2012/08/facebook-settlement-rejected/.

Kyo, F.-Y., Lin, C. S., & Hsu, M.-S. (2007). Assessing gender differences in computing professionals' self-regulatory efficacy concerning information privacy practices. *Journal of Business Ethics, 73*(2), 145–160.

Lally, L. (1996). Privacy versus accessibility: The impact of situationally conditioned belief. *Journal of Business Ethics, 15*(11), 1221–1226.

Lee, D. (2014, August 24). Social network cannot stop IS posts. Retrieved November 19, 2014, from http://www.bbc.com/news/technology-28882042.

Leon, P. G., Cranor, L. F., McDonald, A. M., & McGuire, R. (2010). Token attempt: The misrepresentation of website privacy policies through the misuse of P3P compact policy tokens. In *Presented at the Proceedings of the 9th annual ACM workshop on Privacy in the electronic society* (pp. 93–104). ACM.

Leon, P. G., Cranshaw, J., Cranor, L. F., Graves, J., Hastak, M., Ur, B., et al. (2012). What do online behavioral advertising privacy disclosures communicate to users? In *Presented at the Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 589–598). ACM.

Leon, P. G., Ur, B., Wang, Y., Sleeper, M., Balebako, R., Shay, R., et al. (2013). What matters to users?: Factors that affect users' willingness to share information with online advertisers. *Presented at the symposium on usable privacy and security* (SOUPS).

Loch, K. D., Straub, D. W., & Kamel, S. (2003). Diffusing the internet in the Arab world: the role of social norms and technological culturation. *Engineering Management, IEEE Transactions on*, *50*(1), 45–63.

Louis Harris and Associates, & Westin, A. F. (1997). *Commerce, communication and privacy online*. New York: Louis Harris and Associates.

Lucas, L. A. (2001). Integrative social contracts theory: Ethical implications of marketing credit cards to US college students. *American Business Law Journal*, *38*(2), 413–440.

Madden, M., Rainie, L., Zickuhr, K., Duggan, M., & Smith, A. (2014). *Public perceptions of privacy and security in the post-Snowden era*. Pew Internet Research. http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf.

Manning, R. C. (1997). Liberal and communitarian defenses of workplace privacy. *Journal of Business Ethics, 16*(8), 817–823.

Margulis, S. T. (1977). Conceptions of privacy: Current status and next steps. *Journal of Social Issues, 33*, 5–21.

Martin, K. E. (2011). Information technology and privacy: Conceptual muddles or privacy vacuums? *Ethics and Information Technology, 14*(4), 267–284.

Martin, K. E. (2012). Diminished or just different? A factorial vignette study of privacy as a social contract. *Journal of Business Ethics, 11*(4), 519–539.

Martin, K. (2013). Transaction costs, privacy, and trust: The laudable goals and ultimate failure of notice and choice to respect privacy online. *First Monday, 18*(12).

Martin, K. E. (2014). Privacy notices as tabula rasa: An empirical investigation into how complying with a privacy notice is related to meeting privacy expectations online. *Available at SSRN 2518581*.

Martin, K., & Shilton, K. (2015). Why experience matters to privacy: How context-based experience moderates consumer privacy expectations for mobile applications. *Journal of the Association for Information Science and Technology*.

Mattioli, D. (2012, August 23). On Orbitz, Mac users steered to pricier hotels. *Wall Street Journal.* http://online.wsj.com/article/SB10001424052702304458604577488822667325882.html.

Mayer, J., & Narayanan, A. (2013). Privacy substitutes. *Stanford Law Review Online, 66*, 89.

McCole, P., Ramsey, E., & Williams, J. (2010). Trust considerations on attitudes towards online purchasing: The moderating effect of privacy and security concerns. *Journal of Business Research, 63*(9–10), 1018–1024.

McDonald, A. M., & Cranor, L. F. (2008). Cost of reading privacy policies. *ISJLP, 4*, 543.

McDonald, A. M., & Cranor, L. F. (2010). Beliefs and behaviors: Internet users' understanding of behavioral advertising. In *Presented at the proceedings of the 2010 research conference on communication, information and internet policy*.

