5-2017

# "We Were Not Prepared to Tell People Yet": Confidentiality Breaches and Boundary Turbulence on Facebook

Jocelyn M. DeGroot
*Southern Illinois University Edwardsville*

Tennley A. Vik
*Emporia State University*

# "We Were Not Prepared to Tell People Yet":

# Confidentiality Breaches and Boundary Turbulence on Facebook


## Abstract

Communication Privacy Management theory provides a framework for investigating confidentiality breaches that occur on Facebook. Open-ended online questionnaires served as mechanism for collecting data about privacy violations and the resulting boundary turbulence. Privacy violations validated three a priori categories (Petronio & Reierson, 2009) of confidentiality breaches (privacy ownership violations, discrepancy breaches of privacy, and pre-emptive privacy control). Findings indicated that the lack of established explicit privacy rules led to privacy violations and boundary turbulence. Results also provided insight regarding motivations of privacy violations, reactions to privacy violations, and the role of privacy rules in the violation.


Keywords: Communication privacy management, Facebook, privacy rules, boundary turbulence, online communication

## 1. Introduction

"Congrats on your pregnancy! I can't believe you haven't announced it yet!" With one public Facebook post, a Facebook user has violated the privacy of another. Information ownership and privacy rules are becoming blurred as technology advancements have exceeded the rate of developing up-to-date privacy settings and privacy norms online. Facebook has become one of the main tools for social interaction, as Facebook had over 1 billion active daily users for September 2016 (Facebook, 2017). Due to its fast advancement and popularity, privacy violations on the website via a person's wall or news feed has become an important communication concern among users. A *New York Times* article discussed this very notion, explaining that although individual users might be careful with what they post online, online friends and colleagues can often disclose personal information for them (Lohr, 2010). This unwanted public disclosure of private information can be problematic because, as Walther and Parks (2002) found in their investigation of warranting theory, people are more likely to judge a person based on what others post on that person's social networking site (SNS) rather than on what the person him or herself posted. By studying examples of unmet expectations of privacy online, we can begin to better understand why people violate others' privacy in an online setting and how communication can be adjusted to better protect that privacy.

Communication Privacy Management (CPM) theory addresses the dialectical tension between disclosure and privacy, describing how and why people decide to reveal or conceal private information. Prior research has examined CPM in a variety of face-to-face (FtF) contexts including families (Afifi, 2003), healthcare (Petronio & Kovach, 1997), and in the workplace (Allen, Walker, Coopman, & Hart, 2007). Recently, studies have focused on one's own online self-disclosure and perceptions of privacy on SNSs (Acquisti, Brandimarte, & Loewenstein,

2015; Child, Pearson, & Petronio, 2009; Christofides, Muise, & Desmarais, 2009; Debatin, Lovejoy, Horn, & Hughes, 2009; Ellison, Vitak, Steinfeld, Gray, & Lampe, 2011; Millham & Atkin, in press; Trepte, Dienlin, & Reinecke, 2014; Vitak, 2012; Vitak & Kim, 2014; Waters & Ackerman, 2011). Child and colleagues have extensively explored CPM as it occurs online, examining the parent-child relationship and parental Facebook friend requests (Child & Westermann, 2013) as well as privacy management during blogging (Child, Haridakis, & Petronio, 2012; Child et al., 2009).

Although many researchers have explored CPM online, few have focused on the privacy violations and resulting unrest that occur when one person reveals something confidential about *another* person online. These actions can have adverse consequences on interpersonal relationships. Houghton and Joinson (2010) found that privacy violations can negatively affect friendships, citing issues related to trust and respect. Petronio and Reierson (2009) describe an informal confidentiality contract that exists between interpersonal partners. When this contract is violated our expectations of trust within the interpersonal relationship may shift causing a climate of distrust. Further, Wang et al. (2011) assessed the regrets that people felt after sharing private information (their own or co-owned), and identified that one regret resulted from revealing another person's secret. In the present study, we focus on the topic of the privacy violation, perceived motivations behind them, and reactions to breaches in confidentiality. The purpose of this research is to analyze privacy violations on Facebook that led to boundary turbulence, investigating instances in which people violate confidentiality of another party.

### *1.1. Communication Privacy Management*

CPM explains the process of concealing and revealing private information and is based on three main elements – privacy ownership, privacy control, and privacy turbulence – that help

us understand behaviors related to the disclosure of private information (Petronio, 2002, 2013). First, *privacy ownership* supports the notion that individuals believe they own private information about themselves, and others who are granted access to this information are authorized co-owners (Petronio, 2013). People then feel entitled to control the flow of the information, which comprises the *privacy control* component of CPM. People establish privacy rules and boundaries to keep information confidential or share the information in an orderly fashion, an action termed boundary establishment. Petronio (2002) warns that it is important to establish explicitly stated privacy rules soon after the information is revealed. She recommends setting concrete rules before a disruption occurs in order to avoid turbulence, essentially so individuals are not given the opportunity to make mistakes. Individuals with whom information is shared become "shareholders" and are expected to follow the original owner's privacy rules, which can be either explicitly or implicitly stated. Explicitly stated rules are direct with clear expectations for how a confidant should treat the information (Petronio, 1991, 2002). This type of rule includes a disclosure warning or prior restraint phrase, such as "Don't tell anyone until I say you can" (Petronio, 2002; Petronio & Bantz, 1991). Implicit rules are ambiguous and can lead to *boundary turbulence*, the third element of CPM (Petronio, 2013). Boundary rule mistakes are a common cause of boundary turbulence (Petronio, 1991). Petronio (2002) argued,

> If the discloser only *hints* at a rule for how to access or protect the private information, the confidant may not really understand the way he or she should treat privacy management. This uncertainty may result in misunderstandings and hurt feelings when the rule is not applied in the way the discloser envisioned. (p. 78) [emphasis in original]

Further disorder can occur because individuals do not always obey privacy rules, even if they are explicitly established (Petronio, 2002). That is, the co-owner of information does not

treat private information in the manner that the original owner expected. Petronio posited that boundary turbulence would likely occur if the privacy management system breaks down. She explains, "When people are unable to collectively develop, execute, or enact rules guiding permeability, ownership, and linkages, the coordinating efforts of privacy management are confounded and boundary turbulence occurs" (2002, p. 177).

