Privacy Revisited:
From Lady Godiva's Peeping Tom
to Facebook's Beacon Program

Kirsten Martin
The Catholic University of America, USA

ABSTRACT

The underlying concept of privacy has not changed for centuries, but our approach to acknowledging privacy in our transactions, exchanges, and relationships must be revisited as our technological environment – what we can *do* with information – has evolved. The goal of this chapter is to focus on the debate over the definition of privacy as it is required for other debates and has direct implications to how we recognize, test, and justify privacy in scholarship and practice. I argue privacy is best viewed as the ability of an individual to control information within a negotiated zone I illustrate this view of privacy through an analysis of Facebook's Beacon program and place the case in the context of both privacy violations and successful business strategies. I find privacy zones are illuminating for situations from 10th century England to current social networking programs and are useful in identifying mutually beneficial solutions among stakeholders.

Privacy Revisited:
From Lady Godiva's Peeping Tom to Facebook's Beacon Program

> After months of Lady Godiva's lobbying for tax reform for their village of Coventry, her husband Leofic, Earl of Mercia, exasperatingly challenged Lady Godiva to ride naked through the town center before all the people in order to get her wished tax relief. Lady Godiva immediately contacted the great magistrates of the city and informed them of Leofic's challenge. Given the dire economic status of the town, these community leaders agreed to have all citizens of Coventry return to their homes and remain behind closed doors so as to not lay eyes upon Lady Godiva during her ride through the center of town. At noon on the appointed day, Lady Godiva let down her hair which covered her in a semi-modest degree, mounted her horse and, accompanied by two knights, rode through town. As was agreed upon, the roads were clear and the market was eerily quiet from the absence of barter and negotiations. Suddenly, Lady Godiva was notified of an errant young man peeping through a window by her horse's neigh. The knights soon realized that the young man was Tom the Tailor who was immediately struck blind as some sort of divine punishment but not before he was able to turn and tell his tale to others in the house.[1]

INTRODUCTION

While the notion of privacy has been a focus of concern for centuries, recent developments have changed how we approach acknowledging privacy. Peeping Tom violated privacy norms by peering through a window to view a disrobed Lady Godiva riding through town, whereas current privacy concerns are more likely to arise in a virtual world such as SecondLife rather than in a township, or by compromised by a cyber-voyeur, hacker, on computer program rather than by an individual peering through a window. Two related trends have necessitated a revisiting of how we acknowledge privacy. *First, information is increasingly the basis for an organization's value proposition and, for some, the entire business model.* While business has always relied upon consumer information to complete transactions, more of that information is stored or being repurposed for behavioral marketing or custom recommendations. All organizations have stakeholders such as employees, suppliers, governing bodies, and communities who share information in increasingly important ways.

Second, our information is both greased and sticky. By becoming separated from us, our information is 'greased' in the words of technologist James H. Moor (1997). Information can slip quickly from protected, legitimate storage to an unprotected, illegitimate individual through the click of a mouse. At the same time, I argue that information is 'sticky' in that organizations can link and aggregate information which was previously separated and compartmentalized. As such, our information is increasingly in permanent records which are searchable rather than only observable (Lessig, 1998, 1999). Where department stores previously recorded customers' preferences on index cards to notify them of upcoming sales, grocery chains now store previous and current purchases to customize coupons and Amazon.com monitors browsing and purchases to suggest additional products. Where Lady Godiva briefly rode through town at noon on an appointed day, Facebook retains information to be linked to, searched, revealed, or repurposed for an indeterminate amount of time. Perhaps the type of information requested and stored is similar, but the format of the information is different in important ways.

These shifts make the information both *valuable* and *vulnerable* to organizations and individuals: valuable by facilitating customized services and lowering transaction costs and vulnerable by being

identifiable and searchable thereby creating a larger target for illegal hacking or unintended violations of privacy. As I will argue, these trends point to the control view of privacy as being increasingly useful and applicable : when our information was 'attached' to us as in the case of Lady Godiva in the beginning of this chapter, the ongoing control of information was not important to our conception of privacy as we controlled our information by controlling who has access to ourselves. This is not the case now. Now, our information is not contained by physical barriers but rather negotiated through virtual barriers: the equivalent to asking a friend to turn their back while you change or asking your child to cover their ears while you talk to another adult.[2]

The goal of this chapter is to develop an understanding of privacy for business ethics as a common concern among stakeholders. To do so, I focus on the debate over the definition of privacy as it is required for other debates and has direct implications to how we recognize, test, and justify privacy in scholarship and in practice. I argue that privacy is best viewed as the ability of an individual to control information within a negotiated zone or space. I illustrate this view of privacy through the case of Facebook's Beacon program and analyze the case in the context of privacy zones and contemporary examples of both privacy violations and successful strategies to protect stakeholders' privacy. While the tactics we employ to protect privacy have evolved, previous work on privacy need not be rendered moot. STS scholar Deborah Johnson refers to this as the genus-species account of moral issues: we may find multiple and evolving applications of privacy while not necessarily changing the genus of privacy (Johnson, 2006).

Privacy scholarship breaks into a series of overlapping and interconnected debates seeking to identify harms, justify the acknowledgment or existence of privacy, or parse privacy rights. Yet these debates, such as the justification, rights, cohesion, and substitution debates, rely upon a definition of privacy: the scope of privacy and/or privacy violations is a fundamental assumption to all subsequent debates. In other words, an argument seeking to justify the acknowledgement of privacy is predicated on a shared definition of the scope of privacy; a discussion about minimal privacy rights secured in the law similarly necessitates a definition of privacy. Thus, in this chapter I focus on the scope or definition debate as it pervades other theoretical debates, provides the basis for research assumptions, and has direct implications for how we recognize, test, and justify privacy in scholarship and in practice. I do not dismiss or ignore these ongoing debates; rather, these debates serve to highlight the benefits and harms, the stakeholders involved, and the pervasiveness of privacy concerns. I discuss these alternative debates at the conclusion of the analysis in light of the arguments of this chapter. In addition, I steer away from conventional approaches which seek to identify privacy minimums by examining privacy as if the parties involved seek mutually beneficial solutions similar to Lady Godiva and the magistrates. As such, I use pragmatic scholarship from legal scholars such as Rosen (2001) and Scolove (2006) for their philosophical reasoning rather than their prescriptions for laws and regulations.