Meyer, R. (2014, June 28). Everything we know about Facebook's secret mood manipulation experiment. *The Atlantic*. http://www.theatlantic.com/technology/archive/2014/06/everything-we-know-about-facebooks-secret-mood-manipulation-experiment/373648/.

Miller, S., & Weckert, J. (2000). Privacy, the workplace and the internet. *Journal of Business Ethics, 28*(3), 255–265.

Miyazaki, A. D. (2009). Perceived ethicality of insurance claim fraud: Do higher deductibles lead to lower ethical standards? *Journal of Business Ethics, 87*(4), 589–598.

Moor, J. H. (1997). Towards a theory of privacy in the information age. *ACM SIGCAS Computers and Society, 27*(3), 27–32.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review, 79*(1), 119–158.

Nissenbaum, H. (2009). *Privacy in context: Technology, privacy, and the integrity of social life*. Stanford, CA: Stanford University Press.

Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus*, *140*(4), 32–48.

Nozick, R. (1974). *Anarchy, state, and utopia*. New York: Basic Books.

Ohlhausen, M. K. (2014). Privacy challenges and opportunities: The role of the Federal Trade Commission. *Journal of Public Policy and Marketing, 33*(1), 4–9.

Persson, A. J., & Hansson, S. O. (2003). Privacy at work: Ethical criteria. *Journal of Business Ethics, 42*(1), 59–70.

Peslak, A. R. (2005). An ethical exploration of privacy and radio frequency identification. *Journal of Business Ethics, 59*(4), 327–345.

Phillips, R. A. (1997). Stakeholder theory and a principle of fairness. *Business Ethics Quarterly, 7*(1), 51–66.

Phillips, R. A., & Johnson-Cramer, M. E. (2006). Ties that unwind: Dynamism in integrative social contracts theory. *Journal of Business Ethics, 38*(3), 283–302.

Pollach, I. (2005). A typology of communicative strategies in online privacy policies: Ethics, power and informed consent. *Journal of Business Ethics, 62*(3), 221–235.

Popescu, M., & Baruh, L. (2013). Captive but mobile: Privacy concerns and remedies for the mobileenvironment. *The Information Society*, *29*(5), 272–286.

Posner, R. (1981). The economics of privacy. *The American Economic Review, 71*(2), 405–409.

Rachels, J. (1975). Why privacy is important. *Philosophy and Public Affairs, 4*(4), 323–333.

Regan, P.M. (2011). Response to Bennett: Also in Defense of Privacy. *Surveillance and Society.* 8(4).

Roman, S., & Cuestas, P. J. (2008). The perceptions of consumers regarding online retailers' ethics and their relationship with consumers' general internet expertise and word of mouth: A preliminary analysis. *Journal of Business Ethics, 83*(4), 641–656.

Rosen, J. (2001). *The unwanted gaze: The destruction of privacy in America*. New York: Random House Books.

Ross Jr, W. T., & Robertson, D. C. (2000). Lying: The impact of decision context. *Business Ethics Quarterly*, 409–440.

Rowan, J. R. (2000). The moral foundation of employee rights. *Journal of Business Ethics, 24*(4), 355–361.

Samarajiva, R. (1997). Interactivity as though privacy mattered. *Technology and privacy* (pp. 277–309). Cambridge, MA: MIT Press.

Schoeman, F. (1984). *Privacy: Philosophical dimensions of the literature: An anthology*. Cambridge, MA: Cambridge University Press.

Schwartz, B. (1968). The social psychology of privacy. *American Journal of Sociology, 73*(6), 741–752.

Shaw, W. H. (2003). *Ethics at work: Basic readings in business ethics*. Oxford: Oxford University Press.

Shields, M. (2014, October 22). Snapchat strikes an anti-native advertising tone. *Wall Street Journal*. http://blogs.wsj.com/cmo/2014/10/22/snapchat-strikes-an-anti-native-advertising-tone/.