Petronio (2002) outlined several reasons for unsuccessful boundary coordination that leads to boundary turbulence, including intentional rule violations, boundary rule mistakes, fuzzy boundaries, and boundary definition predicaments. These violations can "disrupt relationships" and "compromise a sense of trust" (Petronio & Reierson, 2009, p. 376). Betrayal is one instance of intentional rule violation, and this breached confidentiality causes boundary turbulence (Petronio & Reierson, 2009). Information exposure is sometimes done out of resentment, suspicion, or doubt; however, in most cases it is done out of uncertainty (Petronio, 2007). Although boundary rule mistakes can be the result of people acting irresponsibly, these mistakes are often due to people having a momentary lapse in judgment, making incorrect assumptions, or misunderstanding expectations (Petronio, 2002). Moreover, fuzzy boundaries can also lead to uncertainties about information ownership and boundary turbulence (Petronio, 2002). Finally, boundary definition predicaments occur when people make private disclosures in public spaces (such as a Facebook wall).

Solove's (2008) taxonomy of privacy, he identified four activities that lead to privacy-related problems: information collection, information processing, information dissemination, and invasion. Behaviors in the information dissemination category are of increased interest, as these actions also appear to cause boundary turbulence. Specific activities in this category include breaches of confidentiality and disclosures. These are similar to Petronio and Reierson's (2009)

notions of betrayal and information exposure, respectively, that cause boundary turbulence.

We have established that co-ownership of private information can be difficult and can result in boundary turbulence. Petronio and Reierson (2009) expand upon CPM theory by describing in detail breaches of confidentiality and how those breaches impact trust in interpersonal relationships. They create three categories to describe these breaches of confidentiality: privacy ownership violations, discrepancy breaches of privacy, and pre-emptive privacy control. They *describe privacy ownership violations* as, "…people's ability to exercise ownership and control according to their assumptions about rules for regulating their private information is violated" (Petronio & Reierson, 2009, p. 377). Whereas *discrepancy breaches of privacy* are defined as, "…anticipated expectations belonging to an original owner about his or her privacy do not match the actual way co-owners regulate third-party access or the way others gain access to become internal or unintentional co-owners" (Petronio & Reierson, 2009, p. 376). Finally, *pre-emptive privacy control* rules are established because, "previous privacy breaches or a lack of certainty about levels of trust" (Petronio & Reierson, 2009, p. 378). Each of these concepts is posited as a means for understanding a violation of confidentiality (i.e. where boundary turbulence is likely to occur). Because breaches of confidentiality are a central focus of this study, these empirically derived categories from FtF encounters may provide a fruitful area of theoretical focus for this study.

In response to boundary turbulence, the people involved try to correct the problem. They revisit, readjust, or renegotiate privacy rules and expectations of others within the, now-disrupted, collective boundary (Petronio, 2002). Petronio (2002) also indicated that people who breach privacy rules are likely to be reprimanded, excluded from future disclosures, given limited information in future conversations, or warned of their violation. These sanctions also

help identify rules that might have been implied rather than explicitly stated.

Confidants may contribute different private information to the collective boundary, taking into account the breadth and depth of the disclosure. Petronio and Reierson, 2009 note that disclosure is not always reciprocal; the breadth, depth, and intensity of the secret may vary from confidant to confidant which can shift the burden of the collective boundary. Incongruity of disclosure must be addressed in order to restore equity in the relationship. In FtF interactions, people try to restore balance and "equalize the incongruity by asking personal, probing questions" (Petronio & Reierson, 2009, p. 370; see also Petronio & Kovach, 1997). However, online there is not a mechanism to restore equity, particularly on SNSs when a confidant discloses private information to excess of co-owners.

This is not the first study to use CPM in an online context; however, this study's unique theoretical contributions are to first, understand how privacy breaches are happening in online communication, and second, address the inability to stifle a breach in privacy online. For example, Petronio and Reierson (2009) suggest creating a confidentiality contract with a third party should he or she become a co-owner. However, with SNSs, there are many co-owners of information instantaneously. An example of this in a FtF interaction would be using a megaphone to announce private information to a crowd. Although this example may seem preposterous, it serves as a hypothetical example of how many third-party members would need to be involved in a confidentiality contract in an online confidentiality breach.

Although CPM was originally developed to explain offline privacy management, it has also been used to help explain disclosures in online settings (Child & Starcher, 2016; Child et al., 2009; Christofides et al., 2009; Debatin et al., 2009; Ellison et al., 2011; Vitak, 2012), which are further discussed.

### *1.2. Communication Privacy Management in an Online Setting*

Characteristics of communicating online, such as online disinhibition and context collapse, can affect why one reveals information online that does not solely belong to him or her. Although the online context can have an effect on why privacy violations happen, outcomes of privacy violations online are similar to those that occur offline, as those whose privacy was violated adjust their communication or their relationships with the violators.

#### *1.2.1. Characteristics of Online Communication*

First, the online disinhibition effect can result in communication that violates another person's privacy. Suler (2004) defined the online disinhibition effect as, "people [saying] and [doing] things in cyberspace that they wouldn't ordinarily say and do in the face-to-face world" (p. 321). Six factors contribute to online disinhibition, including dissociative anonymity, invisibility, and asynchronicity (Suler, 2004). Because of the anonymity afforded by Facebook and other social media, it is less face-threatening to make statements to or about other people online versus offline. Next, aspects of invisibility reduce one's awareness of the presence and reactions of others, also reducing the perceived risk of disclosing information. Similarly, the asynchronicity provided by online communication allows people to avoid coping with someone's immediate reaction to a statement. Suler identified two types of online disinhibition: benign and toxic. Benign disinhibition refers to revealing personal things about oneself or showing unusual acts of kindness, and toxic disinhibition refers to rude and harsh language, anger, and threats. Either type of disinhibition can lead to people disclosing information and violating another's privacy. Revealing information could be the result of an honest misunderstanding with good intentions, indicative of benign disinhibition. For example, one person might congratulate another in a Facebook posting before the original information owner made the success public.