BACKGROUND

The concept of privacy can appear nebulous as teenagers now post all of their activities on Facebook only to declare their lives private, and managers bemoan employee surveillance while implementing behavioral marketing for their online customers. As I illustrate below, seemingly inconsistent strategies, research, or behavior may be grounded in a narrow understanding of privacy. Here I outline two approaches to the scope of privacy—the *control* and *restricted access* versions of privacy—and introduce the mechanism of information or privacy zones as useful to conceptualize privacy within business ethics. As seen in many nuanced arguments for and against each view, how we define privacy has implications not only for our theoretical justifications of privacy, but also in how we conduct research on expectations of privacy and how we navigate privacy in practice.

Privacy as restricted access

The restricted access view of privacy holds that privacy is "fundamentally about protection from intrusion and information gathering by others" (Travani and Moor, 2001, p. 6p. and, therefore, requires a degree of inaccessibility of individuals and their information from the senses of others (Allen, 1988; Reiman, 1995; Brin, 1998). According to this view, privacy is protected when information is hidden, and privacy violations occur when information or an individual is revealed. This view of privacy is easy to detect and model as information is either hidden or not hidden, revealed or not revealed. As an added benefit, once the information is revealed, privacy norms do not apply since the information is no longer private and the individual can hold no expectation of privacy.

An immediate reaction is to argue that, according to the restricted access view, individuals are always private since one is always inaccessible to others to some degree (Elgesem, 1999) or, in a related vein, that individuals are never completely inaccessible and therefore never completely private. However, these arguments would hold for both the control and restricted access version of privacy (i.e. one can never be in complete control, ergo, one can never be in total privacy) and are therefore not compelling or helpful in differentiating the two. However, the restricted access view's problems are most clearly illustrated through the belly dancer and prisoner accounts. These problems lead some to take what I consider extreme measures to make the case for the restricted access version of privacy.

Privacy without restricted access: the belly dancer account.

The first problem with the restricted access version of privacy is that we frequently give access to information or reveal ourselves while still retaining an expectation of privacy; restricted access is not necessary for a notion of privacy. We have private conversations, act in ways that we expect to remain private('what happens in Vegas, stays in Vegas'), or ride naked through a village marketplace as in the case of Lady Godiva. I refer to this as the belly dancer problem: when a belly dancer performs, she reveals herself and gives others access to information about her belly; yet she retains an expectation of privacy in that her belly is not available for public access or surveillance once she decides the dance is over. Further, she is able to negotiate rules, justifiably in my estimation, that no image of her belly can be recorded and leave the privacy zone she has created through a social contract with her guests. Similarly, when Lady Godiva gives her husband access to her body, the case is not a privacy violation nor would he be correct in assuming that the information about her body is public based solely on his access to it.

The line of reasoning which has the belly dancer (or Lady Godiva) *without* any expectation of privacy relies upon the idea that every dissemination of information is a loss of privacy. This argument is logically extended to conclude that those who argue for privacy must be hiding something (Scolove, 2007) or are hypocritical (Wasserstrom, 1978). Accordingly, economists develop a choice in theory and in research—a false choice, I believe—of releasing information versus protecting information (Acquisti, 2002; Acquisti and Grossklag, 2004). The focus on restricting access becomes a problem of keeping information secret (Scolove, 2007) thus leading to the determination that privacy is inefficient due to fraud and misrepresentations (Posner, 1981) and supports discussions such as "The Economics of Privacy as Secrecy" (Hermalin and Katz, 2005) and the positioning of the rights of society to know information about individuals (Singleton, 1998) for the good of the community (Brin, 1998). As demonstrated by its advocates, such a view of privacy lacks practicality; a definition of privacy is not sustainable or useful if recognizing it necessitates the breakdown of a community or a market or positioning the claims of the individual as subsumed to the needs of an efficient market or a good society.

Restricted access without privacy: The prisoner problem.

Second, an individual can have access restricted without realizing a private situation. Consider a prisoner in a cell who is behind locked, solid doors. The restricted access view of privacy would have the prisoner in a private situation with the guard holding the key since access is technically restricted. Yet, prisoners and prisons are traditionally used to illustrate the harms of a lack of privacy (e.g. Foucoult, 1977; Reiman,

1995); a definition of privacy which implies prisoners are in a private situation becomes theoretically inconsistent. Two extreme and unsustainable reactions attempt to solve the prisoner problem. First, privacy could be relational—as in the prisoner is in a private situation with respect to certain people but just not the guards (Allen, 1998). Second, the threat of privacy violations could have a similar if not identical effect to actual privacy violations (Reiman, 1995); however, threats of privacy violations come when an individual does not have control over access to themselves or their information and we quickly fall into the control version of privacy as described below.

