Privacy in conflict: How implicit behavior norms inform expectations of privacy[1]

Ryan Malphurs
Texas A&M University
rmalphurs@gmail.com

This paper examines how online participants construct privacy within the digital age by investigating the tools participants implement to assemble the social boundaries of privacy. Group participants vary in their understandings of privacy, creating the potential for privacy violations that may impact both the online as well as offline community. Building upon previous online studies of privacy, this paper informs how group participants construct a contextual understanding of privacy, and how a violation of privacy impacts both offline and online interaction within groups and organizations. Open-ended surveys, public email discussions, personal interviews, and a focus group help explain how organizational members construct privacy as a normative behavioral value, reveal members' conflicting views of privacy, and expose how online privacy violations impacted members' online and offline interaction. This paper concludes by recommending that organizations determine an appropriate method, specific to departmental needs (e.g. codes, policies, or general understandings), to prevent future privacy violations.

Introduction

The delineation between public and private spaces is an often contested site within contemporary society. The legal system has attempted to determine the extent of a chairperson's personal surveillance on other board members (Kaplan 2006), but as the offline world struggles between complications of public and private realms, the internet faces its own set of challenges. Private internet users must consistently negotiate blurred boundaries between the public and private. The ambiguity users struggle with continues within organizational settings in departments that have varying expectations of interdepartmental online communication and that lack explicit rules of conduct. University departments use mass emails or listservs to contact, inform, address issues important to department members, socialize, and debate socially relevant issues.[2] University departments

1 The author would like to thank Dr. Heidi Campbell for her insight and assistance.

2 Although this study examines privacy within the unique organizational environment of a university, findings may be extrapolated and shaped to fit any organizational context. However, the university setting proves unique because privacy has long been a cherished right for professors and students alike; thus, when an individual's privacy has been violated by those at the highest level, the action proves disconcerting and challenges expectations of privacy within academic settings. Universities also provide an environment in which online interaction often intermingles with offline affairs, creating a unique environment to understand how the online and offline worlds interact.

often explore and debate sensitive social issues; however, problems arise when intra-departmental online debates occur within a public university, particularly when there is no clear or coherent articulation of online behavioral expectations. Most people agree the internet is a public space, so how do organizational members construct a sense of privacy when the organizational online environment lacks any formal rules of conduct concerning privacy, particularly for sensitive debates within a department? Organizational members in this position begin to shape privacy as a norm through online behavior, yet this norming results in conflicting views of privacy that may cause privacy violations and disrupt both online and offline organizational interaction.

Numerous studies have examined online behavioral norms (Baym 1995, Campbell 2004, McLaughlin et al. 1995, Mnookin 1996, Witmer 1996) and privacy within the online environment (Branscomb 1997, Greenleaf 1997, Kirsh et al. 1997, Metzger 2004,Vigas 2005); however, few studies have examined how online organizational members, or offline organizational members who communicate online, construct privacy through online behavioral norms. Still fewer studies examine how online privacy violations, either actual or perceived, impact both online and offline interaction between organizational members. Given the internet's growth within group and organizational interaction, an understanding of how groups and organizations construct privacy may reduce privacy violations, thereby ensuring more productive online communication between members and preventing privacy violations from impacting the offline world of an organization or organizational member. Instead of creating explicit recommendations that might prevent privacy violations for organizations to follow, this paper primarily investigates privacy as a behavioral norm and the offline implications of online privacy violations.

This study's findings suggest that organizational member's offline understandings of privacy inform their online approaches to privacy, and like offline understandings of privacy, organizational members construct online privacy as a behavioral norm. The study's findings reveal that organizational members hold incongruent expectations of privacy within the online environment, which could lead to privacy violations between members who hold incompatible views. Lastly, the study exposes that online organizational privacy violations may result in offline consequences, which in turn relate to online behavioral changes, often resulting in stunted online communication between organizational members.

In order to examine these issues, the construction of privacy is explored through an incident in which a member of a university department forwarded posts outside of the department, which originated in an internal online discussion. The posts concerned the university president. The posts eventually made their way to the president himself, and prompted the president to respond personally to one of the posters. Studying this case provides a fascinating collision of the online and offline worlds in which online interaction could

have offline consequences, and yet the case study also raises important questions surrounding privacy. Why did department members believe that privacy existed within an online context? How did they create privacy within a public medium? Do departmental members agree on similar expectations of privacy? If they disagree, what would be the ramifications of disparate understandings? How can university departments and other organizations prevent privacy violations during professional interactions?

Crafting a response to these questions requires an understanding of how previous privacy studies inform the current debate, both historically and in relation to online contexts. The case study is then presented, focusing on how privacy is constructed as a behavioral norm within an online environment, particularly when that online environment lacks any articulation of expected online behavioral norms. The case study also examines the repercussions of an organizational member violating the department's implicit norm of privacy, both in terms of online and offline consequences. The present research leads to an analysis of the case study's findings and their relationship to previous literature. Finally the paper concludes with a summary of major findings and a discussion of how an organization may use this study's findings as a means to norm an understanding of online privacy.

Understanding Privacy

The concept of privacy is a relatively recent phenomenon and was of very little concern to previous moral philosophers like Locke, Rousseau, or Mills; even our founding fathers felt that it was an unimportant issue (Moor 2000). Most critics argue that the idea of privacy was established by Warren and Brandeis' famous essay on privacy published in the 1890 *Harvard Law Review* (Introna 2000). Since then privacy has gained significant public importance, particularly through the 1960s and the development of the internet. Scholars have not settled on a single definition, yet they generally identify three dominant facets of privacy in their examinations: 1.) privacy's socially and contextually contingent nature prevents an encapsulating definition, 2.) the necessity and utility of privacy in human interaction, and 3.) the legal and practical implications of natural and normative privacy. An examination of these dominant facets of privacy leads to a discussion of how previous scholars have explored both online behavioral norms and online privacy and suggests that privacy in this case study should be understood as a socially constructed normative concept within society. This understanding allows readers to see how privacy may be shaped and crafted within organizations, in order to recognize and avoid environments which may contribute to privacy violations.