On the other hand, a person could maliciously reveal private information about another in order to cause distress, a mark of toxic disinhibition.

Context collapse (Marwick & boyd, 2010) is another factor that can affect CPM in an online context. Context collapse refers to multiple distinct audiences on an SNS combining (or "flattening") into one broad audience due to the nature of the SNS (p. 122). *Digital crowding* is a similar concept that explains how information meant for one audience can be seen by another audience (Joinson, Houghton, Vasalou, & Marder, 2011). Essentially, Joinson et al. (2011) argued that privacy threats on SNSs result from excessive social contact. Visible communication (e.g., wall posts, picture tagging, or comments) linked to a Facebook user by his or her Facebook friends can threaten the user's privacy. For example, Person A tags his or her friend, Person B, in a Facebook post. Now, all of Person A's friends can see what Person B was tagged in, and, depending on Person B's privacy settings, Person B's friends can see this item too. As evident, it has become increasingly difficult to navigate the multiple audiences on an SNS and meet one's privacy needs (Marwick & boyd, 2010).

### *1.2.2. Outcomes of Online Privacy Violations*

As evident, online disinhibition can create an environment wherein communication boundaries are violated, causing a host of problems. Communication, privacy, and technology intertwine to cause boundary turbulence in online contexts such as Facebook. People generally take steps to rectify any issues resulting from a privacy violation in order to regain face, as they recognize the importance of maintaining a positive online presentation of self. As indicated earlier and explained by warranting theory, others' comments on a user's Facebook page are seen as more credible than if the user made the post him or herself (Walther & Parks, 2002; Walther, Van Der Heide, Hamel, & Shulman, 2009). In addition, Walther, Van Der Heide, Kim,

Westerman, and Tong (2008) found that a person's social and task attractiveness are affected by others' comments on his or her Facebook wall.

After a violation occurs on Facebook, the person whose privacy was violated can detag him or herself (i.e., remove the link to the user on the Facebook friend's page), ask the poster to remove the offending post, or contact Facebook; however, research indicates that the most effective way to enforce privacy management is to communicate about boundaries when initially sharing information to prevent boundary turbulence from occurring in the first place (Petronio, 2002). To practice effective privacy management, Petronio (2002) also recommends implementing privacy rule foundations, coordinating collectively owned boundaries, and unifying the collectively owned boundaries. CPM rules and boundaries need to be established (both on- and offline) to avoid or prevent potential conflict. Boundaries help the people involved understand who owns specific information, as someone with unclear boundaries often commits privacy violation, resulting in lost trust and explicitly declared boundaries in future interactions.

In some situations, the transgressors experience remorseful emotions after revealing confidential information about another person online. Although users might initially feel "safe" posting sensitive or even malicious information online due to online disinhibition, they often have regrets after publishing the information. Wang et al. (2011) identified reasons people had post-sharing regret. One reason stemmed from revealing a friend's secrets and other sensitive content. Participants in the study said they made these later-regrettable posts because they were trying to be funny, needed to vent frustration, had good intentions (e.g., a "congratulations" type of post), or simply did not think about the consequences of the offending post.

### *1.3. Research Questions*

In this study, we aimed to further explore the notion of boundary violations and

turbulence in an online setting, specifically as these issues transpire on Facebook. We sought to focus on the revelation of co-owned information on Facebook. That is, we examined instances in which a person revealed information about another person on Facebook that was meant to be private. To investigate these issues, we posed the following research questions:

RQ1: What topics are most commonly associated with privacy violations on Facebook?

RQ2: What are potential reasons for the privacy violations on Facebook?

RQ3: Were privacy violators provided with privacy rules prior to the violation?

RQ4: How did people react to privacy violations on Facebook?

## 2. Methods

### *2.1. Participants*

Participants were recruited in a variety of ways. A link to the online questionnaire was posted on Facebook (as the site is the focus in this investigation) with a brief explanation of the study and eligibility requirements. Professors from several universities teaching a variety of communication classes also made in-class announcements of the study to their students, and the link to the questionnaire was posted to their online Learning Management Systems.

Participants were eligible for the questionnaire if they were 18 years of age or older and had a privacy violation experience on Facebook. A *privacy violation experience* was defined as having one's own privacy violated or violating the privacy of another individual. One hundred sixty-nine people completed the qualitative questionnaire, including 94 women and 75 men who ranged in age from 18 to 59 years old, with a mean age of 21.14 years. Participants spent an average of 1.73 hours per day on Facebook and reported an average of 692 Facebook friends. Seventy-three percent ($n$ = 123) of the participants' used Facebook to maintain relationships, 73% ($n$ = 122) used Facebook for entertainment, 61% ($n$ = 103) for networking, 13% ($n$ = 21) for

professional use, and 5% ($n$ = 9) for other uses, which included expressing themselves or gathering information about products. Participants could select more than one reason.

### *2.2. Questionnaire*

After affirming eligibility for the study and agreeing to the conditions of the online consent form, the participant was directed to an online, open-ended questionnaire hosted by Qualtrics. In the first part of the questionnaire, participants were asked to think about their most recent experience of when they perceived someone as violating their privacy by revealing information about the participant on Facebook. Participants described that experience by providing information about the post's content. They were then asked additional questions about that privacy violation and their responses to it.

In the second part of the survey, participants were asked if they had ever violated someone else's privacy via a Facebook post. If the participant answered "Yes," the questionnaire continued by requesting him or her to describe the privacy-violating post and answer additional questions about their participation in the privacy violation. Thirteen percent ($n$ = 23) of participants indicated that they had violated another's privacy at some point. We found no differences in the responses when comparing the violator and violatee perspectives. Finally, all participants completed the demographics portion of the survey. All materials and procedures were approved by the Institutional Review Boards at the authors' institutions.

