

PATRICIA A. NORBERG, DAVID A. HORNE,
AND DANIEL R. HORNE

Standing in the Footprint: Including the Self in the Privacy Debate and Policy Development

Personal information can be considered a shared good, since in many cases this information is accessed, used and distributed by more than just the individual. Thus, how personal information is defined or characterized and why it is valued differs based on whether or not one is the person whom the information describes. This article shows how current debates that influence policy and regulation are largely based on economic and social frameworks, points out policy issues that are evident due to the absence of a "self-perspective," and suggests how inclusion of the "self" might lead to more effective policy in the future.

Personal information sharing is core to both social exchange and, in today's economy, commercial interaction. Yet, the pervasive nature of information sharing and the commoditizing of personal details challenge the current perspective of informational privacy. This has led to continued debate over privacy and consumer/personal information as the needs of commercial and social constituents are balanced against the rights and perceived danger to the individual. This balancing act is exemplified in the recent media coverage of LifeLock, the identity protection firm that offers "fraud alert" coverage on credit files (Lieber 2008). Here, the commercial need for customer credit information creates an opportunity for identity theft, which leads to paid services to protect consumers from such danger.

For an individual who is unequivocally and permanently attached to a set of personally identifying characteristics, the special nature of self-perception and the value of identity can be compromised when both descriptive and intimate information is provided to another, either in a social situation or in a commercially base exchange. For the permanently attached body, personal details that are shared, be it for goal achievement or otherwise, may be thought of as sacrifices of the self (Belk 1988).

Patricia A. Norberg is an associate professor in the Department of Marketing and Advertising, Quinnipiac University (patricia.norberg@quinnipiac.edu). David A. Horne is a professor in the Department of Marketing, California State University-Long Beach (dhorne@csulb.edu). Daniel R. Horne is an associate professor in the Department of Marketing, Providence College (dhorne@providence.edu).

Such consideration of self-sacrifice is in contrast to the more prevalent privacy debate perspectives that personal information exchange involves a social dilemma and/or one of economic value, property, and shared use (Cress, Kimmerle and Hesse 2006). Where the social perspective rests on the assumption that improving the overall welfare of the group directs the choice of what, if any, information should be publically disclosed, the economic perspective focuses on the debate over whether personal information should be subject to control beyond that of the individual; that is, how others' information is retained and used/reused and to what extent this leads to greater economic value.

While researchers have not neglected pursuing theoretically grounded arguments to debate the privacy issue, collectively we have been remiss in mostly excluding theory of the self—the individual and his/her relationship to the information *in isolation of any exchange* that may take place. Such a discussion is likely to be enlightening, as it is this “absolute” view that in whole or part may drive the cognitive and emotional appraisals associated with the sharing of personal information in both commercial and social situations. As highlighted later in this article, we suggest that the underlying dynamic of the self plays an important role in delineating what is and is not private and drives the success or lack thereof in the outcomes of various regulatory and/or marketplace initiatives.

In the following text, we present a brief discussion of privacy and then present the economics-based rationale for information sharing, the value of information in a social system, and finally the value of information to the self. Policy developments based on the economics and social frameworks are also included. Emphasis on the third view, the self-perspective, constitutes the contribution of this article. Although not fully integrated into the political discourse on privacy now, we argue that our assessment of the interactions between the economic-social aggregate and the individual, and the resulting action–reaction interplays, will offer new perspectives for privacy discussions and policy direction. The article closes with a discussion regarding the trade-off among economic, social, and self concerns and the importance of an expanded yet integrated view of privacy that can accommodate the concerns on all three dimensions.

PRIVACY

Privacy is a concept traditionally associated with personal interactions. In marketing exchanges, a key question of interest is whether or not “privacy” of the consumer in a marketing context can be thought of in

the same way as “privacy” in a personal, nonmarketing context. On an abstract or philosophical level, privacy is very much an individualistic concept and may be equated to an individual’s preference for keeping inaccessible aspects about one’s self (c.f. Edmundson 2004). From the viewpoints of marketing practice and policy development, the concept of privacy must be made actionable, and thus more concrete definitions of privacy have been offered by both marketing (e.g., Culnan 1993; Goodwin 1991) and legal scholars (e.g., Cohen 2000; Schwartz 2004; Solove 2001; Warner 2005; Warren and Brandeis 1890). With reflection and debate, several aspects of consumer privacy have gained considerable attention from researcher: (1) the right to be left alone (Foxman and Kilcoyne 1993; Goodwin 1991), (2) the right to control one’s information or limit access (Foxman and Kilcoyne 1993; Goodwin 1991; Sheehan and Hoy 2000), and (3) the right to protect one’s individuality (Wasserstrom 1978). The right to be left alone relates to a consumer’s need to control when and where they are contacted (maintaining private time and space), and for what purpose. The right to control one’s information or limit access relates to the consumer’s need to have a say about how their personal information is used by commercial exchange partners and whether or not that information should be used or shared with third parties. Lastly, the right to protect one’s individuality relates to an individual’s need to define themselves and not be defined by any other entity. In other words, this third aspect concerns the commercial mining of a consumer’s personal details to develop an understanding of all that can be learned about them.

Policies have been developed to address the first two definitional components, yet the third has been difficult to accommodate using our existing frameworks. As will be emphasized in this paper, bringing the right to protect one’s individuality into policy debates can be fruitful, though it may also be in a very real sense at odds with the current social and economics perspectives that currently prevail. Table 1 identifies the major components and considerations for each of the three perspectives discussed in this paper.