Privacy's amorphous and socially contingent nature has led scholars to avoid specific definitions, instead suggesting characteristics of the concept. Miller and Weckert (2000) examine privacy's ineffable nature within the online environment. They state privacy is "the condition of not having

undisclosed personal knowledge by others…Personal knowledge…consists of facts about a person which most individuals in a given society at a given time do not widely want known about themselves" (Miller and Weckert 2000, 256). In their attempt to define privacy, they emphasize that the individual is the determinant factor concerning what is or is not private. They also suggest privacy relates to social and power relationships between people, noting that "on the one hand privacy consists of not being interfered with, or having some power to exclude, and on the other privacy is to be held to be a moral right, or at least an important good" (2000, 256). Lucas Introna (2000) suggests a similar understanding in which privacy is a relational concept between members in a society, culturally relative, limits access or control of personal information or private domain, a claim of immunity from judgment by others, and a relative concept that shifts with each matter at hand (190). Miller and Weckert's descriptions, along with Introna's, not only demonstrate that privacy is a largely relative concept shaped by social norms and contexts, but they also convey that privacy cannot be fully defined nor fully described because it is a relative concept that shifts between individuals and societies. Because privacy is a relative and socially contingent concept, online groups and communities must construct their own concept of privacy as a behavioral norm. In relation to organizations, this suggests that if members lack an explicit statement or an agreement upon an understanding of privacy, then disparate views of privacy are likely to develop, thus increasing the possibility of a privacy violation.

Scholars generally agree that privacy is a necessary value for individuals. Miller and Weckert's (2000) argue, for example, that corporations should give employees a sense of privacy in order to ensure production rates. Introna (2000) believes self-actualization requires privacy because "without privacy there would be no self. It would be difficult, even impossible, to separate the self from the other" (194). Similar to Introna, and Miller and Weckert, Gumpert and Drucker (2000) situate privacy as a psychological necessity along Maslow's hierarchy of needs, arguing that humans have, what Moor (2000) calls, an intrinsic right to privacy; that is to say, a necessary value for human existence (Moor, 2000, 203).

Moor argues that humans do not require intrinsic privacy, but rather instrumental privacy, meaning that privacy functions as a means toward an end; in particular, as a means of providing security within a society. Moor also divides privacy into natural and normative distinctions. Privacy can therefore be natural in regards to a "situation in which people are protected from intrusion or observation by natural or physical circumstances" and normative relating to "a situation protected by ethical, legal, or conventional norms" (p.207). Moor's distinction proves helpful in understanding the complexity of privacy situations. He blends the two types of privacy to create a useful understanding of how natural privacy contributes to normative privacy, "an individual or group has normative privacy in a situation with

regard to others if and only if in that situation the individual or group is naturally protected from intrusion, interference, and information access by others" (207). In other words, a physical boundary, such as a building or a room, provides natural privacy by preventing outside intrusion, which is necessary for normative privacy to exist. Moor's article provides insight into the case study by revealing that a mass department email would not have natural privacy, because it lacks the ability to keep others out, but it would have normative privacy based upon social conventions.

The previous scholars reveal significant views surrounding the nature of privacy. Their contributions may seem scattered, but they all contribute valuable insight to the nature of privacy. Miller and Weckert provide a definition of privacy that foregrounds its relative nature. They, like Introna, list characteristics of privacy in order to grasp its amorphous nature. The three critics demonstrate the encompassing and variable nature of privacy. Despite privacy's ineffable nature and scholars' reluctance to define it, Gumpert and Drucker, along with Miller and Weckert, and Introna, believe that privacy is a psychological need for humans. While Gumpert and Drucker view privacy as an intrinsic value, Moor argues that it functions as both an instrumental and intrinsic value. These critics again lend further credence to the view of privacy as a socially relative concept and argue for the importance of privacy within groups and organizations. They illustrate the tension between natural and normative, and intrinsic and instrumental privacy. In regards to the case study at hand, a normative and instrumental view of privacy will be the most pragmatic approach.

Privacy defines the borders between the public and the private through laws and rules as well as ethical norms. A significant amount of research has been generated concerning privacy laws or codes and organizations (e.g., Branscomb 1997, ,Camp 2004, Greenleaf 1997, Kirsh et al. 1997, Schulman 2000, Smith 1994, Woo 2006), and these articles still heavily revolve around "natural and normative" and "instrumental and intrinsic" distinctions of privacy.[3] However, this paper primarily focuses on how online communities establish normative privacy to govern their behavior. Normative privacy most nearly correlates with the case study under because it reflects the larger concern of privacy within online an online environment.[4]

Literature concerning online social communities foregrounds online behavioral norms, and comparisons between studies reveal privacy's socially contingent nature; however, studies have failed to deal directly with privacy as a behavioral norm. Significant research follows the development of online communities because they serve as microcosms within which researchers study the development of societies from their online origins (Mnookin 1996).

3 For an example of this tendency to dichotomize privacy see Schulman (2000) and Woo (2006).

4 I found no studies pertaining to privacy concerns within universities that would have proven relevant to the topic at hand.