### *2.3. Analysis*

To make sense of the data gathered though the questionnaire, we utilized thematic analysis to help organize, describe, and interpret the information (Braun & Clarke, 2006). We first used open coding to examine and categorize questionnaire responses into themes. For example, one participant indicated that someone posted condolences for the death of the

participant's grandfather prior to that information being public. This response was coded as "death/condolences." We used the constant comparative method (Glaser & Strauss, 1967) to compare each privacy violation topic to the next in order to garner unique codes. We coded 78 responses before theoretical saturation (when no new responses are given; Glaser & Strauss, 1967) was reached. This coding resulted in nine themes that represent the various topics of privacy violations via Facebook: congratulations, relationship status, surprises, death/ condolences, pictures, location, family issues, contact information, and fights. We then engaged in axial coding to combine similar topics, resulting in two overarching categories: Pre-emptive Disclosure Violations and Discrepancy Breaches of Privacy. The same process of open and axial coding was then repeated for each question from the questionnaire, reaching theoretical saturation each time.

## 3. Results

Using an open-ended questionnaire, we asked participants questions about situations in which a post by another person on Facebook violated their privacy. Using thematic analysis of participants' responses, we identified main privacy ownership violation, motivations for violations, reactions to privacy violations, establishment (or lack thereof) of privacy rules, and changes in communication behaviors.

### *3.1. Privacy Ownership Violation*

As stated earlier, axial coding revealed two overarching themes categorizing privacy ownership violation on Facebook: a) Pre-emptive disclosure violations, or prematurely announcing items the original information owner would have eventually posted, and b) Discrepancy breaches of privacy, or items the original owner probably would have *never* posted.

#### *3.1.1. Pre-emptive disclosure violations*

*Pre-emptive disclosure violations* refer to the discussion of private information not originally owned by the other party, yet the original information owner likely would have posted it eventually. Examples in this category related to changes in one's relationship status, attempted surprises, and condolences for a death.

*3.1.1.1. Congratulations*. The majority of pre-emptive disclosure violations were related to a situation in which a congratulatory Facebook post about an accomplishment, purchase, or change violated the participants' privacy and "took away the excitement" of announcing an accomplishment themselves. An example of a pre-emptive disclosure violation read,

> I had found out that I was pregnant, but didn't want to post it online until probably around 20 weeks, and one of my cousins had put something about "I hear congrats are in order" when I was around 12 weeks.

In another example, a person explained that a friend of hers tagged her in a Facebook post about her acceptance into college before she was able to tell her parents the news.

*3.1.1.2. Relationship status change*. The second largest group of violations revealed a relationship status change, such as a newly dating couple, an engagement, a prom date, or a breakup. One participant explained a violation about her new relationship status:

> I was newly single and a bit embarrassed/shaken about breaking up with my long-term boyfriend. I went out with my girlfriends and we all took pictures. One of my friends titled the album "[Name] is single and ready to mingle!" This was before I had taken off the relationship status on Facebook, and I was still Facebook friends with the ex.

Another person wrote, "I was recently proposed to in December. Before my fiancé and I told all of our family members, one of my friends posted on my wall 'congrats on your engagement.'"

*3.1.1.3. Surprise*. Some privacy violations revealed and ruined a surprise visit, gift, or

party. A participant complained, “My aunt posted a picture of the gift I bought my parents for their anniversary before I gave it to them.” Another person explained that he was planning on sneaking to his hometown to surprise his friends and family, but someone posted a comment revealing his intended visit before he got there, ruining the surprise.

*3.1.1.4. Death/condolences*. The final pre-emptive disclosure violation involves people posting condolences about a death before the person knew about the death or before the whole family was notified properly. For example,

> When my dad passed away last year, out of respect, the family is supposed to announce the death first. I felt my privacy violated on Facebook when numerous people posted about my dad. I know they think they were doing good, but in fact they weren’t. Due to the fact that other family members did not know yet and they had to find out via Facebook due to the fact that we didn’t get a chance to tell everyone yet.

Another participant explained, “I wasn't sure how to deal with it when a cousin posted a condolence on my site regarding a death in the family that had not yet been widely communicated.”

*3.1.2. Discrepancy Breaches of Privacy*

A second group of privacy violation topics comprised the discrepancy breaches of privacy category. These messages would not have been announced by the original owner because it was confidential or inappropriate to share with non-intimate others. Examples of discrepancy breaches of privacy included pictures, one’s location, private family issues, personal contact information, and fights that the original owner wanted to keep unknown or unseen.

*3.1.2.1. Pictures*. The largest subcategory of discrepancy breaches of privacy posts included pictures of the participant. The photos revealed unattractive or drunk participants, a

childhood picture (a “throwback”), or that the participant was somewhere they were not supposed to be located. Some examples in this category include, “A friend of mine posted pictures of me while away on a float trip that I wasn’t supposed to be on. I told her not to post them, but she forgot and still posted a few that I was in,” and, “In high school, my coach threatened to kick me off the football team because he saw a picture of me holding a beer. I was not friends with him on Facebook at the time.”

*3.1.2.2. Location*. Location was revealed by tagging the participant in one’s status or by posting a photo of the participant in a location that he or she should not have been located. One participant described her experience,

> Once my parents called me while I was at a concert that I didn't want them to know about. I went to the bathroom away from the noise and convinced them that I was at my dorm studying for the night. Later, when I checked my Facebook, I saw that one of my friends had tagged me in a post about being at the concert, and I had to untag myself and delete the post from my page before my parents would see it and know that I had lied.

Another person had a similar incident when he was tagged at a beach when he was supposed to be in class reviewing for a test, and he had recently friended the professor of that class.

*3.1.2.3. Private family issues*. Some participants listed family-related situations as topics inappropriately discussed on Facebook. These issues focused on abuse, medical concerns, and parents divorcing. One person explained that a family member of hers had cancer and was undergoing surgery. That family member wanted to keep that information within the family until more information about the diagnosis was known; however, another family member posted something on Facebook, revealing the diagnosis to everyone. In another instance, a participant revealed to her friend that her parents were getting divorced. This friend commented about the

divorce on a status before the family's friends and extended family members were told, which caused embarrassment for both the participant and her parents.