ECONOMIC, SOCIAL, AND SELF-PERSPECTIVES

The Value of Personal Information to the Economic System

Our economic system relies on the idea of exchange, whereby transactions, either direct or indirect, require all parties to surrender something of value in order to acquire something they value more

TABLE 1
Perspectives on Privacy

Economic:

Enables information flow—Anything that inhibits information flows inhibits commerce and pushes cost up.

Theoretical Emphasis: Coproduction

- Consumer information is input; institution decides on whether or not coproduction is technologically and economically feasible.
- Output generated with coproduction should be greater than if coproduction was not present. Otherwise, there would be no additional value.

Issues:

- Assumes knowledge of opportunity costs on the part of consumer producers.
- Incentives to shirk in production activities if hard to detect.
- Observability = Opaque

Economic Perspective and Monitoring Role of Government:

- Current legislation protects right to be left alone (DNC, Can-SPAM) and right to control access to information (credit freezing and internet advertising). From economic perspective, these are inhibitors to commerce.

Social:

Enables information flow—Individuals have an obligation to participate for overall welfare of the group.

Theoretical Emphasis: Social Dilemma

- Unfair to take advantage of a social system without contributing to it.

Issues:

- Assumes consumer can manage the contribution process and determine the fair share of contribution.
- Assumes individual shares more information as the relationship strengthens.
- Observability = Masked

Social Perspective and Monitoring Role of Government:

- Current legislation protects consumer control over information.

Self:

Gatekeeper to information flow—Individual manages appropriate level of disclosure to safeguard identity.

Theoretical Emphasis: Self-Perception

- Individual has right to maintain their identity without infringement that is not transparent to them.

Issue Resolution /Benefit of New Perspective:

- Satisfies issues with economic perspective by making the process of coproduction transparent. Consumer participates in deciding if coproduction is technically/economically feasible.
- Satisfies issues with social perspective by allowing for participation in determining fair level of contribution to social welfare.
- Less incentive/opportunity to shirk.
- Observability = Transparent

Self-Perspective and Monitoring Role of Government:

- New role of government is to oversee on a broader level, instead of enforcing specific/narrow regulations that do not keep up with technological change.
 - Business becomes the guardian over information (the organization is granted access to consumer and therefore should bear more of the risk of information misuse, be it through secondary sharing, theft or other misuse).
 - Consumer decides on the degree/pace of disclosure and extent of use, thus participating in overall welfare while ensuring inputs to coproduction are valued appropriately.
-

(Alderson 1965; Gundlach 1996; Houston and Gassenheimer 1987). A truism that you cannot receive “something for nothing” is embedded in the consumer psyche, and there exists an expectation that some “cost,” whether it is financial, social, or time, is associated with nearly every activity undertaken. In addition, advanced market economies have come to rely extensively on consumer information to design product offerings which appeal to current and perspective customers and to efficiently and effectively communicate with these same consumers/customers.

With regard to efficiency, certainly modern levels of economic activity and growth would not be possible without smooth flows of information, and economic theory suggests that anything that inhibits information flows inhibits commerce and increases costs (Stigler 1961). This perspective argues then that the ability of a system to deliver maximal benefit is impeded when the market and the opportunities it affords cannot function optimally. People’s real and efficient choices are constrained when they know less about the marketplace, and the existence of informational asymmetries is thought to promote less efficient markets (Akerlof 1970).

With regard to *design* of products and services, the input of information from consumers in economic terms can be conceived as a type of coproduction, since the consumer contributes this information, like a raw material, toward the production of other goods and services. Coproduction involves the combined efforts of regular producers, who directly produce goods and services for exchange, and consumer producers, who indirectly contribute by engaging in various activities, in this case by disclosing personal information, to create value (Parks et al. 1980). Interestingly, though the consumer contributes to value creation in this economic framework, it is worthy to note that *institutions* determine the level at which coproduction is technically and economically feasible and when to discourage coproduction based on inefficiency (Parks et al. 1980). Thus, they are primarily in charge of determining the appropriate mix of regular and consumer activities (and therefore degree of consumer information needed) to produce goods and services. The ensuing outputs from processes that rely on coproduction should be greater than the outputs produced without coproduction (Parks et al. 1980). At the point where no additional value is produced via increases in coproduction (e.g., increases in consumer information disclosed), it should not continue. For example, a consumer’s credit history is a required raw material for efficient lending, and thus access might be considered necessary to create value. However, whether or not a consumer owns a dog does not relate to, nor provide raw material for, a decision to extend credit, and therefore

would not add value or would be considered unnecessary in facilitating the lending process.

Lastly, if we rely on economic arguments, then we must recognize that the economic perspective would include discussions of (1) "wage rates" in which the contributing inputs should be translated for regular producers and (2) opportunity costs (wage equivalents) associated with the inputs of consumer producers. In these interdependent relationships, however, the apportioning of benefits and costs might be difficult to determine. Owing to this, and as argued by Parks et al. (1980):

Regular producers and consumer producers may face incentives to shirk in their productive activities if they anticipate that their shirking will go undetected due to the difficulty of monitoring productivity. Where undetected shirking is a possibility, market exchange may fail as producers of either type cannot be sure that others will conform to their sides of the bargains. Interdependent production relationships may be doubly threatened by shirking where the consumer producer activities are collective in nature. (p. 8)

The often opaque nature of informational transactions creates opportunities to shirk on both sides. Firms can utilize the raw material (information) in ways that are unimagined and unwanted by consumers which potentially creates a moral hazard. Consumers, on the other hand, can provide adulterated or falsified raw materials, that is, distort the truth or lie (Horne, Norberg, and Ekin 2007).