While some communities, such as LamdaMoo have established specific rules that govern their online landscape, within these rules, groups establish appropriate modes of conduct called behavioral norms. Behavioral norms represent a significant component of internet research (Blanchard and Markus 2004, Byam, 1995, Campbell 2004, McGlaughlin et al. 1995). Privacy has also represented a significant area of internet studies (Branscomb 1997, Drucker 2000, Greenleaf 1997, Gumpert and Kirsh et al. 1997, Introna 2000, Metzger 2004, Moor 2000, Sheehan 2002 Weckert and Miller 2000), however very few studies focus or examine how privacy serves as a behavioral norm. Blanchard and Markus (2004) and Campbell (2004) found a strong tendency for members of online communities to produce trust amongst them. In contrast, Diane F. Witmer's (1996) study of sexually explicit online communication determined that the majority of subjects "considered privacy unimportant or extremely unimportant, and another 25% were neutral" (9). Witmer, Blanchard and Markus, and Campbell's studies expose how social microcosms pattern behavioral norms, which vary as a concept and relative norm between social groups. Both groups uniquely construct their concepts of privacy through divergent techniques. These studies help to reinforce privacy's normative and socially contingent nature.

This literature review establishes the relative and socially contingent nature of privacy, but has eschewed a definition of privacy. An understanding of privacy grounded in a specific definition will help with the paper's further inquiry. For discussion purposes, privacy is a culturally relative and relational concept that shifts with each situation and exists between members in a society as a means to limit access or control of personal knowledge or private domain, from judgment by others. The definition blends components provided by Introna (2000) and Miller Weckert (2000), and emphasizes the socially and contextually contingent nature of privacy. Since the online environment seemingly lacked particular rules, the case study at hand suggests that examining privacy as a behavioral norm is necessary. Scholars have also conducted significant studies concerning online behavioral norms, yet few have addressed privacy as a behavioral norm. Privacy, like any other group norm, is relative to the group, and constructed through patterned behavior. Introna explains that "privacy through the rules, rituals and so on that demarcate the public/private domain for a specific class of relationships, creates simplified relational structures that allow the individual to cope with the complexity—also to appropriately invest in a selected set of intimate relationships" (193). Privacy becomes a norm that groups must attempt to establish through patterned behavior. New members joining a group create the challenge of educating new members in the group's behavioral expectations, and older members will correct the inevitable mistakes made by new members in order to maintain their environment. However, it seems likely that not all members will share the organization's norms and, in regard to privacy, develop their own understanding of its meaning in relation to the

organization. Disparate beliefs of privacy within an organization could have significant online and offline consequences.

This paper's findings answers Anne Branscomb's plea that "surely there are some areas in the electronic environment that should be maintained as private spaces. These would be comparable to a private home or club where friends and peers may share private and confidential communication" (p10). Branscomb's plea reflects the paper's larger question: How online privacy is constructed within an organization? This case study offers an understanding of how groups construct online privacy, as a means to help organizations and communities prevent future online privacy violations. In order to explore the social consequences of incongruent understandings of privacy in online and offline communication, a case of perceived online privacy violation is now explored, with the purpose of answering three research questions arising from the previous discussion of privacy which the current literature:

1. Does privacy function as an online behavioral norm in an electronic environment that lacks explicit rules of conduct, particularly in regards to privacy?

2. How does an organization, when it lacks explicit rules of conduct, norm privacy as an online behavior? And, do members develop congruent understandings of privacy through this norming process?

3. What online and offline consequences might organizations suffer from online violations of privacy?

Exploring the Construction and Conflict of Privacy

On September 29, 2006, at a public university, a professor forwarded by email an article that had appeared that day in the university's school paper to faculty, staff, and graduate students. The article contained a letter from the university president admonishing students for their comments on diversity, which had previously been printed in the school's newspaper. A professor then sent the article to a department office assistant, asking her to forward the article to professors, graduate students, and staff of their department. As the article was forwarded to members within the department, various members applauded and criticized the president's column. In all, six people responded to the article via the departmental email list: 2 graduate students praised it, and 2 students and 2 professors criticized it. Thirty minutes after posting a critical commentary about the president's speech to the group, a graduate student received a personal email from the university president attacking the student for his email.[5] The president chose to ignore the comments of other graduate students and professors, singling out the comments of this one particular graduate student. After learning about this situation, departmental

5 This particular graduate student had been the victim of a hate crime a year earlier, during a wave of hate crimes against international students. Following the attack the graduate student formed a university wide student organization that criticized the university's lack of response to the spate of incidents.

members were notably distressed, not only by the president's response, but by the perceived violation of trust and privacy of someone forwarding internal departmental communication outside of the department. This resulted in faculty members discussing the incident, both online and in faculty meetings, without graduate students present or privy to these communications.

Directly following the incident, the department head, a veteran professor, and a staff person all sent out mass department emails condemning the forwarder's actions and calling for the need for privacy and the right to freedom of speech. These emails communicated the seriousness of the forwarder's actions and revealed that these faculty members felt it incumbent on themselves to convey the communicative rupture they experienced. While emails created narratives from which positions can be extrapolated to frame the public response to the incident, surveys were used to determine whether behavioral norms concerning privacy were largely agreed upon among the faculty or the graduate students. Although professors and graduate students were dismayed by the forwarder's actions, why did they believe a degree of privacy existed within the department's mass email discussion? Exploring this incident and the ensuing dialogue following it provides a valuable insight into the incongruent expectations of privacy which can occur within organizations and the resulting social consequences.

