RESPONSES TO PRIVACY TURBULENCE: THE IMPACT OF PERSONALITY TRAITS ON RECALIBRATION AND PRIVACY BOUNDARIES ON FACEBOOK

A Thesis
Submitted to the Graduate Faculty
of the
North Dakota State University
of Agriculture and Applied Science

By

Valerie Joy Fechner

In Partial Fulfillment of the Requirements
for the Degree of
MASTER OF SCIENCE

Major Program:
Communication

June 2016

Fargo, North Dakota

North Dakota State University
Graduate School

Title

RESPONSES TO PRIVACY TURBULENCE: THE IMPACT OF PERSONALITY TRAITS ON RECALIBRATION AND PRIVACY BOUNDARIES ON FACEBOOK

By

Valerie Joy Fechner

The Supervisory Committee certifies that this ***disquisition*** complies with North Dakota State University's regulations and meets the accepted standards for the degree of

MASTER OF SCIENCE

SUPERVISORY COMMITTEE:

Dr. David Westerman
Chair

Dr. Ann Burnett

Dr. Andrew Mara

Approved:

06/22/2016
Date

Dr. Mark Meister
Department Chair

ABSTRACT

As individuals use social media to create and maintain relationships and connections, they must also decide how to manage the private information that they disclose to their connections. If private information is handled improperly online, it may evoke varying responses that affect previously held privacy boundaries. Using communication privacy management theory (Petronio, 2002) as a framework, this study seeks to understand how the severity of a privacy violation impacts the Facebook users respond to online privacy turbulence. It also investigates how personality characteristics influence these responses. Results reveal that more severe privacy violations are met with more discussion of the privacy violation and thicker privacy boundaries both between the owner and the violator and between the owner and their social media network. Findings also imply that some of the Big Five personality traits impact the relationship between severity and the outcome variables.

ACKNOWLEDGEMENTS

I would like to thank everyone who has helped me achieve this great accomplishment during the past two short years. First, I would like to thank my advisor, Dr. David Westerman, for all his help, guidance, knowledge, and feedback throughout this process. It has been great working with you and I would never have gotten this far without you. Thank you also to my committee members, Dr. Ann Burnett and Dr. Andrew Mara, for their feedback and insight during my proposal and final defense (and thank you for letting me pass).

I would also like to thank the NDSU department of communication for giving me an education I am proud of and teaching me so much about the study of communication. In these two short years I have learned so much about the communication field and have developed as a researcher and as a scholar. Thank you to all the professors that have invested their time and energy into my education. Specifically, I want to thank Dr. Stephenson Beck, Dr. Carrie Anne Platt, Dr. Zoltan Majdik, Dr. David Westerman, and Dr. Ann Burnett. You have all helped me think until my head hurts and achieve more than I ever thought possible.

Thank you to my parents and family for supporting me through this process. Thank you also to my fellow NDSU masters and doctoral students: Emily, Jen, Bethany, Kelli, Amanda, Bryce, Whitney, Katie, Kelsey, and many others. Thank you all for being my friends, resources, teachers, and supports during my journey at NDSU. I have learned so much from each of you and look forward to seeing where life takes us all.

TABLE OF CONTENTS

LIST OF TABLES

INTRODUCTION

In 2012, a Belgian trade group released a video to the Internet that featured Dave, a gifted mind reader (Knowles, 2012). In the video, participants are randomly selected from the streets of Brussels and asked to participate in an upcoming TV program. If they agree, they are ushered into a tent to meet Dave the Psychic. During the psychic readings, the participants listen in awe as Dave reveals seemingly random facts about the participants ranging from general to very specific and personal. What the participants do not know is that the source of Dave's psychic abilities is not supernatural, but come from one place: the Internet. All of the information revealed by the psychic is found online in just the time that the participant is in the room. Though the video was created as a Public Service Announcement to warn Internet users of hackers that can easily find and abuse private information, it reveals something deeper about how the Internet is being used. None of the participants seemed to realize that this information was public knowledge. They were entirely surprised that a complete stranger could know such intimate details of their lives. The Internet has become so infused with everyday life that users are forgetting that their activity is public and permanent.