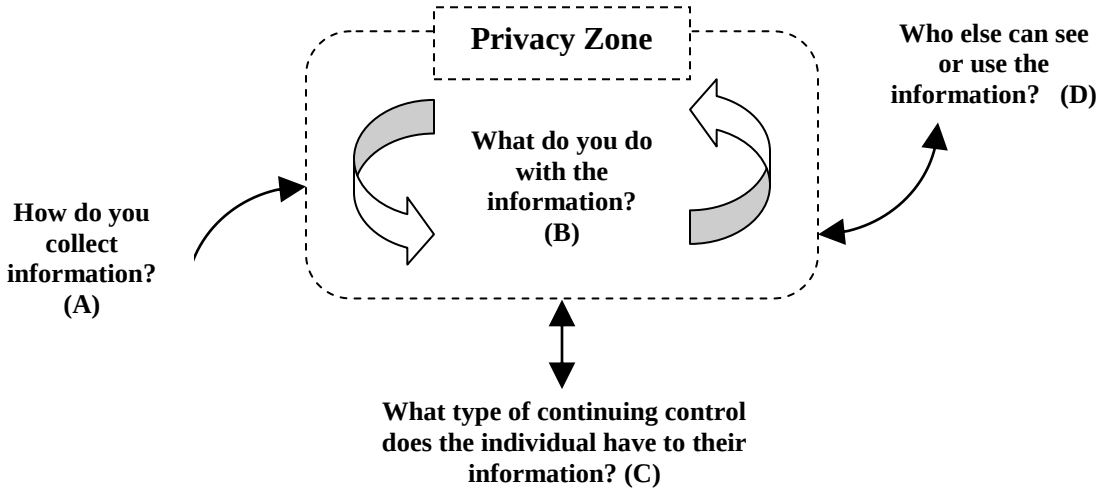
Perhaps at the most basic level, most individuals do not subscribe to this version of privacy with every dissemination of information as a loss of privacy.[3] Individuals have an expectation of privacy when they have handed over information as in the case of medical records, vacations in Vegas, or having a conversation over coffee. Thus, research on privacy within business mistakenly attributes individuals as relinquishing privacy when sharing information.

Privacy as the Control of Information

Alternatively, the *control* view of privacy builds on the ability of individuals to determine when, how, and to what extent information is communicated and used. Privacy is not merely the absence of information accessed by others, it is the control we have over our information: the manner in which information about an individual is accessed, disseminated, searched, and communicated to others (Westin, 1967; Elgesem, 1999; DeCrew, 1997; Fried, 1984). As stated perhaps most famously by Westin, "privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (1967, pg. 7).

One benefit of the control version of privacy is that information can be transferred or revealed to another party without losing the notion of privacy. Even as information becomes separated from us, e.g., is logged into a hospital system or is posted within a defined community within a social networking site, we still retain an expectation of privacy according to this view. In practice, with the advent of information becoming both separated and searchable, control of information no longer equals holding the keys to the locked room or closing the blinds. We have virtual rooms or zones (Moor, 1997; Scolove, 2006). Individuals let information into certain zones and are able to control when it leaves that zone. As illustrated in Figure 1, individuals are better able to protect their privacy if they know (a) the boundaries of privacy, (b) the uses of information within those boundaries (c) their ability to control and monitor the use of information, and (d) under what conditions information enters and leaves the zone. Lady Godiva created such a space in her agreement with the citizens to turn their backs so as to create a virtual privacy zone within the middle of the village market where her information would remain private. Peeping Tom pierced the veil of that zone by opening the window to view Lady Godiva and sharing what he saw with others.

Figure 1: Zone of Privacy



Some scholars writing on privacy have taken a similar approach to recognizing private areas (Simmel, 1950; Samarajiva, 1997), spaces, (Scolove, 2006; Jiang, Hone, and Landay, 2002), spheres (Rosen, 2001), situations (Moor, 1997), or zones (Moor, 1997). For most, the space or sphere surrounds an individual—either the target of the information or an individual holding the information—and the goal of inquiry is centered on identifying harm of the target or the responsibility for the 'data holder' (e.g., Scolove, 2006). The use of information zones or spaces within computing shifts the use of zones from centering on the individual to a virtual space which can exist without an individual—an important notion with information being housed in negotiated zones which may have multiple parties involved (such as the citizens of a village in the case of Lady Godiva) or multiple stakeholders impacted by that information. Two interesting dissents from the control approach to privacy attempt to demonstrate that information control is not necessary or sufficient for privacy yet inadvertently serve to further highlight the utility of the privacy zone metaphor.

Control without privacy

The cases where individuals may reveal particular information, such as medical records (Travani and Moor, 2001), or reveal all information (Schoeman, 1984) are positioned as exemplary of individuals who can maintain control of information without an expectation of privacy; this counter argument attempts to maintain that individuals control who has access to information yet cannot simultaneously claim the information is private. However, in the former case, control is maintained through a surrogate or second party who oversees the zone of privacy agreed to by the individual in much the same manner as I maintain security of my house by contracting with a security company. I still expect security even if I ask someone else to help maintain it, and an individual still can expect privacy when handing over information to a doctor, a lawyer, a close friend, or even a good waiter. In the case of the latter, we may not agree with someone who reveals 'too much,' but that does not necessitate a loss of privacy over other information or forgo the possibility of negotiating the terms of a zone of privacy. It should be said that no one really knows if someone has revealed *everything*—only the individual knows what everything is and if they have revealed it (barring some sort of invasive scanning or interrogation technique, which would be a violation of control and, ipso facto, of privacy by any standards). Rather, this particular dissent becomes a paternalistic argument as to what type and quantity of information is appropriate to share and with whom.

Privacy without control

A second type of dissent from the control view of privacy attempts to identify situations where individuals are in a private situation without control over themselves or their information. For example, we might consider cases such as an individual on a desert island (Schoeman, 1984) or the impossibility of actually retaining complete control over information (Moor, 1997) to demonstrate that control of information cannot be necessary for privacy. However, individuals do maintain their privacy, if they are in control of their existence on a secluded island, by selecting their zone of privacy. If I fly to a desert island, and can return when I please, I am in a private situation; if I go to a secluded room and return when I please, I can also expect to be in a private situation. Note the similarity to the prisoner problem above: both have individuals secluded with varying degree of restricted access and are therefore considered in a private situation. According to the control approach, the prisoner described above would not be in a private situation when the guard held the key but would be in a private situation if the *prisoner* held the key—a similar analysis to the desert island dilemma (Schoeman, 1984). Counter to these dissents, and key to the control view of privacy, if an individual consents to any information flow–either access by a third party or proactive revelation by the individual—there is no privacy violation (Scolove, 2006, pg. 484); we may not like the type or amount of information revealed, but the individual does not necessarily give up their claim for privacy.