Methodology

In order to investigate and analyze this case study, public departmental emails discussing the incident were collected. Data collection also included an anonymous open-ended survey on general views concerning the function of the department's mass email list which was distributed to graduate students, faculty, and staff. This was followed up by interviews with professors and graduate students on their personal views of privacy and how the incident impacted their online behavior. Finally, a focus group was conducted with graduate students to investigate how online behavioral norming may have influenced their views of the department's mass email list.

Surveys were distributed to 71 professors, staff, and graduate students within the university department. Eight graduate students and one associate professor responded to the survey. While response levels were low, the completed surveys represent varying personal opinions about public and private spaces within the internet. Surveys and public emails are augmented by interviews and a focus group, which were used to collect more diverse views of privacy. Four professors, a staff member who headed the IT department, and the graduate student who was victim to the forwarder's action were interviewed. The four professors varied in rank (three full professors, and one associate professor), as well as administrative positions (one department head, and one assistant department head). The focus group included five graduate students of varying experience levels. All interview and group participants were asked questions concerning their general understanding

of privacy, their understanding of privacy within the department email list, and how the departmental privacy violation impacted their online and offline interaction within the department. The International Review Board approved the human subject methods adopted for this study.

Findings

1. Does privacy function as an online behavioral norm in an electronic environment which lacks explicit rules of conduct, particularly in regards to privacy? Findings confirm that privacy functions as a behavioral norm in a space without formal rules of conduct. New department users observed the online behavior of other department members in order to determine how to shape their own online actions.

2. How does an organization norm privacy as an online behavior when they lack explicit rules of conduct, and do members develop congruent understandings of privacy through this norming process? Members extrapolated expectations of privacy from their offline environment and other online experiences as a means to inform their online departmental behavior and shape their expectations of their fellow departmental members. Members expected fellow members to use their previous understandings of privacy to gauge what content or messages should or should not be considered private. When members deviate from departmental online behavioral norms, then senior members of the department publicly condemn the deviant behavior both through private meetings and emails. Emails somewhat clarified departmental expectations of privacy; however, some members still disagreed with the department's use of the mass email list as a business, political, and social tool.

3. What online and offline consequences might organizations suffer from online violations of privacy? Some members were cognizant that their online conduct could have offline consequences; however, other members, such as full professors, felt unconstrained in their communication. The forwarder's actions had a varying effect on department members. Those with tenure felt unimpeded by the forwarder's action, while those in more vulnerable positions (i.e. graduate students, staff, assistant and associate professors) were deeply impacted by the forwarder's action, either deliberately trying to prevent the forwarder from impacting their communication or significantly changing their communication pattern by stripping it of humor or refraining from discussions occurring within the department's email. The forwarder's violation of privacy disrupted online department discussions and destroyed the sense of privacy department members held.

Privacy as a Behavioral Norm within a Public Forum

To understand how privacy functioned as a behavioral norm within the department, it is important to understand both the purpose of the department's email list and the lack of rules that governed its use. The department's email

functioned as convenient means of communicating issues to a large audience. One staff member stated,

> Generally, the list is used by faculty to inform the department of meetings and meeting times, of successes of graduate students and/or other faculty; to alert people to the many lectures that are given within the department, the university, or the community at large…Occasionally, the list is used by faculty to discuss freedom of speech issues and/or hot topic issues around the university.

Emails from the department's various members were commonplace and part of the day-to-day affairs of the department. One professor articulated that the department's email system "feels like a private conversation, but in fact it's a public medium." Although the department's email served as a central form of communication within the department, the department email lacked any formal rules for interaction. Interviewees and focus group members echoed similar understandings of the department's email system. One professor acknowledged "we're operating on principles that aren't articulated…we don't articulate an explicit meaning of privacy because we assume, and myself included, that we're operating on the same understanding." The head of the department also clarified that "there's no formal instruction or guidance on protocol of electronic communication… instead people used their common sense judgments."

Without formal rules of conduct new department members relied on their observations of other department members' online interaction to learn departmental online behavior. Surveys confirm this expectation, one respondent claimed that they "learned by example": "I simply observed discussion on the listserv." Another respondent echoed a similar perspective by stating that "there was no didactic process of instruction, but a dialectical one in which the informal rules of conduct were communicated by doing (e.g., by reading how others responded to posts in an informal manner… and when or under which conditions response was appropriate)." All nine respondents agreed that no formal codes of conduct existed for online interaction within the mass department email system, but they did recognize that implicit behavioral norms were communicated by example through the observation of interaction by other online members. One graduate student stated in an interview that "there is no clearly defined agreement…it was more like a norm. It was accepted…it's just like an understood norm we are socialized into."

Interviewees agreed that, although they lacked formal rules to follow, implicit behavioral norms were apparent and participants felt obligated to respect these norms. They also specified that privacy seemed to be an implicit norm that department members accorded one another. One senior professor mentioned "at the very implicit level I have been operating as if there is a norm . . . I don't think I was the only one who assumed we were talking within

the department." A graduate student made a similar comment, stating "There is this norm that when you are talking about something [sensitive] you are not expected to go and talk about it outside." While students and professors acknowledged an online norm concerning privacy they largely suggested that it was related to offline experiences. One graduate student suggested the same etiquette that governs sensitive issues offline should also govern our online interactions by noting that "breeching of trust by sending an email or talking across the table isn't all that different." The department head's reference to "common sense" reinforces the expectation in which participants should rely on their offline sense to inform their decisions online.