Current regulatory debate does indeed have a definite "information as economic enabler" component, focusing on free or restricted flow of so-called consumer producer inputs. For example, Richard Brodsky's (Democrat, New York State Assembly) "Third-Party Internet Advertising Bill of Rights" is vigorously opposed by the Interactive Advertising Bureau (IAB), whose stance is that targeted advertizing helps drive the internet economy and increases access through free services and content. Clearly, the industry group is categorizing information as an economic stimulus that would be harmed by any intrusion from an outside hand. Representative Brodsky's position suggests that the model of noninterference is basically one-sided against the individual consumer. Given the absence of national legislation, a major state such as New York passing such a consumer-centric law could have far reaching impact and thus the industry's collective efforts to limit or completely thwart the bill (Corbin 2008). Likewise, all the existing and pending legislation concerning the "freezing" of access to consumers' credit histories (as a means to thwart

identity theft) are opposed by credit bureaus and many retailers and financial institutions who offer "Instant Credit," as they perceive such legislation as an impediment to the free flow of information and thus business opportunities. For example, during the three years it was under consideration, the debate about Georgia's new "credit freeze" law that went into effect August 1, 2008, was consistent with this economic perspective. The resulting law fashioned innovative compromises that allowed temporary "thaws" of the freeze for literally 15 minutes to allow a credit application to be processed. Even with time limitations, commerce could still continue unabated when high motivation exists (Peralte 2008).

Consumers have shown disregard for some of these economic arguments, especially when aggregately aggravated. The Do-Not-Call Registry (the FCC's and FTC's response to Do-Not-Call Implementation Act-Public Law 108-10 signed March 11, 2003) and Can-SPAM (actually the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003-Public Law 108-187 signed December 16, 2003) have been enacted to address consumer's desire, first to be left alone and not bothered by unwanted telephone calls or pornographic e-mail solicitations, and second to control one's contact information to those deemed worthy in the consumer's mind. The strong and persistent voice of consumers convinced regulators to act against the interests, economic arguments, and substantial lobbying efforts of direct marketers (FTC 2000). As listed in its 2007 Annual Report, there were over 107 million phone numbers included in the Do-Not-Call Registry by the end of FY 2005 (FCC 2007). The FCC reports more people adding their *cell* numbers to the list as an urban myth suggesting that a national 411 database of mobile phones will soon be available to telemarketers continues to circulate. Calls to phones, pagers, and other devices that require consumer payment for use are in most cases off-limits for commercial solicitations (FCC 2008).

In essence, these regulations attempt to address the right to be left alone and the right to control information or limit access, but the patchwork of bills to address these specific issues might be neglectful in addressing the more important issues that seem to underlie the economic perspective—the need for transparency in the system to prevent shirking and/or malfeasance, thereby promoting a balance between institution *and* consumer participation in determining appropriate levels of input for the production of products and services that are superior to those absent of such coproduction. With respect to the economic perspective influence on policy, the absence of recognition that the consumer should have a role in determining the appropriate level of resource contribution is problematic. Consideration of a "self- perspective," as will be discussed later on the

in the paper, would call for such a role whereby the governing bodies may become overseers, not regulators *per se*.

The Value of Personal Information to the Social System

The social perspective ties into economic efficiency arguments to some extent, but rests more on the position that communication is the foundation of social networks, and personal information sharing is critical for such a social system to function. It can be deemed unfair that one could take advantage of an efficient system yet not have contributed to the underlying data sharing process that makes it all possible, as this would create a social dilemma (Sell and Wilson 1991). The perceived benefit to the individual of not having their data profiles comingled with millions of others does not outweigh their obligation to participate, even when they are not overtly visible in the market. Defining value, likewise, is in terms of societal benefit, but this presents a challenge, since "overall welfare of the group" depends on numerous underlying social arrangements (Coase 1960).

As part of numerous social arrangements, individuals take risks in sharing parts of the "self" with others, as the other parties can use the shared information in unexpected and/or undesirable ways. This is similar to the economic argument of interdependence. However, individuals manage social interactions and relationship building processes by disclosing information about themselves in ways that might minimize risk, while also securing positive and ongoing relationships (Zwick and Dholakia 2004). For example, an individual might initially approach social discourse by divulging superficial information about himself/herself. Over time, the comfort or trust level in the exchange partner increases and more intimate information is shared as the relationship strengthens (Archer 1980).

Yet, embedded in societies are commercial participants, and thus the exchange of information between members of a society includes commercial entities. For these entities to survive, they also must rely on relationships, also known as social networks. The need for long-term associations with customers and business partners that result in a better understanding of exchange partners (or "knowing" who they are) is often emphasized in the relationship marketing and retailing literature (Mackey 2005). Although a parallel can be made between personal exchanges and marketing exchanges based on this perspective, the differentiating characteristics of commercial-consumer interactions are what make the comparison questionable.

The contentiousness occurs because observations and the management of information sharing in commercial contexts are not in the open arena but rather exist in an unseen world of bits and bytes (Warner 2005). Thus, the individual's ability to control interactions on his/her own terms is diminished, tying directly back to the issue raised before about the importance of the individual to control one's information. Although casual acquaintances, such as those on a random air flight or more regularly on a commuter rail, may exchange pleasantries or even some fairly personal information, access to information among most passengers is limited to that which can be directly observed and the bits and pieces of personal information that might be exchanged in the process of small talk. Certainly, it would be more difficult for the acquaintance to access additional information beyond that which is exchanged on the commute without the active participation of the subject party.