Most individuals use the Internet daily for communicating with friends and family, getting news updates, online banking and shopping, and even making new friends. Over half of all teens have made new friends online and communicate with existing friends through text messaging and other mediated forms of communication (Lenhart, 2015). As individuals use the Internet to create and maintain relationships and connections (Craig & Wright, 2012), they must also decide how to handle the private information that they disclose to these connections. Notably, there may be information that is especially difficult to manage. Pew Research found that 42% of teens say that they have had someone post something about them online that they

cannot control or change (Lenhart, 2015). Furthermore, about one quarter (27%) of teens reported experiencing conflict over something that happened online or through text messaging (Lenhart, 2015). This inability to regulate personal content could lead to undesired private information being shared to large audiences. Private information is viewed as public territory for some, and this can cause conflicts for users' relationships and their networks.

One reason for these conflicts occurs from overlooking the public nature of the information online. Research finds that social media users grossly underestimate the size of their audiences (Bernstein, Bakshy, Burke, & Karrer, 2013). When comparing the actual number of content viewers to the believed number of content viewers, the user's estimation was only 27% of the actual audience size. This demonstrates how blind Internet users are to the sizeable network that has access to their posts. Social networks also merge many different audiences and identities, a concept known as context collapse (boyd, 2007). It can be difficult to decide which information is appropriate to disclose to a whole network (Vitak, 2012). This overlap of audiences can cause conflict if the diverse audience is not considered when posting information.

When users share information on the Internet, they make decisions regarding which information to make public and which information they should keep private (Bazarova, 2012; Child, & Agyeman-Budu, 2010; Debatin, Lovejoy, Horn, & Hughes, 2009). These decisions create privacy boundaries that govern how and to whom private information is disclosed. Owners may decide to reveal the information to others, creating co-owners of the information (Petronio, 2013). The owner and co-owners set up rules around the information that control who has access to the information and what behavior is appropriate. If individuals act outside the previously established privacy rules and reveal something to others or to the whole online network that was meant only for one or two people, privacy turbulence may occur (Child, Petronio, Agyeman-

Budu, & Westermann, 2011). Privacy turbulence can change the owner's future privacy decisions and may have implications for both the online network and the relationship with the individual who caused the turbulence. Privacy turbulence has long been an issue in interpersonal relationships (Petronio, 2002), but the permanence of the Internet adds a new dimension. Mediated conversations do not have the same ephemeral comfort that face-to-face conversations have. This permanence can cause various network and relational issues like de-contextualization of content and increase the likelihood of privacy turbulence.

Using communication privacy management theory (Petronio, 2002) as a framework, this study seeks to understand how Facebook users respond to privacy turbulence online and the factors that impact these responses. Several contributions to online privacy management research result from this study. First, it provides deeper insight into how privacy is managed online, both in interpersonal relationships and between users and their online network. Second, it investigates how users respond to privacy turbulence online. Finally, it investigates how the big 5 personality characteristics (extraversion, agreeableness, conscientiousness, neuroticism, and openness) impact reactions and outcomes of privacy turbulent episodes on Facebook.

LITERATURE REVIEW

Online Privacy Management

As the Internet and technology continue to permeate social life, it is important to understand how individuals manage their private information online. Private information is frequently shared online through social networking sites. Social networking sites, such as Facebook, Twitter, and Instagram are virtual places where individuals portray their identities through the creation of a personal profile. Given the permanence of Internet content, it is valuable to understand the implications of publicly disclosing private information online. Social media users do not always acknowledge how fundamental this way of communicating is to their social lives because it is so deeply engrained into everyday communication (Debatin et al, 2009). The integration of social media into social life adds more potential issues for privacy management as content is permanent and can be viewed by many and taken out of context.

Internet privacy complicates the privacy dynamic by bringing together concerns for privacy boundaries in relationships as well as privacy of information shared to a larger network. Thus, users have to manage privacy rules for both individual relationships and their network. Balancing concerns for certain individuals and the larger network is unique to public Internet platforms. O'Sullivan (2005) refers to this appeal to both individual and group levels as masspersonal communication. Masspersonal communication brings together aspects of both interpersonal and mass communication and recognizes that channels traditionally used for mass communication (message from one to many) are used for interpersonal communication (messages from one to one), and vice versa (O'Sullivan, 2005). For example, a newspaper, which is traditionally thought to be a message from one to many also includes interpersonal elements such as the "Happy Birthday" section or personal ads. Similarly, social media is a

masspersonal medium in that one can write a post for a specific person, but his or her whole network also has access to the message if it is posted in a public space, such as a Facebook wall. This overlap of private/public space can present privacy management concerns. Much of the research surrounding social media privacy concerns network privacy, which involves the privacy settings that determine what information is revealed and concealed to the network rather than on individual relationships. Nevertheless, because it is a masspersonal medium, privacy management occurs on both network and individual levels.