How Privacy is Constructed

As previously stated, department members were operating on the belief that privacy was an implicit norm in the department, largely informed by their offline experiences. In general to reinforce group norms, correcting the mistakes of members proves an important task of norming behaviors within a group. When department members learned the private email had been forwarded outside of the department, senior department members disciplined the forwarder's actions within their emails by articulating a more concrete sense of privacy and behavioral expectations of department members by directly calling attention to the private nature of the online discussion. One member stated "I think it wholly justifiable to have considered the emails and comments made in the emails to be private to the department." Another department member reinforced the private content of the email discussion, explaining that "the content of these emails were clearly intended as an 'in house' (i.e. within the department) colloquy." This same member also reproaches the forwarder's actions by expressing that "I am appalled that this happened…this incident represents for me a breach of trust of organizational norms and standards of confidentiality and respect that have characterized this department." The third department member again clarifies the private content of the emails and chastises the forwarder actions, stating that "One shouldn't forward messages written by others without that person's consent, unless you perceive it as illegal, a threat to yourself or someone."

The three faculty members' rebuking of emails seems to serve two functions. First, rebuking functions as an example of norming behavior to prevent similar incidents from occurring again. All three department members address the forwarder's action as inappropriate. By publicly chastising the person, they norm future online behavior by teaching other members, as well as the transgressor, what actions to avoid. Second, the emails directly teach members how to recognize a private situation by claiming that whether or not the forwarding of an email outside of the department "was due to well intentioned but naïve motives, a personal agenda, or ignorance, doesn't matter. One shouldn't forward messages written by others without that person's consent." The department members' emails establish an example of what type of content and contexts

should be considered private. By pointing out the mistake of an individual, as well as noting the severity of the individual's mistake, the emails attempt to shape future online interaction. Professors and graduate students should now want to refrain from any similar type of mistake.

Focus group members emphasized two divergent views of graduate students and professors concerning the department's email. One member suggested that members viewed the list as "a tool or a forum," stating "I feel like professors are more likely to see it as a forum. I don't know if it's because they have more security, but I know grad students I've talked to definitely see it as a tool." All focus group participants agreed with this assessment; although they disagreed as to whether the email list should be a tool or a forum. One student articulated that "what bothers me most is that it's become a discussion forum;" another student supported this view stating "I don't think the listserv should be a site where people get on their soapboxes and present a particular political or religious ideology."[6] A graduate student complained of the involuntary participation in the department's email list noting, "I wouldn't mind [professor A] saying something I subscribed to, but I'm involuntarily involved in this. If I sign up to a forum that's fine, but I'm not signed up for this. I didn't sign up for this!" Students disagreed as to how the email list should be used, but one student, noting the importance of the email list, stated that "I'm not going to opt out of the listserv for fear that I might miss something important." Focus group participants articulated significant issues surrounding the department's email list, primarily noting the discrepancy between how faculty and graduate students viewed the email list. These incongruent views of the email list, related to a lacking clarification of the list's purpose, may have led to the privacy violation at hand.

While focus group participants were uncertain of the function of the email list, they did agree that privacy can occur within a public space. One student noted, "I think we have an ethical right to privacy…there is an accessibility issue." Survey responses also suggest that privacy can occur within a public space. Seven of the nine respondents believed the department's mass email to be a private discussion, but nuanced their notion of private by stating the communication was private in nature but occurred within a public space. These seven respondents likened the email to a conversation in public that is private in nature, such as

> "a private discussion occurring in a public space…akin to having a personal conversation at your table in a restaurant. You're aware that others might hear, so you lower your voice so you can speak only to the person at the table…. you don't expect the person you're talking to at your table to tell the waiter what you were just talking about.

6 Students call, for lack of a better term, the department's mass email a listerv, but it should be noted that the department's email list is not a listserv and, therefore, lacks the formal requirement of voluntary participation.

Respondents believed that even though their email conversations occurred within a public university they had a social expectation of privacy, rather than a right, because the content of the email conversation was socially sensitive. Department members must use previous understandings of privacy, potentially offline experience, to determine whether or not the content of an email is sensitive in nature. Survey respondents, interviewees, focus group participants and department emails all emphasized the normative nature of privacy within a context. One respondent likened the ethical boundaries to normative group expectations, "I think we do have an expectation of having a private space that can be defined based on affiliations….you don't expect people from outside the department to come and use the kitchen, although that aspect is never articulated in written or verbal form."

Privacy, as a departmental norm, was clarified and enforced by the disciplinary emails sent to the department by various members. The social castigation of the forwarder's action was designed to prevent the action from occurring again; as one interviewee noted, "I hope that whoever did that learned a lesson not to do something like that again…I hope they became more sensitized as a result." While the norm of privacy was clarified, the email list's purpose continues to remain a contested issue. Focus group participants noted divergent views between how faculty and graduate students approach the email list; the discrepancy determined whether views within the email list should be honored as public or private. One student noted "I was mostly surprised that people thought [the email list] was a private thing…I've always treated it as a tool." The differing views concerning the email list's function leaves the department vulnerable to future privacy violations. Even if the sensitivity of a topic is accepted by a department member, how they view the function of the email list can also determine whether or not they will view the discussion as a public or private issue.

Social Consequences of the Forwarder's Actions

Department members' trust was violated by the forwarder's actions. Seven survey respondents believed the department's mass email list was a private forum before the email incident. Six of those seven now viewed the department's email list as a public forum and would be more careful in their future interactions. Some respondents suggested they would interact on a limited basis, making sure they refrained from providing their opinions, with one student noting "I will not use the listserv unless I have to." Overall the seven respondents had experienced a breach of trust and privacy that they felt would change their future interaction on the email list. Three of the respondents claimed their sense of privacy could never be regained, and others suggested they would be careful how they interacted in the future.