Summary

The differences between the control and the access view of privacy are important as they shape what we see as violations, what we do in practice, and how we conduct research. First, the control view of privacy, particularly with the use of privacy or information zones, fits with our common descriptions of privacy: we regularly give access to information while still retaining an expectation of privacy. We share information with friends, colleagues, and businesses with an expectation that the information will stay within a commonly agreed upon, zone. In other words, one can claim an access view of privacy—such as when AT&T announced that they would use consumer information as they saw fit as the information was 'theirs'—however, stakeholder are free to disagree (AT&T revises privacy policy, 2006). This is a descriptive argument for the control view and is exemplified in the many examples (and failed counter examples) such as the belly-dancer problem and the prisoner problem.

However, more importantly, the control view of privacy supports the values we use to justify acknowledging privacy. Within the debate as to how to justify privacy, privacy is supported by identifying the many intrinsic values—such as autonomy (Johnson, 2001; Moor, 1994, 1997) and dignity (Rosen, 2001)—and instrumental benefits of adequately maintaining a notion of privacy—such as for self creative enterprise (Rosen, 2001), to develop a unique personality (Smith, 1979), to try new ideas (Rosen, 2001), to have intimacy (Elgesem, 1999), to develop relationships (Rachels, 1975), and in support of a free society (Reiman, 1975). I argue that these values are supported when individuals have control over their information and not when their information is merely hidden or inaccessible. One cannot develop a unique personality or try new ideas while making themselves inaccessible. Similarly, one main avenue to developing different levels of intimacy and types of relationships is by sharing information with different individuals (Elgesem, 1999; Rachels, 1975). A form of privacy which only ensures that individuals make themselves and their information inaccessible does not support these benefits or values.

In addition, individuals can be harmed through violations of privacy—such as a loss of freedom through controlled behavior and choice (Reiman, 1995), incurring an insult to dignity (Reiman, 1975; Rosen, 2001), being misrepresented or judged out of context (Rosen, 2001, pg. 21), and even psycho-political metamorphosis (Reiman, 1995, p. 42) where individuals act/think conventionally and lose "inner personal core that is a source of criticism of convention, of creativity, of rebellion and renewal." Yet the access-view of privacy would have an individual, say a prisoner, who is the prototypical example for the harms of privacy violations, in a private situation. These harms are incurred as an individual loses control of their information and not when they grant access to this information. We may have a fear or run the risk of being misrepresented or insulted when we share information, as when talking to a friend or performing as a belly dancer, but that risk exists due to the lack of control over that information and not from granting access.

As illustrated in the Facebook example below, the access view of privacy stops at initial data collection (a)—once information has been revealed, it is no longer considered private (see Figure 1). This greatly limits the responsibility of organizations to maintain stakeholders' privacy as their privacy obligation ends at the point of revelation. The control view suggests that individuals are concerned about not only (a) how information is gathered, but also (b) the purpose and use of the information, (c) their control of the information, (d) third party access to the information (see Figure 1). I turn now to illustrate the application of privacy zones in a particular example: Facebook's Beacon program.

EXAMPLE: FACEBOOK AND BEACON

In November 2007, the social networking site, Facebook, offered a free tool to online partners called Beacon to track the activity of Facebook members on partner sites and proactively broadcast such off-Facebook activities to their designated Facebook 'friends' (Jesdanum, 2007). Beacon worked by being embedded in a partner's web site, such as Blockbuster, The New York Times, or Overstock.com, and

gathering behavioral information which was then sent to Facebook to process as either an alert to designated friends or as an item to ignore. Considered at the forefront of online advertising, Beacon was hailed as a mechanism to target potential customers based on their social network through a friend's implied recommendation.

However, Facebook members had difficulty understanding and navigating their role in Beacon (Nakashima, 2007). A notice to opt-out of Beacon broadcasts appeared in a small window and disappeared without Facebook users taking any action, thereby leaving Beacon broadcasts to be sent to the user's identified friends by default. Further, Facebook users were not given the ability to reject all sharing, and the notification window appeared (and disappeared) every time the user entered a partner site (Perez, 2007a; Jesdanun, 2007).

That Facebook faced and continues to face privacy issues is not in question here: stakeholders of Facebook and the Beacon program raised privacy concerns through blogs and newspaper articles. However, views of privacy which rely upon legal regulations or actionable harms could miss these privacy concerns as (1) these violations were not illegal and (2) all information was revealed by individuals on Facebook or on the partner site. Many famous privacy violations emanate from the improper handling of information that has been previously revealed; and Facebook's Beacon program gathered information from retailers' web sites where consumers assumed it would stay.

While much of the focus has been on Beacon as a 'Peeping Tom,' the following analysis of this case illustrates that (1) Facebook's most egregious mistake centered on the ability of users to be notified and make decisions as to the repurposing of their social network and (2) the partners who willingly implemented Beacon may have been the most underreported offenders.

The Role of Facebook

The initial collection of information and third party access to information, the classic definition of a privacy violation in the access-view of privacy, were not issues for Facebook. In fact, Facebook members voluntarily revealed their information within different Facebook 'zones' with a great degree of notification (Facebook). Rather, Facebook's transgression was in not allowing their members to control the use of their networking information.

First, the initial purpose of members revealing their information on Facebook, and subsequently linking friends to that information, was to share the information in order to build relationships; yet, Beacon leveraged information, contacts, and social networks in order to market third party products. The secondary use of their information as a vehicle for marketing distribution was too far afield from the primary, agreed upon use of the members' data. Second, the role of users was severely limited in the ongoing use of their information due to Facebook's anemic approach to alerting users of Beacon (Nakashima, 2007), the decision to use an opt-out strategy,[4] and the absence of an option to turn off Beacon permanently. In effect, Facebook did not allow members to maintain a relationship with their information.