Social media profile privacy settings determine who can and cannot see the information that is posted on a certain page. This is one way of managing online privacy. However, not all users take advantage of these settings. Debatin et al (2009) found that although Facebook users may understand the dangers of posting personal information to their pages, they still desire to include private information in their profiles. These findings suggest that users prefer the benefits of revealing private information, such as accessibility or personal boasting, rather than ensuring privacy safety. One reason for this imbalance could be that using specific privacy settings on Facebook requires a greater investment of time and knowledge (Vitak, 2012). Another reason is that a third person effect occurs in which individuals do not anticipate privacy violations happening to them, even if they have heard of it happening to others (Debatin et al., 2009). Though privacy concerns are present when disclosing information, they may not always be a large contributing factor in the decision to create social media accounts (Acquisti & Gross, 2006). Additionally, individuals who participate in social networking sites may demonstrate higher risk taking attitudes than those without social networking profiles (Fogel & Nemad, 2009). These risk taking attitudes may result in more relaxed privacy settings, leaving them open for privacy violations.

Additionally, concern for privacy can affect how much information a user discloses on social media. Stutzman, Capra, and Thompson (2010) found that individuals who customized their profile privacy settings on Facebook were 2.5 times more likely to disclose information. Additionally, most users disclose information online in order to share information with others as well as to keep up with trends and to show off (Waters & Ackerman, 2011). Some users are aware of the public nature of the Internet and manage their privacy accordingly. Other research suggests that the more users are concerned about privacy, the less they will disclose on Facebook (Stutzman et al., 2010: Vitak, 2012). If users even so much as anticipate that their privacy boundaries will be violated online, they are less likely to share information about themselves (Hesse & Rauscher, 2013). One study found that Facebook users concerned with online lurking or anonymous surveillance on Facebook posted more vague information and used more privacy management than those who were not concerned with lurking (Child & Starcher, 2016). However, Taddicken (2014) found that privacy concern did not impact self-disclosure as much as willingness to disclose. These conflicting findings suggest that several factors may influence disclosure, rather than just privacy concerns.

Communication Privacy Management Theory

The process of revealing and concealing information is a dialectic that many individuals and relationships experience and is at the core of privacy management (Petronio, 2010; Petronio & Durham, 2015). One theory that is particularly useful in explaining how personal information is managed is communication privacy management theory (CPM; Petronio, 2002). This theory seeks to explain why we keep or do not keep information private, how we decide to whom the information is revealed, and what happens when the information is handled improperly. The theory is made up of three elements: privacy ownership, privacy control, and privacy turbulence

(Petronio, 2013). These three elements form a cyclical model in which each of the individual components influence the next. During privacy ownership, individuals decide what information they deem appropriate to disclose to others and what information should be kept secret. This process leads to deciding who should have access to the information, or privacy control. In this stage, the owners of the information set up rules with the co-owners around the shared information. If these rules are broken, it leads to a breakdown of privacy, or privacy turbulence. At this stage, the privacy rules are re-evaluated, leading back to the initial decision of privacy ownership. CPM and the three elements have been explored, tested, and applied in a variety of communication contexts.

Privacy ownership. The first component of CPM, privacy ownership, happens when individuals mark information as private by defining the boundaries surrounding the information (Petronio, 2013). Privacy ownership relies on two assumptions or axioms. First, individuals believe that they are the primary owner of their information and they have the right to reveal or keep secret that information (Petronio, 2013; 2015). Second, the owner of the information may choose to share the information with one or more individuals, making them "co-owners" of the information. When sharing private information with co-owners, mutual boundaries are created that mark appropriate behaviors surrounding that information. Thus, the first component of the CPM process is that individuals assume ownership of their information and may choose to share it with outside individuals or co-owners, which creates boundaries.

Privacy control. Not only do individuals decide which information is private or public, but they also decide how and to whom it is disclosed. This second element of CPM, known as privacy control, involves how individuals control the boundaries of their private information. Petronio (2013) outlines several core assumptions concerning privacy control. The first is that

privacy control functions on the basis that individuals have a perceived right to control their private information through the use of privacy rules (Petronio, 2013). Privacy rules develop as a result of two types of broader criteria known as core criteria and catalyst criteria (Petronio, 2013).