In contrast, though a customer may provide information to a business to complete a transaction and/or to secure future successful transactions, this information provided in a specific context can and often is then combined with other data about the individual (i.e., that was purchased or retained from other sources). Here, the consumer does not realize that they are even "sharing" information, and rarely does a consumer provide information to a company for the purpose of sharing the information with other businesses (hence concern over secondary use). Although the data collection may occur in an area where the consumer reasonably presumes that their personal information is not used for any purpose other than the immediate one, these "observations" may be added to historical databases and data warehouses. The various discreet marketplace interactions that are collected over time form comprehensive dossiers of individual consumer behaviors. Here then, the ability to aggregate data produces a much richer and arguably better predictor of future commercial interactions than is available from the record of a single marketplace interaction. Likewise, the ability to control or limit access by consumers is markedly absent.

Clearly, this goes far beyond the acquaintance on the train accessing information in repeated exchanges. Additionally, like the probable expectation about information sharing by the acquaintance on the train, information provided to close a particular transaction with a commercial entity does not imply permission for the marketer to telephone or e-mail the customer with other marketing pitches. There is an implied "breadth and depth of permission" when a consumer shares information with a transacting marketer (Krishnamurthy 2001). When marketers use personal information beyond the implied permission parameters, they

may trigger a general level of dissatisfaction with business practices and cause hesitancy on the part of consumers to provide information for future business purposes.

Thus, though there is a common thread in both interpersonal and commercial social exchanges, managing interaction with a commercial partner is characteristically different from managing interaction with another person. Clearly, every time anyone ventures into public, they are giving even a casual observer the right to collect data about their appearance and their behavior. Manner of dress, speech, transportation, destinations, associates, and so forth all are available to the more astute student of observation. However, in modern times, trained data miners, removed though they may be from the actual subjects they study, can produce a bounty of information about shopping habits, payment means, patterns of consumption, levels of income, etc. Some would suggest that there are no grounds to restrict this level of data gathering as it hinges on the observer's right to observe data and then make reasoned predictions based on the patterns found therein (Zimmerman 1992). They argue that any person or entity that makes the effort to gather and classify this data should be able to benefit from its use, and the resultant data profiles now "belong" to the gatherer.

With regard to control over information, legislation has been enacted to inform consumers about the possible use and/or restrictions on information related to health care (Health Insurance Portability and Accountability Act of 1996) and financial information (Gramm-Leach-Bliley Financial Modernization Act of 1999), has limited access to video rental records (Video Privacy Protection Act 1988), has protected information disclosed by children (Children's Online Privacy Protection Act 1988), and has prompted the posting of privacy policies on corporate websites (FTC 2008). Recent legislative proposals that also attempt to address some of this concern have clear contractual components that revolve around the consequences and need for restoration of protection following data "breaches." Senators Leahy and Specter's S.495, the Personal Data Privacy and Security Act" (PDPSA), outlines requirements of notice of breaches by the data collection entities. Their language is quite specific with regard to type of miscues, the time taken to inform consumers, and enforcement by the FTC, Secret Service, and state and Federal attorneys general. Tellingly, "breach" is a term familiar in contract law that figures heavily in S.495 as well as Senator Feinstein's S.239 and Representative's Rush and Stearns's H.R. 958, which have to do with information protection. The FTC would be charged with enforcing any lapses. Still,

these are remediations, while the crux of the issue is that personal data of an individual was somehow misused in the first place.

These regulations treat the arrangement between the consumer and the data gatherers as some sort of contract that must be “fixed” when problems occur. However, the fixing is rooted in the notion that parties have come to some sort of agreement as to the responsibilities and liabilities of each side and the specific remedies that are appropriate for failure to conform to the terms of the arrangement. They are also predicated on the ability of the informed consumer to self-protect (Beales, Craswell, and Salop 1981). The concept of “self” and its impact on the privacy transgressions does not appear to be addressed in any of the proposed legislation, nor do the remedies make attempt to restore the “self” to their prebreach position.

Considering the Value of Personal Information to the Self

Altman and Taylor (1973) described an individual’s “self” in terms of concentric circles, whereby intimate details about the individual are contained in the innermost circles and less intimate details reside in the outer circles. Inner circles are more deeply rooted in the self and therefore include information that a person would want to safeguard the most. Belk’s (1988) extensive review of the findings from self-perception research specifically focuses on various forms of possessions as being associated with extensions of the self. In one study, personally identifying characteristics and attributes were rated third out of eight categories associated with the self, following after body parts and psychological/intraorganismic processes (Prelinger 1959). McClelland (1951) suggested that control dictates the strength of which a possession is perceived as part of the self, and Prelinger’s (1959) findings support this contention. Belk (1988) also asserts that possessions that are unintentionally lost result in a reduction of the self, and an individual’s first reaction following a loss is to attempt to restore the self. He argues that the loss of possession can take place when “functions and property of individuals are taken over by institutions” (p. 143), even when that takeover was not intended to create a loss. Finally, Belk (1988) suggests that one’s possessions can become contaminated if another is incorporated, however involuntary. On the basis of Prelinger’s (1959) findings, we would expect stronger perceptions of loss or contamination when the possession is personal information as compared with other forms of possessions.

Although these self-perception conceptualizations may be familiar to scholars who study the behavior of consumers, these do not appear to be emphasized in the application to privacy. Instead, when framing the discussion of privacy as one of information, we seem to strip the context of the self away. This may be due to the possibility that from the self-perspective, economic prosperity, and social contribution do not offset either preferences for solitude and privacy, the risk associated with the potential Orwellian misuse of centralized databases (Warner 2005), or even the discomfort of knowing that the department store at which you shop keeps purchase records including that of your increasing pant waist size.