Shilton, K., & Martin, K. E. (2013). Mobile privacy expectations in context. In *TPRC*.

Simmel, G. (1906). The sociology of secrecy and of secret societies. *American Journal of Sociology, 11*(4), 441–498.

Singleton, S. (1998). *Privacy as censorship: A skeptical view of proposals to regulate privacy in the private sector*. Cato Institute No. 295.

Sloan, R. H., & Warner, R. (2013). *Big data and the 'New' privacy tradeoff*. Chicago-Kent College of Law Research Paper No. 2013–33.

Sloan, R. D., & Warner, R. (2014). *Self, privacy, and power: Is it all over?* Chicago-Kent College of Law Research Paper No. 2014-04.

Smith, J. H., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly, 35*(4), 989–1015.

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review, 154*(3), 477.

Soule, E. (2002). Managerial moral strategies: In search of a few good principles. *Academy of Management Journal, 27*, 114–124.

Steel, E. (2011, October 27). U.S. Senator wants details on how MasterCard, Visa use customer data. *Wall Street Journal.* http://blogs.wsj.com/digits.

Stutzman, F., & Hartzog, W. (2012). Obscurity by design: An approach to building privacy into social media. In *CSCW' 12 workshop on reconciling privacy with social media*.

Tavani, H. T. (2008). Floridi's ontological theory of informational privacy: Some implications and challenges. *Ethics and Information Technology*, *10*(2–3), 155–166.

Tavani, H., & Moor, J. H. (2001). Privacy protection, control of information, and privacy-enhancing technologies. *SIGCAS Computers and Society, 31*(1), 6–11.

Thompson, J., & Hart, D. (2006). Psychological contracts: A nano-level perspective on social contract theory. *Journal of Business Ethics, 68*(3), 229–241.

Thurm, S., & Kane, Y. I. (2010, December 17). Your apps are watching you. *Wall Street Journal*. http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html.

Tufekci, Z. (2008a). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology, and Society, 28*, 20–36.

Tufekci, Z. (2008b). Grooming, gossip, Facebook and myspace. *Information, Communicaiton and Society, 11*(4), 544–564.

Turow, J., King, J., Hoofnagle, C. J., Bleakley, A. & Hennessy, M. (2009). *Americans Reject Tailored Advertising and Three Activities that enable it*. http://ssrn.com/abstract.

Ur, B., Leon, P. G., Cranor, L. F., Shay, R., & Wang, Y. (2012). Smart, useful, scary, creepy: Perceptions of online behavioral advertising. In *Presented at the proceedings of the eighth symposium on usable privacy and security* (p. 4). ACM.

Van Oosterhout, H., & Heugens, P. (2009). Extant social contracts in global business regulation: Outline of a research agenda. *Journal of Business Ethics, 88*(4), 729–740.

Van Oosterhout, H., Heugens, P., & Kaptein, M. (2006). The internal morality of contracting: Advancing the contractualist endeavor in business ethics. *Academy of Management Review, 31*(3), 521–539.

Wagner, K. (2014, May 16). Moves app backtracks, shares user data with Facebook. *Mashable*. http://mashable.com/2014/05/06/moves-data-sharing-facebook/.

Walzer, M. (1983). *Spheres of justice: A defense of pluralism and equality*. New York: Basic Books.

Walzer, M. (1994). *Thick and thin: Moral arguments at home and abroad*. South Bend, IN: Notre Dame Press.

Warren, D. E. (2003). Constructive and destructive deviance tn organizations. *Academy of ManagementReview*, *28*(4), 622–632.

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

Wempe, B. (2005). In defense of a self-disciplined, domain-specific social contract theory of business ethics. *Business Ethics Quarterly, 15*(1), 113–135.

Westin, A. (1967). *Privacy and freedom*. New York: Atheneum.

Winter, S. J., Stylianou, A. C., & Giacalone, R. A. (2004). Individual differences in the acceptability of unethical information technology practices: The case of Machiavellianism and ethical ideology. *Journal of Business Ethics, 54*(3), 2.