Two survey respondents suggested that email list members should have diminishing expectations of privacy the larger the department's email list becomes. They argue a smaller department with a smaller email list promotes

greater interaction and stronger relationships between members, while a larger department with a larger email list prevents members from establishing the necessary bonds to promote privacy. One respondent elaborated that privacy changes "when it's taken to the level of sharing personal opinions to a list of 82 people."

Interviewees and focus group participants provided a variety of views as to whether or not the email list was a public or private forum. The majority of people agreed that it was a private discussion within a public form of communication; however, they also largely believed that group and social norms should have been an indicator to keep the sensitive topic private. Focus group members varied in how the event impacted them and they largely were divided by how they viewed the purpose of the email list. Those who viewed the email list as a forum no longer considered it so, and those who viewed the email list a tool did not have their views changed by the incident. The investment of trust in the department's email list seemed to be a primary factor which changed member's online interaction. One focus group member noted "I think the bigger violation of trust is forwarding without telling… having that courtesy to say 'would you be opposed to me doing this'…I think that's where the violation of trust is." Because some graduate students had their trust violated, most agreed that they viewed the department and some of its members with suspicion. The forwarder's action disrupted the sense of community and trust graduate department members had for one another. One student stated

> I didn't ever want to be involved in a conversation online again….there is someone who is untrustworthy…there's no way of knowing who's going to send to who. It seemed like a breech of trust to me…there was something that was lost so now it is only a tool to me and will never be a forum.

The international student who suffered the repercussions of the forwarder's actions stated that he felt "someone breeched my trust" and he now viewed department members with suspicion because he viewed the forwarder's action as a personal attack. The student noted that "I wasn't shaken by the incident, but I would be lying if I claimed it didn't affect me negatively." Graduate students who regularly debated within the department's email list now felt they should refrain from such actions. One student mentioned "I'm not as spontaneous anymore as I used to be and irony and sarcasm, which are so my style, tend to take backstage now." Other students tried to deliberately prevent the incident from impacting their online behavior by continuing their online brashness, although they noted that they often considered the "worst-case scenario" their actions might cause before responding or engaging in a debate. While graduate students varied in how the incident impacted their online, most agreed that the incident had made an indelible impression that would permanently impact their online

behavior. The majority also suggested that they now viewed the department with an air of suspicion

Professors' online behavior went largely unchanged, although the incident did prompt most to be more sensitive about privacy matters. The department chair noted that "I'm more mindful about sending sensitive information on." Other professors echoed similar perspectives. One department member shared that her communication was flattened by the forwarder's action stating "I was conservative before and I'm more conservative now, if that's at all possible…I'm more conservative about interjecting humor." The department member elaborated "that's not the kind of behavior I would have expected five years ago…there was more respect then than what I see now." For this department member the incident marked a permanent change for the department, and one that in her opinion was long coming.

In general, department members varied in their overall estimation of how the forwarder's actions impacted the department as a whole. Some members felt there was little change; however, a small majority felt that "the situation really did degrade the community here in this department." One professor reflected that "we haven't had many interchanges like that particular interchange since that happened…so it may have had a bit of a chilling effect." One graduate student noted, "I think from then on people didn't really respond to public emails…I think it instilled a kind of fear or distress among colleagues…I decided I would not respond to emails from then on." Consensus among graduate students and some faculty members in the department seems to suggest "an online chilling effect" has occurred from the forwarder's actions. At an immeasurable level, the forwarder's action seems to have psychologically distressed department members, influencing how they interact both online and offline.

Discussion

1. *Does privacy function as an online behavioral norm in an electronic environment which lacks explicit rules of conduct, particularly in regards to privacy?*
2. *How does an organization norm privacy as an online behavior when they lack explicit rules of conduct, and do members develop congruent understandings of privacy through this norming process?*

Thus far, this article has suggested that privacy functioned as a behavioral norm within the university department. Lacking any formal codes of conduct that influenced online interaction within the email list, or even a specified purpose of the email list (tool or forum), department members learned how to interact based on observation of more experienced members. Department members, particularly graduate students, were forced to learn online departmental behavior by observing other more experienced members; as one student put it by "follow[ing] the leader and engag[ing] in mimicry." Another

student echoed this idea, noting "because everyone else does it, to do otherwise would be like an outsider." When members made mistakes in the department's online environment, senior members criticized their actions as a means of norming group behavior to a particular understanding of privacy. These findings confirm that norms, such as privacy, were learned based on observed patterns of behavior and this echoes findings by Baym (1995) and McLaughlin et al. (1995). For the university department under scrutiny, privacy functioned as Moor's "normative" value. Department members expected other members to rely on their "common sense judgment" to determine what information should or should not be shared with others. Privacy fluctuates as a relative contextual value, which changes according to situations. Moor, Introna, Miller and Weckert, and others largely held that privacy was a relative and contextually dependent value. If the sensitive department email was forwarded to a spouse of a coworker then it seems less troublesome than if the email were forwarded to the person of whom it was critical.

As departmental members experienced the norming of privacy through observation and modeling, participants also endured norming behavior through chastising emails that sought to clarify departmental expectations of online behavior concerning privacy. Since the department lacked formal rules or an articulation of the function (tool or forum) of the department's email list, the department remained vulnerable to mistakes as each year new students joined the department and were ingratiated into the system through trial and error. As one graduate student succinctly put it, "as far as online [behavior], the best way to learn something is to make a mistake." However, this approach to online communication left the department more vulnerable to online mistakes committed by its members.

Interestingly, students held widely divergent views concerning the function of the department's email list. Some students believed the email list should serve as a tool and a forum where people could communicate necessary business related messages, but could also discuss and engage the department members on a variety of social and political issues. One member expressed that

> this department is one that is almost family oriented, so to me it wouldn't be appropriate for this particular department to stop having some sort of political or philosophical discussion online…with this departmental culture I think it's appropriate to do the soapbox thing.