*3.1.2.4. Personal contact information*. A few Facebook users posted the participants' private contact information, such as a phone number, student ID card, or password to an online account. In one example, the participant explained an inadvertent privacy violation: "My roommate posted a picture of my car outside of my home. In the picture you can see my street sign, apartment number, license plate number, make and model of car, etc."

*3.1.2.5. Fights*. Violations in this category occurred when people disclosed information about the study participant taking part in physical or verbal fights both on- and offline. For example, a participant described her encounter with a person who chose to continue a prior FtF disagreement on the participant's Facebook page. The participant said, "The person could have private messaged me, but for some reason posted it for all to see."

*3.2. Pre-emptive Privacy Control*

Survey participants were asked if they had set up any rules with the privacy violator regarding the inappropriately revealed message. Some indicated that they established rules at the time they disclosed the information to their friend, but their friend did not adhere to this rule. For example a participant wrote, "I told my friend not to mention it and I was upset to see that he spilled the beans and posted my info for anyone to see." Others mentioned establishing the same rule regarding pictures being posted. They told the person not to upload certain pictures, but the violator uploaded them despite the rule. One participant indicated that he was always mindful of establishing privacy rules when telling someone confidential information: "If I share personal information with people in a conversation, I explicitly say 'DO NOT SHARE THIS ON FACEBOOK.'" Fifty-seven percent ($n$ = 71) said they did not provide co-owners with an explicit

privacy rule. Additionally, almost half of participants who violated another's privacy on Facebook said they were *not* given a privacy rule about the information before they committed the violation. They realized they committed a privacy violation only when confronted afterward.

Some participants said they declared privacy rules for the violator *after* the privacy violation in order to prevent future transgressions. Rules included not posting pictures without permission, not giving out phone numbers, or simply not posting anything about the person. Many of these rules were also coupled with a demand to remove the offending post or photo.

### *3.3. Motivations for Violations*

Based on speculation from the participants, including information from participants who did violate another person's privacy online, it appeared that the motivation for violating another's privacy fell into one of two categories: either malicious or innocent in nature. When people had malicious intent, it was due to jealousy, spite, retribution, or selfishness. One person described her perception of the other's intent, "I would say that they wanted to feel relevant or something by disclosing information that nobody knew." However, another person explained that his friend posted private information "because they were mad at me and wanted to embarrass me."

For the majority of the violations, however, people indicated that the violator probably meant no harm by their Facebook post. Many suggested that their friend was excited, overeager, or proud. One person wrote, "My friend was happy for me. He was proud of me and wanted to share it with everybody else." Others described the violator was trying to be funny by posting their comments. Numerous participants chalked up the violation to a simple accident or that the person probably did not know it was a "big deal" to reveal that information. One participant who violated another person's privacy explained, "I didn't think she would mind me posting it."

### *3.4. Reactions to Privacy Violations*

Participants had various responses and reactions to the privacy violation. Some had an emotional response, others fixed the issue, and another group claimed to be indifferent.

#### *3.4.1. Emotional*

People described their emotional response to the privacy violation as mad, surprised, irritated, disappointed, angry, violated, or betrayed. Many said they "felt cheated" because they wanted to be the one to share their news. One participant revealed, "I was a little perturbed. It should have been my good news to share when I wanted to." Another wrote, "I was mad, surprised someone actually posted something so personal without my consent." Violations related to pictures, family issues, contact information, and death resulted in the most negative emotions, likely because they are considered "high risk" topics (Warren & Laslett, 1977). Yet, the people who confided high-risk secrets failed to provide privacy rules nearly half of the time.

#### *3.4.2. Stifling an online breach*

Some participants in the study said they tried to fix the issue and, in some cases, save face following a violation. Some people quickly posted their announcement themselves. One wrote, "[After the violation] My fiancé put on Facebook that we were engaged and how excited we are. This was so people would hear it from us and not just a friend." Others also engaged in "damage control," and contacted friends and family would should hear the information first-hand instead of on Facebook. These were particularly evident for the topics related to premature congratulations or comments about relationships. A participant said, "I just had to explain to my parents why I had not informed them yet." Additionally, many people utilized Facebook's built-in settings that help control these situations. Some users detagged themselves from a post or picture. Others adjusted their online privacy settings so they have to approve a photo tag, or they

blocked all wall posts. A small number considered deleting their Facebook account. In some instances, people contacted the violator themselves and asked for the offensive post or picture to be removed. Some privacy rules were created and clearly described after the violation, and other people chose to make changes in their communication with friends who violated their privacy.

*3.4.3. Indifference*

The final example of reaction to a privacy violation was that of indifference. Some people said they were not fazed by the revelation, and others simply ignored the post. One person claimed, "I just let it go." Another respondent was not mad at the violator; she was mad at herself. She explained, "I knew that it was a mistake of my own that I made by sharing the information with her."

*3.5. Relationship and Communication Changes*

As a result of the privacy violations identified in this study, many participants' communication and relationships with the violator changed due to a newly developed lack of trust with the violator. In some instances, the person blocked all communication and ended the relationship with the transgressor. Others increased communication with that person in order to provide additional privacy rules.

In many instances, the relationship between the violator and violated did not change. Sometimes it was because the person was not even aware that he or she disclosed something that should have been private. Others indicated that the relationship and communication did not change because the person who revealed the secret "meant no harm" or that it was revealed "by accident." One participant said the relationship did not change, "but I just feel weird around the person thinking that they might be intentionally trying to find out information about me."

In a few instances, people actually increased communication with the person who

violated their privacy. One person who admitted to violating another's privacy explained, "She communicates to me more what is going on with her other friends so I know when to avoid sharing information about her." Another revealed, "Now we are in a constant battle to get back at each other by posting funny pictures and statuses about each other." She went on to say that the incident likely made their friendship stronger. This reaction was rare.

In many situations, the respondent declared that he or she decided to be selective about the topics discussed with the violator due to lost trust in him or her. For example one person said, "I no longer tell her anything that I want to be a secret or anything that is supposed to be a surprise." Another person explained that this circumscribing type of communication led to a modified relationship, "I do not feel as if I can trust her with information anymore so our conversations are generic." Others indicated that they still share information with the violator, but they wait until everyone else knows about the information first.