Fortunately, Facebook's remedy focused on fixing their members' ability to control their information. Within days of the uproar reaching the mainstream media, Facebook decided to give users the option of permanently turning off Beacon for their 55 million users and apologized for their mistakes (Liedtke, 2007). Where previously consent was assumed, Facebook would now ask members to opt in to the service and would not automatically store information from third-party partner sites. In addition, Facebook members are now asked to allow the broadcast of their activity before their off-Facebook activity is sent to their friends thus shifting to an opt-in notification. Even with improvements, Facebook members still were not offered the ability to easily disable the Beacon service. Further complicating the situation and infuriating online communities, users were not informed that data on their activities was

always flowing back to Facebook nor given the option to block that information from arriving at Facebook; Facebook merely promised to disregard or not use certain information. In fact, if a Facebook member ever decides to have their computer 'remember' their login information, Facebook could tie activities from third-party sites even if the user was logged off Facebook or had opted out of the Beacon broadcast.

The Role of Partners

Little attention was paid to the Facebook partners who voluntarily implemented Beacon. These partners, such as Blockbuster, Sony Online Enterntainment, eBay, The New York Times, and IAC, took a wide range of approaches to the adoption of this surveillance technology (Perez and Gohring, 2007). As became apparent through journalistic inquiries and the persistence of the online community, Beacon captured detailed data along with the IP addresses of *all visitors* on a partner site—Facebook members and non-Facebook members—and determined whether or not to store and broadcast the information once the tracking information was sent back to Facebook (Liedtke, 2007). Partners controlled if and how the Beacon program would work for them. As advertised on Facebook's website, a partner could "add 3 lines of code and reach millions of users" (Beacon).

Similar to our analysis of Facebook's role, the behavioral and purchasing information on the partner site was freely provided by the user as they shopped. However, users did not expect their purchasing information on overstock.com, for example, to be sent to their Facebook friends: media outlets repeated the story of a woman whose engagement surprise was ruined when she was notified of her boyfriend's purchase of a diamond ring on overstock.com (Nakashima, 2007). Even after modifications, Facebook decided not to modify Beacon's ability to "indiscriminately track actions of all individuals on partner sites which implemented beacon" (Perez, 2007c). This facet of Beacon was referred to as 'broad user tracking' as Beacon captured "addresses of web pages visited, IP addresses, and the actions taken on the site" of nonmembers and members of Facebook and deletes the data upon receiving it (Perez, 2007b). The partners' decisions to repurpose behavioral and purchasing information for marketing and to provide that information to Facebook (a third party) violated the users' expectations of privacy by reusing the information provided and sending the information outside the privacy zone.

Not all partners implemented Beacon without changes. Overstock.com stated, "We have a specific threshold that the program needs to meet, in terms of privacy, before we'll be turning it back on" (Perez and Gohring, 2007). Others opted to trust Facebook to delete the information they sent back via Beacon thus still allowing user information to leave the partner's zone. Kongregate, an online gaming site, used the program to track games people play but not other activities on their site. In a similarly nuanced installation, Six Apart asks their users to opt-in and only inserts the script for the Beacon program at that point. In other words, Six Apart turns off Beacon for users who ask not to be included so that their information is never collected or sent to Facebook. Ebay also uses Beacon in a limited fashion by applying the program to sellers only and using an opt-in strategy.

Much has been publicized about both voluntary and involuntary penetrations of information zones through third-party access and surveillance. GE Money lost a digital tape with customer information (Morning Edition); an intruder gained access to a computer that contained customer information of millions of TJX shoppers (Dash, 2007); AOL researchers released three months' worth of users query logs to public which contained personally identifiable information (Hafner, 2006). The decision of partners to release behavioral information is a similar violation of privacy and should be categorized with similar breaches of privacy in business.

Beacon Summary

If we relied upon the access-view of privacy, information which was provided by users (on partner sites) or members (on Facebook) could not be considered private. Yet, the blogging community, members, users, the press, and all other stakeholders of Beacon viewed the Beacon program as violating privacy. As summarized in Table 1, Facebook's mistakes in the initial release of Beacon amount to improper notification of members as to the repurposing of their Facebook relationships. However, the role of some partners was much larger. Partners reused behavioral information for marketing purposes and sent the information to multiple third parties.

Table 1: Privacy Violations with Facebook's Beacon Program

	Facebook	**Partners**
a. Collection of information	Facebook member provided links to friends.	User provided behavioral and purchasing information by navigating the partner's web site.
b. Use of information	Links repurposed for marketing by Facebook. Original purpose for members to communicate with friends.	Behavioral information repurposed for marketing by partner site. User used as 'spokesperson' for products and services without their consent.
c. Continued relationship with information	Members initially not adequately notified nor given the ability to opt out of the program.	Users not given the opportunity to (a) not have their information collected or (b) not have their information reused.
d. Third party access to information	No third party received information on member-friend links.	Facebook given access to behavioral information. Member's friends received broadcasted information on browsing and purchasing behavior.

Just as Peeping Tom broke the negotiated zone to view Lady Godiva, these partners took information from a negotiated zone and provided it to others in a similar manner. Facebook may have been the public face for this story as the developers of the program, for which they bear some responsibility for the design and use of that program. However, the partners' decisions as to if and how to implement Beacon violated the privacy of Facebook and non-Facebook members and, thus, were the greater violators of privacy. These partners, as the guardians of behavioral information, became the equivalent of Lady Godiva's knights turning and telling the tale of Godiva's ride through the marketplace.

FUTURE RESEARCH DIRECTIONS

In this chapter, I break from conventional approaches looking for privacy minimums and examined privacy as if the parties involved seek mutually beneficial solutions similar to Lady Godiva and the magistrates. Specifically, I argued that privacy is best viewed as the ability of an individual to *control* their information within a particular privacy or information zone and illustrated this view of privacy through the example of Facebook's Beacon program and analyzing the role of multiple stakeholders in violating and securing privacy zones. I turn now to consider the implications to privacy scholarship and practice.