Yet, other members viewed the list as a tool only, one member articulated the conflicting position noting

> I was mostly surprised that people thought it was a private [forum]…but as far as changing behavior…it's the same way I've always treated it, as a tool. And I'm sorry but I have to say when I get some of those [professor A] emails I think 'who cares, why is this in my inbox, why do I have to see this right now.'

Those department members who viewed the email list as a tool felt offended to see members treat the email list as a forum because they felt as if the discussions were forced upon them. Department members' divergent views suggest that some members resisted the department's attempt to norm online behavior. As the previous student suggested, "as far as changing behavior…it's the same way I've always treated it, as a tool." Unless these differing views of the email list are resolved, the department could experience more serious consequences due to incongruent behavioral norms.

In interviews with faculty members, they seemed to take for granted that the email list should function as both a tool and a forum; none suggested that it should only function as a strictly business communication tool. On the other hand, graduate students voiced their confusion with the department's email list, particularly when they first entered the department. One student explained that

> faculty members who don't change much from year to year have a sense of established culture. New people don't have that sense of established culture, and so it's still as if you're in training. You're still learning the culture and so it seems different from the grad student perspective not only because of issues of power, but because how much a person identifies with this culture.

One member suggested that the department's size prevents members from forming close connections with each other and the loss of these interpersonal connections may have led to privacy problems. A student echoed her alienation within the department expressing frustration at not knowing other department members:

> If I don't know the people sending it, I feel no obligation… Not only am I not initiated in the culture, but I don't know who you are and you're sharing this message, so that makes me even more likely for me not to feel the need. You're sending me this message to me and I don't know you, don't know what you're about. I feel less beholden to that concept.

This student did not feel compelled to respect her coworkers because she lacked any real connection to them. She lacked a context for understanding their positions within online discussions. Faculty members seemed to overlook the fact that other department members might disagree as to the function of the email list and this presumption could have played a role in the department's privacy violation.

3. Do organizations suffer online and offline consequences as a result of privacy violations?

Online and offline consequences, and conceptions of whether the email list served as a public tool or a private forum, were related to hierarchical

positions within the department. Professors' online behavioral habits remained largely unchanged following the email incident. Potentially, this is because their positions within the university were secure and a no member in their ranks was affected by the incident. While professors largely remain unchanged in their online behavioral styles, some graduate students shifted dramatically, both in their online communication and their view of department members. Those graduate students who treated the list as a tool remained largely unchanged by the incident; however those who treated the email list as a forum were deeply affected. Graduate students largely acknowledged that "the last thing I need is a higher up pissed at me," and so they felt the best course of action "was to just sit by passively." Those who regarded the email list as a forum now treat the list as a tool. Some graduate students were resistant to allow the forwarder's actions to impact them, but they conceded that they still considered political repercussions to their online actions. Students who considered the list a forum were more likely to view other department members suspiciously because their trust had been violated. Of course, the international student who was contacted by the university suffered the most harm because it fundamentally changed the way he viewed the department and, for him, it caused "irreparable harm." Department members varied in how the privacy incident impacted offline and online interaction within the department. As a community the department no longer engages in forum debates, not as a rule, but because few people seem willing to discuss sensitive issues among those they cannot trust to maintain a sense of privacy.

Since privacy serves as an online behavioral norm which shares connections with offline social conventions of privacy and since privacy violations have real offline consequences, how might organizations prevent a similar incident from occurring? Kollock and Smith (1996) suggest that only cooperation from all members can bring about a change in interaction, but they also recommend the implementation of rules. Findings suggest that because privacy is an instrumental behavioral norm, rules, protocols, or guidelines may be helpful in clarifying to new members how they are to interact within the department's email list. The difficulty with behavioral norms is that they are usually observed by new members, which often requires mistakes in order to grasp the group's social expectations. New members must intuit how to interact within the group, and guidelines could help facilitate this process. Furthermore, department members' divergent views of the email list's function would also be an important matter in which members should reach agreement to protect each others' sense of privacy. Because it can not successfully keep information from nonmembers, members might agree that the department's email list does not demonstrate natural privacy. Nonetheless, members could rely on behavioral norms to treat the content of information as private and thereby rely on larger offline social norms. Or if protocols articulated that the email list should be treated as a private space,

then members who disagreed with this view could abstain from conversations but continue to respect the privacy of their fellow members.

When asked about how to prevent a similar situation participants varied in their responses, however, most were opposed to rules or protocols, largely because they could not be enforced. Participants noted that if rules or protocols could not be enforced then it left other members vulnerable by providing a false sense of security. Graduate students all agreed that a discussion during graduate student orientation would have been helpful to teach them the various purposes the email list served and also to emphasize the importance of privacy in relation to online discussions. All participants agreed that a discussion should take place to reach a consensus within the department. Because privacy is a contextually relative value whose group expectation varies between communities, organizations need to examine how privacy plays a role in their particular environment. Clearly business organizations will have a different understanding than a university department. Each specific organization or department within an organization should examine the role privacy plays in their community and then determine what course of action could best prevent a future privacy violation, because serious consequences result from privacy violations. Organizations which use online communication and lack an explicit statement concerning privacy make themselves vulnerable to privacy violations and a potential social rupture within internal communication.