Finally, some participants explained that they cut off communication in some manner, and others effectively ended the relationship with that person. Several simply blocked the violator from posting anything on his or her Facebook wall or tagging the person in anything. Others said, "I deleted him from Facebook," "I don't speak to him anymore," or, "We do not talk and she is no longer my friend." It is notable that nearly all of the people who violated one's privacy related to family-issues were given an explicit privacy rule (which was ignored). These transgressions led to terminated communication in each instance.

## 4. Discussion

This study highlighted boundary violations and turbulence in an online setting by investigating instances in which a person breached confidential info owned by another person on Facebook. We were able to address the research questions by identifying topics associated with a

privacy violation, perceived motivations for the violation, use of privacy rules, and reactions to the violation. Primarily, analysis revealed that the use of explicit privacy rules would have likely prevented many privacy violations and related boundary turbulence, though some confidentiality breaches are likely to occur in spite of explicit rules (Petronio & Reierson, 2009; see also Petronio, 2002).

The discrepancy breaches of privacy (see Petronio & Reierson, 2009) had a higher risk than the pre-emptive disclosure violation (see Petronio & Reierson, 2009), which were meant to be a secret forever. A discrepancy breach of privacy is risky to the original information owner and can result in a high level of vulnerability when others discover the information (Warren & Laslett, 1977). Although high-risk episodes or topics tend to be accompanied by a thicker privacy boundary with higher need for control (Petronio, 2002), people in the current study who revealed this confidential high-risk information (e.g., family issues, contact information, or death-related topics) were rarely given explicit privacy rules.

According to Petronio (2002), the five different types of risk are security, stigma, face, relational, and role. These particular risks describe what violators should take into consideration prior to the privacy violation. Based on the findings in this study, these risks were overlooked by the privacy violators, as individuals disclosed information without considering the original information owner's emotions, status, or well-being. This discovery, coupled with the finding that privacy rules are rarely discussed, underscores the importance of creating *explicit privacy rules* (see Petronio, 2002) and communicating those with any information co-owners. A possible relational script to create a privacy marker (i.e., shared privacy boundary) is simply to say, "this is not Facebook official," when communicating private information. This simple script may provide a practical means of making privacy expectations explicit to a confidant negating

possible disclosure missteps that result is an accidental disclosure. Although this script will not correct other disclosures of confidential information, accidental disclosures encompassed the majority of the violations in this study. Wang et al. (2011) found that accidental revelations still resulted in regret. Therefore, it is suggested that if the original information owner provides no privacy rules, the new co-owner of information should ask for a privacy rule or guidelines as to how the information should be protected.

Although (Petronio, 2002) recommended that people explicitly declare any privacy rules at the time of information dissemination, more than half of the participants in the present study did not provide the new shareholder with an explicitly stated privacy rule. Again, boundary turbulence often occurs because of boundary rule mistakes, usually made as the result of uncertainty (Petronio, 2007). So, if one neglects to clearly identify a privacy rule and provide that to the co-owner, who is truly at fault if the co-owner shares that information with others?

Managing privacy differs from person to person based on their unique interpretation of disclosure. No "typical" set of rules exists for each privacy disclosure; however, broadly speaking, communication needs to be clear so expectations do not go unmet, thus creating boundary turbulence. People often have norms regarding their expectations of privacy on Facebook, but many do not often follow the norms themselves when disclosing others' information. For example, numerous participants indicated that they did not provide their friends with privacy rules regarding the secret because they thought their friends would know better than to post the private information on Facebook (for discrepancy breaches of privacy). Others thought that their co-owners would know not to post anything on Facebook until the original owner him or herself made the news "Facebook official" (for pre-emptive disclosure violations). These indications reveal the use of implicit rules (Petronio, 1991), which are only alluded to by

the original information owner. The current study indicated that implicit rules were not enough to keep the co-owner from unintentionally sharing information meant to be kept private. Petronio (2002) posited that some privacy rules become habitual, creating patterned actions or *routinized rules*. The fact that violators did not "know better" reveals a lack of these routinized rules. It is apparent that we do not have agreed-upon norms for information disclosure online, signifying a need to explicitly declare privacy rules when sharing private information with others.

Further, the findings indicated that when people chose to utilize explicit privacy rules online, they did so because they realized Facebook users do not have a standard rule that everyone follows (i.e., Do not share something on Facebook that has not already been made "Facebook official" by the original information owner), even though many people believe such a norm exists. It appears that people do not acquire this rule through socialization when they join Facebook (or any other SNS for that matter), nor has this rule stabilized yet, ensuring consistent use (as described in Petronio, 2002). Moreover, though this implicit rule exists and is learned through SNS interactions, people choose to stifle breaches offline. When third party confidentiality breaches occurred, trust with the co-owner was compromised, and subsequently, participants report increasing the rigidity of boundaries (see Petronio, 2002) or terminating the relationship. As such, privacy breaches have lasting real implications for the participants' daily lived-experiences with others both online and FtF.

Trepte et al.'s (2014) longitudinal research indicated that users' negative experiences on SNSs do have an effect on informational privacy behaviors but did not have an effect on social (i.e., their general audiences) or psychological (i.e., kinds of information shared) privacy behaviors. That is, people adjusted the information posted online, but they did not modify their overall accessibility online. Participants in the current study did revisit, readjust, and renegotiate

their privacy rules and expectations in response to boundary turbulence, as forecasted by Petronio (2002) and reified in Trepte et al.'s (2014) research. This was evident in the responses to boundary turbulence as people attempted to resolve the issue. Much of the activity here focused on face-saving maneuvers (staving off face-risk, Petronio, 2002) such as quickly posting the announcement themselves, explaining themselves to friends and family, or detagging, deleting, or defriending on Facebook. While the use of privacy tools to protect one's privacy online is useful, Litt (2013) found that certain groups of people (based on demographic characteristics, motivation, and SNS experiences) are more prone to take advantage of SNSs' privacy tools. So, although people might intend to make necessary adjustments to protect their privacy, they might not have the knowledge of or experience with the SNS to properly use the available privacy tools.