An important issue then is that of misperception in current policy with respect to protection; the notion that one's personal data (including phone number, social security number, age, height, and weight, etc.) are protected to at least the same degree as says a television may be erroneous. It is likely implausible to the typical consumer that their personal belongings do *not* necessarily include their personal information. Ironically, though personal data profiles may be protected by property rights, they belong to the multiple entities (Internet search engines, credit-reporting firms, direct mailing list suppliers, financial institutions, etc.) that compiled the information. Presently, most data about the behavior of a consumer are not the consumer's to own or control.

Research in the extended self offers insights into the types of disclosure and "self-reactance" behaviors consumers engage in to maintain the self—behaviors that we should expect with regard to privacy and personal information sharing (see also Milne, Bahl and Markos 2008). It is for this reason that we suggest it is appropriate to explore potential contributions to policy development from this theoretical perspective. While it clearly is not new to contend that consumers want to control their identifying details, we suggest now that this desire for control interferes with achieving the idealistic social and economic objectives set forth currently in regulatory and marketplace initiatives and should be considered by policy makers. The self-literature provides a strong support for how intimately a "person" and their information are matched. In essence, they are truly the same thing; personal information from a self-view is part of an individual's humanness.

With such a perspective, it makes more sense to massage the current economic and social perspectives on "contribution" to include more consumer participation about the level of input, as it is a "part" of them that is given up. In other words, allow the consumer the transparency

to understand the degree to which they are able to keep their identity intact—to keep things personal to them, well, personal. Alternatively, firms and other social agents must become the guardians over that information, and they become the agents fully charged with protecting it. On the basis of this alternative, it would appear that we need to shift the responsibility of “fixing” such things as data breaches and information theft back onto institutions or others in charge of governance over the data. Clearly, that is not the case today, where a consumer needs to spend hours on the phone fixing credit files, canceling credit cards, calling regulators and police departments in order to communicate with many stakeholders that someone else has “deceived them.” In real wages, that is a costly process.

PUBLIC POLICY GAP

To address the privacy question effectively, it is important to understand why consumers engage in behaviors that limit firm access to personal details and why firms engage in information sharing without consideration of any “self” behind the data. In other words, we must consider that the lens of the marketer is very different from the consumer’s own lens and use this as a basis for developing more effective exchange environments and public policies employed to create them.

On the one hand, from the firm’s perspective, it might seem reasonable to argue that the consumer is part of the (marketing) channel, in that information provided is a resource and facilitates efficient movement of goods from the producer to other end users. Consistent with the concept of coproduction, one would argue that the consumer should be afforded channel member rights and privileges that are contractually arranged to protect property interests of each channel member. Yet, how that contractual arrangement should be structured and how the contracts might be enforced are really at issue for policy makers under this structure (Ayres and Funk 2003). This perspective also implies that consumers not only have access to full information but also think like *homo economicus*.

In contrast, from the consumer’s perspective, the notion of being part of a marketing channel is likely foreign to how consumers envision their roles in the marketplace. Exchanges of information may not be thought about so much from a property perspective as one stemming from the self, as embedded in society or in an absolute sense. Thus, to the consumer who is unquestionably attached to the information that describes “who they are,” giving up information can mean (1) contributing to the social

whole, though most neither consider nor place a high value on this; or more importantly (2) sacrificing part of the self, a decision that is often uncomfortable and unwanted (c.f. Belk 1988). Because consumers are probably not thinking from a contractual perspective, they might be more likely to deal with the discomfort of exposing the self by choosing methods to protect this valued possession. Consequently, their behavior takes on a similar look and feel as those behaviors they exhibit in any other social exchange (e.g., engaging in coping behaviors like refraining from offering details about the self, misrepresenting details about the self, avoiding the interaction completely, etc. [Horne, Norberg and Ekin 2007; Lwin and Williams 2003]).

Along the same line of reasoning, the consumer may overlook, ignore or at best only briefly attend to the policies and procedures communicated by firms, such as notice (Milne, Culnan and Greene 2006), and by regulators, such as healthcare privacy disclosures, because they just do not view the relationship as one of property sharing. Thus, from the consumer perspective, greater contractual arrangements could be just as ineffective as any other legal-based arrangement that is developed to spell out the terms of an "information sharing" agreement from the channels view.

Alternatively, privacy policy might instead be built around the notion that we institute laws based on what we as a society want to realize as valuable (Warner 2005). Commoditizing privacy ignores the issue of how one, through his/her own active and passive disclosure behaviors, may no longer be afforded the ability to establish diversity of the self in society. Yet, isn't it the diversity of selves in society truly what we wish to promote? There are cases where social good and protection of freedom outweighs the benefits of efficiency and laws are enacted to protect the greater good and individual identity at the expense of efficiency, as in the case of the 6th Amendment to the U.S. Constitution, which guarantees a jury of peers even though a bench trial would certainly be more economically efficient. Similarly, it may be quite beneficial to consider where and how protections of individual freedoms in the area of privacy outweigh what might only *appear* to be economic and social gain.

If, as suggested by Goren (2003), the technological advances in expanded communication of personal experiences and interpersonal relations lead to disembodiment and detachment in our "highly publicized communication world," then what actually is the social benefit? An aggregate efficiency does not necessarily mean optimal conditions for the constituent pieces. If members of society always feel shared, when in

fact a sense of aloneness is essential to normal development (Yerushalmi 1992), then the potential of compromising the construction of a secure and functional society should be considered, as individuals are essentially the building blocks of this.

Goren (2003) argues that the collapsing of temporal and psychological private and public space and the expectation of immediate communication leave little room for privacy or little time for emotional or mental processing. She goes on to argue that on both the social and the economic level, the commodification of experience is supported by consumerist attitudes, whereby our consumerist culture might be due in part to "the lack of fulfillment resulting from this unnamed, subtle new detachment from experience in today's supertechnology era" (p. 503).