Implications to Theory: Alternative Debates

Within privacy scholarship, scholars have identified a series of problems to solve, debates to enter, and ways to justify privacy (See Table 2). Where the cohesion debate attempts to categorize privacy harms with varying degrees of commonality versus a mere "hodgepodge" of infractions (Rosen, 2001; Alderman and Kennedy, 1995), the rights debate posits the individual against society—or, as Warren and Brandeis

famously stated, "against the world" (1890, p. 10)—to identify minimal rights to be protected. In particular, I have leveraged Scolove's (2007) deft handling of the interminable rights debate. Scolove argues privacy is not merely instrumental to society or only intrinsic to the individual but a concept with benefits and harms to all—the individual as a member of society and society as a collection of individuals. Such is the approach taken in this chapter by assuming privacy to be of a mutual concern of individuals and organizations in the particular case rather than a contentious argument where party 'wins' and another loses.'

Table 2: Implications to Current Privacy Debates

	Focus of inquiry	**Examples**	**As contributing to this chapter**	**As impacted by this chapter**
Scope Debate	How do we define privacy to use in theory, research, and practice?	Moor (1994); Schoeman (1984)	Focus of chapter.	Privacy is defined as the control of information inside a particular zone.
Justification Debate	What are the benefits to protecting privacy and the harms of privacy violations?	Reiman (1995); Rosen (2001); Elgessem (1999); Rachels (1975)	Privacy is a highly valued concept with many concerned parties. Supports privacy as a mutual concern rather than a point of contention.	Privacy as controlling information supports the intrinsic and instrumental values we associate with privacy (whereas, privacy as restricted access does not).
Rights Debate	How should a right to privacy be protected? Whose interests are we protecting?	Moor (1997); Johnson (2001) Warren and Brandeis, (1890); Brin (1998)	Approach to privacy as an interest of both individual and society. Privacy is something a community acknowledges to the benefit of the individual and the community.	Many stakeholders and communities benefit from being able to control their information through the acknowledgement of privacy zones.
Cohesion Debate (Schoeman, 1984)	Do the harms we are trying to avoid have anything in common or is privacy an umbrella term for a loosely related set of problems?	Schoeman (1984); Alderman and Kennedy (1995); Scolove (2006); Prosser (1960)	Not utilized in this chapter as the debate focuses on identifiable harms as tying together a notion of privacy.	A focus on harms is not necessary for a discussion about privacy.
Substitution Debate	Is there a right to privacy? Can we pierce together other norms, rights, or values to substitute for privacy?	Schoeman (1984); Reiman (1995); Thompson (1975)	Highlights points of vulnerability or opportunities for creating value within a model of privacy zones.	The control view of privacy allows for acknowledging privacy claims which do not rise to the level of intellectual property claims.

The debate over how to justify privacy by identifying the many benefits of recognizing and harms in violating privacy is leveraged in assuming that privacy is important and valuable to different parties. The justification or value for these concerns, it is assumed, has been taken into account by those stakeholders and by Facebook in attempting to navigate the concerns. Rather than taking an antagonistic stance to debating whose 'rights' trump the other, Facebook attempted to find mutually agreeable strategies which met the concerns of multiple parties. Both debates are useful endeavors when identifying commonality among court cases (Prosser, 1960) or moral minimums for future regulation, but these debates may be misplaced given the approach taken in this chapter to highlight opportunities and vulnerabilities.

Alternatively, the substitution debate attempts to build up or substitute privacy with an amalgamation of individual and societal rights, which equate to the right to privacy; this argument attempts to demonstrate that we do not really have a right to privacy, we just call it privacy. For example, rather than a right to privacy, an individual has a right to autonomy with the exchange of information being governed by intellectual property (Samuelson, 2000; Singleton, 1998), information asymmetry (Jiang, Hong, and Landay, 2002), and social contract norms – the latter three concepts being summarized as privacy as fair information privacy (Bennett, 1992). Facebook respected information asymmetry in some circumstances (such as the initial notification of privacy rules and tactics) and not in others (such as the ongoing notification and opt-out policy of Beacon). Facebook respected the control of information without the need for claiming property rights and continued to negotiate their social contract with their stakeholders through blogs and press announcements including an apology.

While I argue privacy is distinct, useful (James, 1931), and not sufficiently substitutable, such examinations remain important by highlighting points of vulnerability or opportunity for creating value within our model of privacy zones. Attempts to build up the notion of privacy from different individual rights do a disservice to both our notion of privacy and those substitutable rights. The use of privacy zones and the control view of privacy makes these substitutable 'rights' illuminating potential points of vulnerability, such as the continuing control of information or full disclosure when gathering information; a discussion with stakeholders as to the unreasonableness of their privacy claims may be short lived.

As noted above, these debates shift in light of the arguments of this chapter. Some debates are transcended, such as the cohesion debate and the rights debate, due to the approach and scope of this chapter to examine privacy as a common concern or source of social friction (Coase, 1960) to be resolved between interested parties. This argument assumes that parties can resolve differences through private ordering rather than through regulations. However, legal scholarship would have something to say about the underpinnings required to negotiate the privacy norms within a particular information space. Such social contract minimums such as informed consent and a right of exit could be considered moral minimums to negotiating privacy.

Yet other debates have been leveraged in this chapter to identify the overall value of privacy to many parties (the justification debate) or to highlight points of vulnerability and opportunity with the privacy model offered here (the substitution debate). All debates, research, and scholarship on privacy necessitate a definition of privacy and are therefore impacted by the treatment in this chapter.