In many cases, the transgression triggered an explicitly-stated rule, in line with Petronio (2002)'s discussion of privacy violations and sanctions. In other instances, people did not mention to their offending friend that a violation took place. One person remarked, "I didn't say anything about it to her [the violator]," which was echoed among other participants. Failing to confront an information co-owner following the privacy violation can perpetuate such violations. Perhaps norms regarding information sharing online do not exist because they simply are not being discussed before or after the violation.

Perhaps the largest influence on the privacy violations stem from the notion that Facebook is essentially public, although it can give the impression of being more private, which inherently points to Petronio's dialectic of privacy and disclosure. Thus, the online environment could be a significant factor leading to privacy violations and subsequent boundary turbulence. The online context may also affect privacy disclosures in other respects as well. For example,

because we might be worried about someone revealing private disclosures online before we get the chance to do it ourselves (even with explicit privacy rules), we might disclose information to people more quickly than we would prefer. This has implications for potential changes in long-standing social norms. Perhaps more pressing is the revelation that social norms are being translated across platforms and into an electronic format. Findings in the present study reveal preliminary information about the development (or lack of development) of social norms in a mediated context. Further research should continue to investigate this norm evolution.

Data was collected in early 2014, which might have some bearing on the outcomes. Acquisti et al.'s (2015) research indicates that users' publicly posted information is on the decline. This behavioral change might be a result of the high number of (unintended) privacy violations that occurred online and the subsequent re-assignment of privacy boundaries. If this is the case, people participating in public forums are regulating private information through the use of more rigid privacy boundaries (see Petronio, 2002). Petronio posits that our privacy boundaries shift throughout our lifespan, with adulthood having the most firm or rigid boundaries. It may be that as participation in SNSs increases, participants are engaging in more "adult" behaviors online, and subsequently restricting disclosure to others through decreasing the amount of disclosure in online public forums.

Future research should continue examining third-party disclosures of information and subsequent privacy management. Although a plethora of research has examined interpersonal self-disclosure through CPM, this study posits a unique contribution; namely, that *co-owners* of information violate the privacy needs of another by disclosing online. To this end, quantitative analysis of this topic would further advance CPM and aid in explanation and prediction of such behaviors. Although a reliable instrument for CPM has yet to be constructed, to advance this

theory, future researchers should employ Likert-type items to establish the *prevalence and severity* of third party privacy breaches online and the *re-construction of privacy norms*/interpersonal trust after a breach occurs.

## 5. Conclusion

This study focused on one online channel in which privacy violations can occur. While the information in this study cannot be generalized to other SNSs (such as Twitter or Instagram), using Harding's (1998) conceptualization of "movability," we can assume that similar violations take place on these various sites as well. Future research could help determine how other SNSs users manage confidentiality breaches. It would be useful to explore online privacy violations from both the violated persons' perspectives as well as the violators' perspectives. Moreover, it would be interesting to compare the privacy violations online to privacy violations offline. That is, do people view violations online as less or more offensive than violations offline and how these offenses impact trust (see Petronio & Reierson, 2009) with the other party. As discussed earlier, context collapse enhances rules violations, as friends of friends might see the information posted. Because we do not often know our Facebook friends' privacy settings, more people might know our information than we presume. Additionally, the warranting effect says people are more likely believe others' posts about us than our own posts about ourselves (Walther & Parks, 2002). Due to context collapse and warranting effect, online privacy violations might have a greater effect on regrets and boundary turbulence than offline privacy violations, as negative posts by others about a person can have a negative effect on one's social and physical attractiveness (Walther et al., 2008) at an exponential rate. Further, as Houghton and Joinson (2010) discovered, privacy violations can and do harm the offline relationship, likely because privacy violators are sometimes excluded from future communication (Petronio, 2002).

In summary, this study serves to help aid in understanding the types of privacy violations and confidentiality breaches that occur online as well as reactions to these violations. The research also further illustrates how principles of CPM operate in an online context, coupled with notions of context collapse, warranting, and online disinhibition.

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347,* 509-514. doi:10.1126/science.aaa1465

Afifi, T. D. (2003). "Feeling caught" in stepfamilies: Managing boundary turbulence through appropriate communication privacy rules. *Journal of Social & Personal Relationships, 20*(6), 729-755. doi:10.1177/0265407503206002

Allen, M., Walker, K. L., Coopman, S. J., & Hart, J. L. (2007). Workplace surveillance and managing privacy boundaries. *Management Communication Quarterly, 21*(2), 172-200. doi:10.1177/0893318907306033

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3,* 77-101. doi:10.1191/1478088706qp063oa

Child, J. T., Haridakis, P. M., & Petronio, S. (2012). Blogging privacy rule orientations, privacy management, and content deletion practices: The variability of online privacy management activity at different stages of social media use. *Computers in Human Behavior, 28*(5), 1859-1872. doi:10.1016/j.chb.2012.05.004

Child, J. T., Pearson, J. C., & Petronio, S. (2009). Blogging, communication, and privacy management: Development of the blogging privacy management measure. *Journal of the American Society for Information Science and Technology, 60,* 2079-2094. doi:10.1002/asi.v60:10

Child, J. T., & Starcher, S. C. (2016). Fuzzy Facebook privacy boundaries: Exploring mediated lurking, vague-booking, and Facebook privacy management. *Computers in Human Behavior, 54,* 483-490. doi:10.1016/j.chb.2015.08.035

Child, J. T., & Westermann, D. A. (2013). Let's be Facebook friends: Exploring parental

Facebook friend requests from a communication privacy management (CPM) perspective. *Journal of Family Communication, 13*(1), 46-59. doi:10.1080/15267431.2012.742089

Christofides, E., Muise, A., & Desmarais. (2009). Information disclosure and control on Facebook: Are they two sides of the same coin or two different processes? *CyberPsychology & Behavior, 12*(3), 341-345. doi:10.1089/cpb.s008.0226

Debatin, B., Lovejoy, J. P., Horn, A., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication, 15*(1), 83-108. doi:10.1111/j.1083-6101.2009.01494.x

Ellison, N. B., Vitak, J., Steinfeld, C., Gray, R., & Lampe, C. (2011). Negotiating privacy concerns and social capital needs in a social media environment. In S. Trepte & L. Reinecke (Eds.), *Privacy online: Perspectives on privacy and self-disclosure in the social web* (pp. 19-32). London, New York: Springer Heidelberg Dordrecht.