If this dissolution of the self potentially has a positive impact on short-term economics but a negative impact on the societal development, then should we not as social scientists investigate how regulation or lack thereof might be reinforcing one of our governmental objectives while impairing the ability to achieve the other? For instance, onerous information requirements may have kept those who early on were infected with human immunodeficiency virus (HIV) from seeking treatment, thereby increasing the overall cost to society through the care and treatment of those subsequently infected. The economic benefits potentially deteriorate in the long run as misaligned incentives from improper or missing regulations erode overall production and innovation.

In this sense then, the legal discourse should not just be one of property, but one of social good and the preservation of the self. The individual with HIV does not want to have his/her "life story" passed along and repackaged, but merely wants to provide enough information about his/her condition to identify a cure and to protect others in the future. Such conversations will bring front and center the possibility of limiting data sharing beyond the initial reason for collection in the commercial realm while not infringing on the social welfare that can be brought about from aggregated data (see Health Insurance Portability and Accountability Act, HIPAA, 1996). Self-theory, in tandem with other consumer theories where appropriate, may better inform our decisions about privacy and other public policy areas that relate to consumer interests. We argue that such theory development is critical to understanding interactions and externalities resulting from any changes that take place to promote economic development or social welfare.

POLICY IMPLICATIONS

In the above review, we suggest that the privacy debate thus far has accommodated both social and economic perspectives, but to a lesser extent it has the self-perspective motivated policy initiatives or testing. Through use and reuse, alienation of information at the discretion of multiple parties is commonplace, and the characteristics and values associated with the self are markedly absent. Yet, the self has not been emphasized as the crux of the privacy problem, even though the issues actually stem from the self by very nature of the term "privacy."

Implicit in this discussion is that the notion of privacy stemming from the individual suggests that privacy is not invariant across cultures. For instance, collectivist cultures may broaden the very definition of personal privacy to include family or clan (Horne, Houston and Horne 2008). Yet, in cultures thought to be more similar to the United States, the importance of self may be seen in policy applications. Personal information in commercial transactions is handled differently in the European Community where the idea that privacy is a "fundamental right" has been officially recognized since the adoption of the European Privacy Directive in 1995 (Barnes 2006). The directive makes the individual's interest in their personal data superior to the organization's interest in the use of the data to promote commerce or the general free flow of information (Barnes 2006). While not as restrictive as the European model, it is felt that Canadian law is moving toward a more formal recognition of the preferred interests of the consumer over the interests of organizations (McClennan and Schick 2007).

In terms of policy, we might make the argument that only by examining how individuals are likely to respond to legislation can we understand the extent to which policy initiatives may be effective. So, instead of the unit of analysis being only society, it must also include the individual. For example, HIPAA may appear effective at the societal level, but that assumes that individuals comply and understand why they are complying. HIPAA appears to provide protection at the aggregate level because parties actively consent. But if consumers do not know to what they are consenting (U.S. General Accounting Office 1998), then the policy cannot be considered effective.

Similarly, other regulatory outcomes provide examples of theoretical efficacy while the actual execution thereof is problematic. Privacy statements may appear to be effective, as the FTC states that almost all of the top 100 commercial sites have posted privacy policies. However, if few read or understand them (Milne, Culnan and Greene 2006; Turow

2003), or few understand the associated risk exposure (Miyazaki and Fernandez 2000), their necessity is called into question. Without this basic level of apprehension and comprehension, compliance may be achieved on the surface but with no substance.

The simplest way to incorporate self into privacy policy and regulatory frameworks would be to adopt more of an “opt-in” culture as is found in Europe, and increasingly in Canada. By forcing consumers to act, opt-in regulation empowers them to explicitly decide the value of information. From an organizational standpoint, this entails a shift of consumer surplus back to the consumer. If the information in fact has sufficient value, then incentivizing the consumer to participate would entail more of a sharing of the surplus that currently exists rather than a wholesale transfer.

In addressing future policy initiatives, it might be fruitful to start with the question, “If we develop legislation that does X, then how will consumers individually respond and what is the long-term effect of those individual responses and coping strategies?” In other words, we need to examine the simple effects, not just the omnibus. Although scholars study some of these phenomena in academic settings, such studies should be part and parcel to policy development. Starting points in the investigation can include examinations of the individual reactions to responses to privacy breaches and the related commercial circumventing of obligations, given the current regulatory environment. For example, individuals may be using a variety of strategies to attempt to manage information exchanges (Horne, Norberg and Ekin 2007), even in light of corporate policies and current *ad hoc* regulations (Lwin, Wirtz and Williams 2007). Such strategies, though allowing the consumer to in part protect their personal details, might not enhance the social or economic well-being that is of interest to policy makers. Additionally, by finding the thresholds in information collection where consumers are most likely to use coping strategies that create negative socioeconomic externalities, policy makers can better address the information collection limitations that should be enforced. Here, the objective would be to allow commercial entities to collect information that facilitates transactions but not to collect information that ultimately may lead to real or perceived manipulation of consumers.

From the commercial side, taking a pulse with regard to how much information is being collected is warranted and can provide insights into how much of the self has actually been “commoditized” and how effective this commoditization actually is in optimizing exchange to all constituents. Consistent with the previous comment then, before moving forward with policy, it might be prudent to find the dividing line between

what data organizations really need to collect to facilitate commerce and that which they collect and use to manipulate human behavior.