Implications to Practice: From Lady Godiva and to Beacon

One strategy being pursued by organizations is to limit the quantity and length of time information is held within a privacy zone. Some search engines are limiting their exposure to privacy violations by deleting search results and user behavior within months; Google has taken a different tack by retaining data for two years (Lohr, 2007). Both companies and stakeholders benefit from balanced information collection and retention polices. Companies who retain information are vulnerable to violations of privacy through the misuse of information or third-party surveillance (Zeller, 2006). Yet, Facebook's current policy of indiscriminately collecting information through Beacon in addition to recent concerns as to the ability of

members to delete their information from Facebook upon quitting (Rampell, 2008) combine to create privacy vulnerabilities to the organization and their members. Holding on to personal information within a negotiated zone of privacy places a burden on Facebook to maintain the security of that data. A definition of privacy—such as the access view—which suggests that individuals either provide necessary information for business transactions and relationships or retain their privacy does nothing to identify how business and stakeholders can develop a strategy to do both. By controlling information in privacy zones, individuals are able to both share and protect their information. Business can take steps in thinking about and managing these issues within an organization. How should organizations partner with individuals to share information with respect? How can technologies be designed to accommodate privacy? How can organizations put control in the hands of individuals to preserve their notion of privacy?

CONCLUSION

Understanding privacy helps us to develop technologies, norms, social contracts, and value systems to support a sustainable exchange of information. The underlying concept of privacy has not changed for centuries, but our approach to acknowledging privacy in our transactions, exchanges, and relationships must be revisited as our technological environment – what we can *do* with information – has evolved.

There is much to be said for all parties in business wanting to understand privacy. Consumers want to exchange information, simplify transactions, have books recommended, and save credit card information while retaining their privacy and the 'right to be left alone' (Warren and Brandeis, 1890). Furthermore, corporations want to limit their vulnerability to information leaks, hackers, or civil subpoenas and minimize the cost of preserving, storing, securing information while still lowering transaction costs and customizing services for customers and stakeholders. A definition of privacy which relies upon the control of information in privacy zones supports the possibility of all stakeholders to achieve their goals.

REFERENCES

AT&T revises privacy policy. (2006). Retrieved September 11, 2009, from *The New York Times* web site: http://query.nytimes.com/gst/fullpage.html?res=9F00E0DB1F31F931A15755C0A9609C8B636/22/2006.

Acquisti, A. (2002). Privacy and security of personal information: Economic incentives and technological solutions. In *1st SIMS Workshop on Economics and Information Security*.

Acquisti, A. & Grossklag, S.J. (2004). Privacy attitudes and privacy behavior: Losses, gains, and hyperbolic discounting. In J.Camp & R. Lewis (Eds.) *The Economics of Information Security*. Kluwer.

Alderman, E. & Kennedy, C. (1995). *The right to privacy*. NY: Knopf.

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

Beacon. 2009. Retrieved May 29, 2009, from Facebook Web Site: http://www.facebook.com/business/?beacon.

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

Brin, D. (1998). *The transparent society*. Reading, MA: Perseus Books.

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

Dash, E. (2007). Data Breach could affect millions of TJX shoppers. Retrieved September 12, 2009, from *The New York Time*s web site: . http://www.nytimes.com/2007/01/19/business/19data.html

Davidson, H.R.Ellis. (1969). The legend of lady godiva. *Folklore*, 80(2), 107-122.

DeCrew, J. (1997). *In pursuit of privacy*. Ithica, NY: Cornell University Press. .

Elgesem, D. (1999). The structure of rights in directive 95/46/EC. *Ethics and Information Technology* 1, 283-293.

Facebook. (2009). Retreived May 28, 2009, from Facebook web site: http://www.facebook.com/about.php).

Foucoult, M. (1977). Discipline and punish: The birth of the prison. In Rabinow, P. (ed.) (1984). *The Foucoult reader*. New York: Pantheon Books.

Fried, C. (1984). Privacy. In F.D. Schoeman (ed.) (1984). *Philosophical dimensions of privacy: An anthology*. Cambridge: Cambridge University Press.

Hafner, K. (2006). Researchers yearn to use AOL logs but they hesitate. Retrieved September 12, 2009, from *The New York Times* web site: http://www.nytimes.com/2006/08/23/technology/23search.html ..

Hartland, E. (1890). Peeping Tom and Lady Godiva. *Folklore*, 1(2), 207-226.

Helft, M. (2007). Google zooms in too close for some. (Retrieved September 12, 2009) *The New York Times* web site: http://www.nytimes.com/2007/06/01/technology/01private.html .

Hermalin, B.E. & Katz, M.L. (2006). Privacy, property rights, and efficiency: The economics of privacy as secrecy. *Quantitative Marketing and Economics* 4(3), 209-239.

Holson, L. M. (2007a). Verizon letter on privacy stirs debate. Retrieved September 12, 2009, from *The New York Times* web site: http://www.nytimes.com/2007/10/16/business/16phone.html.

Holson, LM (2007b). Privacy lost: These phones can find you. Retrieved September 12, 2009, from *The New York Times* web site: http://www.nytimes.com/2007/10/23/technology/23mobile.html.

James, W. (1931). *Pragmatism: A new name for some old ways of thinking.* NY: Longmans, Green, and Co..

Jesdanun, A. (2007). Facebook retreat shows ad-targeting risk. *The Associated Press* Retrieved September 12, 2009, from *The Washington Post* web site: http://www.washingtonpost.com/wp-dyn/content/article/2007/11/30/AR2007113001668_pf.html

Jiang, X. (2002). Safeguard privacy in ubiquitous computing with decentralized information spaces: Bridging the technical and the social. presented at the 4th International Conference on Ubiquitous Computing (UBICOMP 2002), Gotenborg, Sweden

Jiang, X., Hong, J.L., & Landay, J.A. (2002). Approximate information flows: Socially based modeling of privacy in Ubiquitous Computing. *Ubicomp 2002: Ubiquitous Computing*, 176-193.

Jiang, X & J.A. Landay. (2002). Modeling privacy control in context-aware systems. *Pervasive Computing, IEEE* 1(3), 59-63.