Facebook. (2017, January 3). Key Facts. Retrieved from newsroom.fb.com/company-info/

Glaser, B., & Strauss, A. (1967). *The discovery of grounded theory*. Chicago: Aldine.

Harding, S. (1998). *Is science multicultural?: Postcolonialisms, feminisms and epistemologies.* Bloomington: Indiana University Press.

Houghton, D. J., & Joinson, A. N. (2010). Privacy, social network sites, and social relations. *Journal of Technology in Human Services, 28*, 74-94. doi:10.1080/15228831003770775

Joinson, A. N., Houghton, D. J., Vasalou, A., & Marder, B. L. (2011). Digital crowding: Privacy, self-disclosure, and technology. In S. Trepte & L. Reinecke (Eds.), *Privacy online: Perspectives on privacy and self-disclosure in the social web* (pp. 33-45). London, New York: Springer Heidelberg Dordrecht. doi:10.1007/978-3-642-21521-6

Litt, E. (2013). Understanding social network site users' privacy tool use. *Computers in Human Behavior, 29,* 1649-1656. doi:dx.doi.org/10.1016/j.chb.2013.01.049

Lohr, S. (2010, March 16). How privacy vanishes online. *New York Times*. Retrieved from nytimes.com

Marwick, A. E., & boyd, d. (2010). I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society, 13*(1), 114-133. doi:10.1177/1461444810365313

Millham, M. H., & Atkin, D. (in press). Managing the virtual boundaries: Online social networks, disclosure, and privacy behaviors. *New Media & Society*. doi:10.1177/1461444816654465

Petronio, S. (1991). Communication boundary management: A theoretical model of managing disclosure of private information between marital couples. *Communication Theory, 1,* 311-335. doi:10.1111/j.1468-2885.1991.tb00023.x

Petronio, S. (2002). *Boundaries of privacy*: *Dialectics of disclosure*. Albany, NY: State University of New York Press.

Petronio, S. (2007). Translational research endeavors and the practices of communication privacy management. *Journal of Applied Communication Research, 35*(3), 218-222. doi:10.1080/00909880701422443

Petronio, S. (2013). Brief status report on communication privacy management theory. *Journal of Family Communication, 13*, 6-14. doi:10.1080/15267431.2013.743426

Petronio, S., & Bantz, C. (1991). Controlling the ramifications of disclosure: "Don't tell anybody but…." *Journal of Language and Social Psychology, 10*, 263-269. doi:10.1177/0261927X91104003

Petronio, S., & Kovach, S. (1997). Managing privacy boundaries: Health providers' perceptions of resident care in Scottish nursing home. *Journal of Applied Communication Research, 25*(2), 115-131. doi:10.1080/00909889709365470

Petronio, S., & Reierson, J. (2009). Regulating the privacy of confidentiality: Grasping the complexities through communication privacy management theory. In T. Afifi & W. A. Afifi (Eds.), *Uncertainty, information management, and disclosure decisions: Theories and applications* (pp. 365-383). New York, Routledge.

Solove, D. J. (2008). *Understanding privacy*. Cambridge, MA: Harvard University Press.

Suler, J. (2004). The online disinhibition effect. *CyberPsychology & Behavior, 7*(3), 321-326. doi:10.1089/1094931041291295

Trepte, S., Dienlin, T., & Reinecke, L. (2014). Risky behaviors. How online experiences influence privacy behaviors. In B. Stark, O. Quiring, & N. Jackob (Eds.), Von der Gutenberg-Galaxis zur Google-Galaxis. Alte und neue Grenzvermessungen nach 50 Jahren DGPuK (pp. 225-244). Konstanz, Germany: UVK.

Vitak, J. (2012). The impact of context collapse and privacy on social network site disclosures. *Journal of Broadcasting & Electronic Media, 56*(4), 451-470. doi:10.1080/08838151.2012.732140

Vitak, J., & Kim, J. (2014). "You can't block people offline": Examining how Facebook's affordances shape the disclosure process. In S. Fussell, W. Lutters, M. R. Morris, & M. Reddy (Eds.), *The 17th ACM conference* (pp. 461-474). doi:10.1145/2531602.2531672

Walther, J. B., & Parks, M. R. (2002). Cues filtered out, cues filtered in: Computer-mediated communication and relationships. In M. L. Knapp & J. A. Daly (Eds.), *Handbook of interpersonal communication* (3rd ed., pp. 529-563). Thousand Oaks, CA: Sage.

Walther, J. B., Van Der Heide, B., Hamel, L. M., & Shulman, H. (2009). Self-generated versus other-generated statements and impressions in computer-mediated communication: A test of warranting theory using Facebook. *Communication Research, 36*, 229-253. doi:10.1177/0093650208330251

Walther, J. B., Van Der Heide, B., Kim, S., Westerman, D., & Tong, S. T. (2008). The role of friends' behavior on evaluations of individuals' Facebook profiles: Are we known by the company we keep? *Human Communication Research, 34*, 28-49. doi:10.1111/j.1468-2958.2007.00312.x

Wang, Y., Norcie, G., Komanduri, S., Aquisti, A., Leon, P. G., & Cranor, L. F. (2011). "I regretted the minute I pressed share": A qualitative study of regrets on Facebook. *Proceedings of the Seventh Symposium on Usable Privacy and Security, 10*. doi:10.1145/2078827.2078841

Warren, C., & Laslett, B. (1977). Privacy and secrecy: A conceptual comparison. *Journal of Social Issues, 33*(3), 43-51. doi:10.1111/j.1540-4560.1977.tb01881.x

Waters, S., & Ackerman, J. (2011). Exploring privacy management on Facebook: Motivations and perceived consequences of voluntary disclosure. *Journal of Computer-Mediated Communication, 17*, 101-115. doi:10.1111/j.1083-6101.2011.01559.x