SUMMARY

What we have seen so far puts public policy in a quandary in terms of how to approach the data as personal property issue. In some instances, personal information has a history of being a “free” or “public” good. Information, such as that contained in land records and transactions is deemed critical to honest and open markets. So too, the fair and efficient collection of real estate-based taxes is based in part on this transparency.

Commercial organizations would argue that economic forces suggest that treating individual data facts and data profiles as personal property would be a deterrent to an efficient economic system. Legal opinions have given the data gathered by others the full protection of 1st Amendment free speech rights and then argue that a property right protection would have little recourse for violations anyway since harm to an individual would be hard to quantify. A suit seeking redress based on this concept would be economically infeasible to prosecute. Yet, for consumers and their advocates, some solution and feeling of restoring their own control is a steady message. The continuing public appeals have not gone unnoticed by the legislative bodies at both the state and federal levels as numerous statutes are presented and debated, as previously discussed.

In the end, we must ask ourselves, exactly what are our laws attempting to do and why? Promoting disclosure by claiming data is protected may be one goal, while moderating the disclosure process and helping the consumer understand the risk/benefit of disclosure (thereby aiding choice) is quite another. We suggest further consideration of limiting collection and disclosure by attempting to inform individuals when and/or why not to disclose. This is a third and most difficult agenda that has not been at the forefront of policy development. Although it is difficult to integrate into legal doctrine when the long-term effects of not disclosing (as discussed in the above section) are discounted in relation to the more immediate economic benefits, regulators might seek to level the playing field such that consumer participants in the marketplace truly understand why they are engaging in exchange and the outcomes of such exchanges in terms of “self-sacrifice.” In short, regulations that foster transparency and empower the consumer, thereby passing control back to the consumer by allowing their choice to be more readily recognized and exercised, will likely promote individual well-being as well as that of society and commerce.

REFERENCES

- Akerlof, George A. 1970. The Market for Lemons: Qualitative Uncertainty and the Market Mechanism. *The Quarterly Journal of Economics*, 84 (3): 488–500.
- Alderson, W. 1965. *Dynamic Market Behavior*. Homewood, IL: Richard D. Irwin.
- Altman, I., and Taylor, D. 1973. *Social Penetration: The Development of Interpersonal Relationships*. New York: Holt, Rinehart, & Winston.
- Archer, Richard L. 1980. Self-Disclosure. In *The Self in Social Psychology*, edited by Daniel M. Wegner and Robin R. Vallacher. New York: Oxford University Press.
- Ayres, Ian and Mathew Funk. 2003. Marketing Privacy. *Yale Journal on Regulation*, 77 (Winter): 1–61.
- Barnes, Morey Elizabeth. 2006. Falling Short of the Mark: The United States Response to the European Union's Data Privacy Directive. *Northwestern Journal of International Law & Business*, 27 (Fall): 171–197.
- Beales, Howard, Richard Craswell and Steven Salop. 1981. Information Remedies for Consumer Protection. *The American Economic Review*, 71 (2): 410–413.
- Belk, Russell W. 1988. Possessions and the Extended Self. *The Journal of Consumer Research*, 15 (2): 139–168.
- Coase, R.h. 1960. The Problem of Social Cost. *The Journal of Law & Economics*, 3 (Oct): 1–44.
- Cohen, Julie E. 2000. Examined Lives: Informational Privacy and the Subject as Object. *Stanford Law Review*, 52 (5): 1373–1437.
- Corbin, Kenneth. 2008. Mixed Reaction to Pending Online Ad Legislation. InternetNews.com, March 26.
- Cress, Ulrike, Joachim Kimmerle and Friedrich W. Hesse. 2006. Information Exchange with Shared Databases as a Social Dilemma. *Communication Research*, 33 (5): 370–390.
- Culnan, Mary J. 1993. How Did They Get My Name? An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use. *MIS Quarterly*, 17 (3): 341–361.
- Edmundson, William A. 2004. Chapter 19: Privacy. In *The Blackwell Guide to the Philosophy of Law and Legal Theory*, edited by Martin P. Golding and William A. Edmundson. Oxford: Blackwell Publishing.
- FCC. 2007. Annual Report on the National Do-Not-Call Registry. Available online: www.fcc.gov/cgb/donotcall/#moreinfo. (Released January 26, 2007).
- FCC. 2008. FCC Consumer Advisory: The Truth about Wireless Phones and the National Do-Not-Call List. Available online: www.fcc.gov/cgb/consumerfacts/truthaboutcellphones.html.
- Foxman, Ellen R. and Paula Kilcoyne. 1993. Information Technology, Marketing Practice and Consumer Privacy: Ethical Issues. *Journal of Public Policy & Marketing*, 12 (Spring): 106–119.
- FTC. 2000. Before the Federal Trade Commission—In the Matter of Telemarketing Review Comment. File Number P994414. Available online: <http://www.ftc.gov/bcp/rulemaking/tsr/comments/dma.pdf>.
- FTC. 2008. Enforcing Privacy Promises: Section 5 of the FTC Act. Available online: <http://www.ftc.gov/privacy/privacyinitiatives/promises.html>.
- Goodwin, C. 1991. Privacy: Recognition of a Consumer Right. *Journal of Public Policy & Marketing*, 10 (Spring): 149–166.
- Goren, Elizabeth. 2003. America's Love Affair with Technology: The Transformation of Sexuality and the Self over the 20th Century. *Psychoanalytic Psychology*, 20 (3): 487–508.
- Gundlach, Gregory T. 1996. Exchange Relationships and the Efficiency Interests of the Law. *Journal of Public Policy & Marketing*, 15 (Fall): 185–202.
- Horne, Daniel R., Patricia A. Norberg and A. Cemal Ekin. 2007. An Exploration of Consumer Lying in Information-based Exchanges. *Journal of Consumer Marketing*, 24 (2): 90–99.
- Horne, David A., H. rika Houston and Daniel R. Horne. 2008. All in the Family: Toward a Consumer-Centered Framework of Cross-Cultural Privacy. In *Marketing and Public Policy Conference Proceedings*, edited by John Kozup, Charles R. Taylor and Ron Paul Hill (212–219). Chicago: American Marketing Association.