Conclusion

This paper has sought to explain how online privacy is constructed as a behavioral norm within an online public medium. Online privacy is a normative value, meaning that it does not come from physical boundaries; rather, it comes from the expectations that other people will not share certain information. Privacy is contingent on the social situation at hand. When privacy violations occur, online members may reinforce the behavioral norm by shaping online behavior with communication that seeks to correct the future behavior of other members. Members may explicitly state their expectations of online behavior and may also chastise those members who failed to act within the group norms, as a means to reduce the deviant behavior. Organizations may prevent online privacy violations through a number of approaches; however, groups must be cognizant that privacy policies will be unique to the culture and social structure of each specific organization.

Perhaps the most distressing finding is that the department's email list has been significantly changed by the forwarder's actions. Change may result from new students and professors revitalizing online discussions, but it will take time for members to forget the email incident and some members have been irreparably changed by the incident. Technological advancements only served to stifle communication rather than enrich

community. All respondents agreed the email list was an effective forum for general emails, but following the email incident, most believed it should not be used for departmental discussions. In this incident email as a technological innovation which can further facilitate communication has only served to repress communication between individuals and within departments. The inherently public nature of the internet leaves it vulnerable to exploitation or even mistakes that can have long lasting effects on users. Rather than create the Utopian community Rheingold prophesized, the internet may perpetuate the continual struggle of individuals between their public and private selves.

Future research needs to examine whether or not protocols or rules are effective means of preventing privacy violations, how organizations effectively norm online behavior and the differences between using an inter-organizational communication medium as a tool or a forum? Scholars also need to examine the role of privacy in the various online communicative contexts (web blogs, facebook, video sharing services, and listservs among others). This study examines privacy as a behavioral norm by relying on previous analysis of online behavioral norms and online privacy. This study uniquely examines a privacy violation occurring within a university department as a means of learning about issues concerning online privacy; however, similar situations could also be found at various businesses and organizations. In this case, establishing policies concerning privacy would benefit nearly all areas of online interaction be it academic, organizational, business, or social groups. Privacy is a paramount concern for people in our digital age and understanding how privacy functions and how to prevent privacy violations is of crucial importance both now and in future technological changes.

References

Baym, N. K. (1995). The Emergence of Community in Computer-Mediated Communication. In S. Jones (Ed.), *Cybersociety* (pp.138-164). Thousand Oak, CA: Sage Publications.

Blanchard, A. L., & Markus, L. M. (2004). The Experienced 'Sense' of a Virtual Community. *The DATA BASE for Advances in Information Systems*, 35, 65-79.

Branscomb, A. W. (1996). Cyberspaces. *Journal of Computer Mediated Communication*, 2.1.

Camp, J. L. (2004). *Trust and Risk in Internet Commerce*. Cambridge, MA: MIT Press.

Campbell, H. (2004). Challenges created by online religious networks. *Journal of Media and Religion*, 3.2, 81-99.

GreenLeaf, G. (1997). A Proposed Privacy Code for Asia-Pacific Cyberlaw. *Journal of Computer Mediated Communication* 2.1.

Gumpert, G., & Drucker, S. J. (2000). The Demise of privacy in a Private World. In Baird, R., Ramsower, R., & Rosenbaum, S. E. (Eds.), *Cyberethics* (pp.171-188). Amherst, New York: Prometheus Books.

Introna, L. D. (2000). Privacy and the Computer. In Baird, R., Ramsower, R., & Rosenbaum, S. E. (Eds.), *Cyberethics* (pp.188-200). Amherst, New York: Prometheus Books.

Kaplan, D. A. (2006). To catch a leaker. *Newsweek* Sept. 6, 2006. www.msnbc.com Accessed on Nov. 17th 2006.

Kirsh, E.M., Phillips, D.W., and McIntyre, D.E. (1997). Recommendations for the Evolution of CyberLaw. *Journal of Computer Mediated Communication* 2.2.

Kollock, P. and Smith, M. (1994). Managing the virtual commons. *Journal of Computer Mediated*, *Communication*. 109-128.

Marx, G. T. (2001). Murky conceptual waters. *Ethics and Information Technology*, 3.3, 157-169.

McLaughlin, M. L., Osborne, K. K., & Smith, C.B. (1995) Standards of Conduct on Usenet. In S. Jones (Ed.), *Cybersociety* (pp.138-164). Thousand Oak, CA: Sage Publications.

Miller, S. and Weckert, J. (2000). Privacy, the Workplace and the Internet. *Journal of Business Ethics,*28 255-265.

Metzger, M.J. (2004). Privacy, Trust, and Disclosure. *Journal of Computer Mediated Communication*. 9.4.

Mnookin, J. (1996) Virtual(ly) Law. *Journal of Computer Mediated Communication* 2.1.

Moor, J. H. (2000). Toward a Theory of Privacy in the Information Age. In Baird, R., Ramsower, R., & Rosenbaum, S. E. (Eds.), *Cyberethics* (pp.200-213). Amherst, New York: Prometheus Books.

Schulman, M. (2000) Little Brother is Watching you. In Baird, R., Ramsower, R., & Rosenbaum, S. E. (Eds.), *Cyberethics* (pp.155-162). Amherst, New York: Prometheus Books.

Sheehan, K.B. (2002). Toward a Typology of Internet Users and Online Privacy Concerns. *The Information Society*, 18, 21-32.

Smith, J. H. (1994). *Managing Privacy*. Chapel Hill: UNC Press.

Vigas, F. (2005). Bloggers' Expectations of Privacy and Accountability. *Journal of Computer Mediated Communication* 10.3.

Witmer, D. F. (1996). Risky Business. *Journal of Computer Mediated Communication*, 2.4.

Woo, J. (2006). The Right not to be Indentified. *New Media &Society*. 8.6, 949-967.