Johnson, D.J. (2001). *Computer ethics*. NY: Prentice Hall.

Liedtke, M. (2007). Facebook lets users block marketing tool. *The Associated Press*. Retrieved September 12, 2009, from SFGate.com web site: Facebook lets users block marketing tool.

Lohr, S. (2007). As its stock tops $600, Google cases growing risks. Retrieved September 12, 2009, from *The New York Times,* web site: http://www.nytimes.com/2007/10/13/technology/13google.html .
Lady Godiva. (1950). *Western Folklore*. January, 77-78.

Lessig, L. (1998). *The architecture of privacy*. Retrieved September 12, 2009, from The Berkman Center for Internet and Society at Harvard University web site: http://cyber.law.harvard.edu/works/lessig/architecture_priv.pdf

Lessig, L. (1999). *Code and other laws of cyberspace*. New York: Basic Books.

Mitchell, D. (2007). Online ads vs. privacy. Retrieved September 12, 2009, from *The New York Times*, web site: http://www.nytimes.com/2007/05/12/technology/12online.html.

Morning Edition. (2008). GE loses consumers' personal records. Retrieved September 12, 2009, from *National Public Radio: Morning Edition* web site: http://www.npr.org/templates/story/story.php?storyId=18212217.

Moor, J. (1997). Towards a theory of privacy in the information age. *Computers and Society* Sept, 27-32.

Nakashima, E. (2007). Feeling betrayed, Facebook users force site to hone their privacy. Retrieved September 12, 2009, from *The Washington Post*, web site: Feeling betrayed, Facebook users force site to hone their privacy .

Perez, J.C. (2007a). Facebook admits ad service tracks logged-off users. Retrieved September 12, 2009, from *PC World* web site: http://www.pcworld.com/article/140225/facebook_admits_ad_service_tracks_loggedoff_users.html.

Perez, J.C. (2007b). Facebook Tweaks beacon again; CEO apologizes. Retrieved September 12, 2009, from *PC World* web site: http://www.pcworld.com/article/140322/facebook_tweaks_beacon_again_ceo_apologizes.html

Perez, J.C. (2007c). Facebook doesn't budge on Beacon's broad user tracking. Retrieved September 12, 2009, from *PC World* web site: http://www.pcworld.com/article/140385/facebook_doesnt_budge_on_beacons_broad_user_tracking.html.

Perez, J.C. & N. Gohring. (2007). Facebook partners quiet on beacon fallout. Retrieved September 12, 2009, from *PC World* web site: http://www.pcworld.com/businesscenter/article/140450/facebook_partners_quiet_on_beacon_fallout.htm.

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

Prosser, W.D. (1960). Privacy. *California Law Review* 48, 383-396.

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

Rampell, C. (2008). What facebook knows that you don't. Retrieved September 12, 2009, from *The Washington Post*. http://www.washingtonpost.com/wp-dyn/content/article/2008/02/22/AR2008022202630.html .

Reiman. J.H. (1995). Driving to the panopticon. *Santa Clara Computer and High Technology Law Journal* 11(1): 27-44.

Reiman, J.H. (1975). Privacy, intimacy, and personhood. *Philosophy and Public Affairs* 6(1), 26-44.

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

Samarajiva, R. (1997). Interactivity as though privacy mattered. In P.E. Agre & M. Rogenberg, (eds.) *Technology and privacy: The new landscape*, Cambridge, MA: MIT Press: 283.

Samuelson, P. (2000). Privacy as intellectual property? *Stanford Law Review* 52(5), 1125-1173.

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

Scolove, D.J. (2007). 'I've got nothing to hide,' and other misunderstandings of privacy. *San Diego Law Review* 44.

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

Simmel, G. & K.H. Wolff. (1950). *The sociology of georg simmel.* Glencoe, IL: Free Press.

Smith, R.E. *Privacy: How to protect what's left of it.* Garden City, N.J.: Doubleday Books.

Singleton, S. (1998). Privacy as censorship. *Policy Analysis*, 295. The Cato Institute. .

Travani, H.T. & J.H. Moor. (2001). Privacy protection, control of information, and privacy –enhancing technologies. *Computers and Society* March, 6-11.

Thomson, J.J. (1975). *Philosophy and Public Affairs* 4(4), 295-322.

USA Today. (2007). "Fired Wal-Mart worker reveals covert operations. Retrieved September 12, 2009, from USA Today, web site: http://www.usatoday.com/money/industries/retail/2007-04-04-walmart-spying_N.htm

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

Wasserstrom, R.A. (1978). Privacy: some arguments and assumptions. In F.D. Schoeman (ed.) (1984. *Philosophical dimensions of privacy: An anthology.* Cambridge: Cambridge University Press.

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

Westin, A.F. (1966). Science, privacy, and freedom: Issues And proposals for the 1970s. Part I-the current impact of surveillance on privacy. *Columbia Law Review* 66(6)

Zeller, T. (2006). Your life as an open book. Retrieved September 12, 2009, from *The New York Times*, 8/12/2006.

NOTES

[1] Compiled from Davidson (1969); Sidney (1890); "Lady Godiva" (1950).

[2] The latter example is from the movie Old School where a father, in search of the ability to speak freely with friends, would ask his son to merely cover his ears by saying "ear muffs" rather than remove the child from the room.

[3] In an attempt to incorporate individuals' control in any discussion of privacy—including access versions of privacy—scholars differentiate scope versus the definition of privacy with the latter including some attempts at control (Reiman, 1995), dismiss consent as being implied in all interactions, relationships, and transactions (Singleton, 1998), or combine the two versions to create the control/restricted access version of privacy (Moor, 1997).

[4] An opt-out strategy defaults to the user being included in the program unless they specifically 'opt-out.' In other words, Beacon broadcasts would be sent to a user's identified friends unless the user opted out of the service. This is in contrast to the recommended opt-in strategy where users are not assumed to give consent and are asked to proactively opt-in.