- Houston, Franklin S. and Jule B. Gassenheimer. 1987. Marketing and Exchange. *Journal of Marketing*, 51 (October): 3–18.
- Krishnamurthy, Sandeep. 2001. A Comprehensive Analysis of Permission Marketing. *Journal of Computer-Mediated Communication*, 6 (2): Available online: <http://jcmc.indiana.edu/vol6/issue2/krishnamurthy.html>.
- Lieber, Ron. 2008. Outspoken Champion of Identity Protection Tussles with Skeptics. *New York Times*, May 24.
- Lwin, May O. and Jerome D. Williams. 2003. A Model Integrating the Multidimensional Developmental Theory of Privacy and Theory of Planned Behavior to Examine Fabrication of Information Online. *Marketing Letters*, 14 (4): 257–272.
- Lwin, May. Jochen Wirtz and Jerome D. Williams. 2007. Consumer Online Privacy Concerns and Responses: A Power-Responsibility Equilibrium Perspective. *Journal of the Academy of Marketing Science*, 35 (4): 572–585.
- Mackey, Jack. 2005. Franchisors Reap Multiple Benefits from Increasing Customer Loyalty. *Franchising World*, 37 (5): 49–50.
- McClelland, David. 1951. *Personality*. New York: Holt, Rinehart, & Winston.
- McClennan, Jennifer and Vadim Schick. 2007. “O, Privacy” Canada’s Importance in the Development of the International Data Privacy Regime. *Georgetown Journal of International Law*, 38 (Spring): 669–694.
- Milne, George R., Shalini Bahl and Ereni Markos. 2008. What did You Buy? When Consumer Consider this Information Sensitive. In *Marketing & Public Policy Conference Proceedings*, edited by John Kozup, Charles R. Taylor and Ronal Paul Hill (126–127). Chicago: American Marketing Association.
- Milne, George R., Mary J. Culnan and Henry Greene. 2006. A Longitudinal Assessment of Online Privacy Notice Readability. *Journal of Public Policy & Marketing*, 25 (Fall): 238–249.
- Miyazaki, Anthony D. and Ana Fernandez. 2000. Internet Privacy and Security: An Examination of Online Retailer Disclosures. *Journal of Public Policy & Marketing*, 19 (Spring): 54–61.
- Parks, Roger B., Paula C. Baker, Larry L. Kiser, Ronald Oakerson, Elinor Ostrom, Vincent Ostrom, Stephen L. Percy, Martha B. Vandivort, Gordon P. Whitaker and Rick Wilson. 1981. Consumers as coproducers of public services: Some Economic And Institutional Considerations. *Political Studies Journal*, 9 (7): 1001–1011.
- Peralte, Paul. 2008. Credit-freeze law adds muscle to fraud fight. *Atlanta Journal-Constitution*, 60 (141): May 20.
- Prelinger, Ernst. 1959. Extension and Structure of the Self. *The Journal of Psychology*, 47 (January): 13–23.
- Schwartz, Paul M. 2004. Property, Privacy, and Personal Data. *Harvard Law Review*, 117 (May): 2056–2128.
- Sell, Jane and Rick K. Wilson. 1991. Levels of Information and Contribution to Public Goods. *Social Forces*, 70: 107–124.
- Sheehan, Kim Bartel and Mariae Grubbs Hoy. 2000. Dimensions of Privacy Concern Among Online Consumers. *Journal of Public Policy & Marketing*, 19 (Spring): 62–73.
- Solove, Daniel J. 2001. Privacy and Power: Computer Databases and Metaphors for Information Privacy. *Stanford Law Review*, 53 (July): 1393–1462.
- Stigler, George J. 1961. The Economics of Information. *The Journal of Political Economy*, 69 (3): 213–225.
- Turow, Joseph. 2003. Americans and Online Privacy: The System Is Broken. Annenberg Public Policy Center of the University of Pennsylvania. Available at <http://www.asc.upenn.edu/usr/jturow/internet-privacy-report/36-page-turow-version-9.pdf> (Last accessed March 11, 2009).
- United States General Accounting Office. 1998. Health Insurance Standards: New Federal Law Creates Challenges for Consumers, Insurers, Regulators. GAO/HEHS-98-67.
- Warner, Richard. 2005. Surveillance and the Self: Privacy, Identity, and Technology. *DePaul Law Review*, 54: 847.

- Warren, Samuel and Louis Brandeis. 1890. The Right to Privacy. *Harvard Law Review*, 4 (5): 193–220.
- Wasserstrom, Richard A. 1978. Privacy: Some Arguments and Assumptions. In *Philosophical Law*, edited by Richard Bronaugh. Westport, CT: Greenwood Press.
- Yerushalmi, Hanoach. 1992. Psychoanalytic Supervision and the Need to be Alone. *Psychotherapy*, 29 (2): 262–268.
- Zimmerman, Diane L. 1992. Information as Speech, Information as Goods: Some Thoughts on Marketplace and the Bill of Rights. *William and Mary Law Review*, 33: 665.
- Zwick, Detlev and Nikhilesh Dholakia. 2004. Whose Identity Is It Anyway? Consumer Representation in the Age of Database Marketing. *Journal of Macromarketing*, 24 (1): 31–43.