Core criteria. Each individual develops common ways through which private information is generally managed. Core criteria refer to the consistent or stable ways in which people manage privacy (Petronio, 2013). Core privacy preferences stem from underlying criteria such as gender, culture, family, and privacy orientations (Petronio & Durham, 2015). These criteria are shaped through societal values and socialization. One factor that may influence core criteria is personality. For example, self-disclosure is affected by willingness to disclose information, which is sometimes determined by personality (Taddicken, 2014).

Catalyst criteria. There will be times when an individual manages privacy in a way that differs from his or her core criteria, called catalyst criteria. Catalyst criteria are triggers that change previously established privacy rules because of some abnormal event or behavior. Catalysts may include liking and attraction, relational breakdowns or other unique situations, or a fluctuation of the risk-benefit ratio (Petronio, 2002; 2013; Petronio & Durham, 2015).

Both core and catalyst criteria are used to shape privacy rules surrounding private information. After rules are established, they are managed between the owner and co-owner. Thus, another assumption of privacy control predicts that control is successful through the coordination and negotiation of privacy boundaries with co-owners (Petronio, 2013). Privacy rules can be communicated either explicitly or implicitly (Venetis, Greene, Magsamen-Conrad, Banerjee, Checton & Bagdasarov, 2012). For example, if the information is health related, owners are more likely to communicate explicit rather than implicit rules to the co-owner, which

suggests that sensitivity of information could influence coordination and negotiation of privacy rules (Venetis et al., 2012). Furthermore, Kennedy-Lightsy, Martin, Thompson, Himes and Clingerman (2012) found that those who disclose risky information engage in more boundary coordination than those who disclose less risky information. If rules are not coordinated and negotiated properly, privacy may not be successfully managed.

The last two assumptions of privacy control involve collective privacy boundaries. Individuals may choose to disclose the same information to more than one person, creating multiple co-owners. The first assumption concerning collective privacy boundaries predicts that co-ownership results in jointly held and operated collective privacy boundaries in which all members may contribute to the private information. For example, the family unit exhibits collective boundaries through regulation of private information from outsiders (Petronio, 2010). A family includes several members that reveal private information to each other simultaneously and therefore need collective privacy boundaries to maintain the information within the family unit.

The last assumption suggests that, "collective privacy boundaries are regulated through decisions about who else may become privy, how much others inside and outside the collective boundary may know, and rights to disclose the information" (Petronio, 2013, p. 11). These decisions represent three types of rules: boundary linkage rules, permeability rules, and ownership rules. Individuals consider outsiders, or boundary linkages, when forming boundary alliances (Petronio, 2002; 2010). Owners and co-owners must determine whether or not they are able to share the information with outsiders and how much information they are able to share. A person has varying responsibility, or linkage, to the information depending on their connection to the information. For example, the family unit develops certain boundary linkage rules when

determining what information to keep private as a family and what to disclose to outsiders (Petronio, 2010). Next, permeability rules define how much information the owner reveals to the co-owner, or the level of access the co-owner has to the information. These rules can range from complete openness to disclosing very minimum detail about the information (Petronio, 2010).

The owner determines rules concerning how responsible the co-owners are for the private information. If privacy rules are not clear between the owner and co-owner, it is possible that the co-owner will not assume the desired responsibility of the private information (Petronio & Durham, 2015; Venetis et al., 2012). Whether rules are implicit or explicit can impact the perceived responsibility of privacy rules. If a co-owner perceives rules surrounding the information, whether implicit or explicit, the information is less likely to be shared (Venetis et al., 2012). Likewise, if there are no rules perceived by the co-owner surrounding the private information, it is more likely to be shared. Thus, communicating ownership rules is very important in establishing co-owner responsibility to the information. Taken together, these three rules are used to guide the collective boundaries set up between the owner and co-owner(s). The criteria used to control the sharing of information, how much information is shared, and how co-owners' behavior is managed regarding the private information make up the element of privacy control.

Privacy turbulence. Though owners set up rules and negotiate boundaries with co-owners to protect themselves and their information, the established boundaries can be violated, resulting in privacy turbulence. A privacy violation can be difficult to predict, and violations can range from simple disruptions in privacy boundaries to complete breakdowns of established rules (Petronio, 2013; 2015). Generally, the occurrence of privacy turbulence is a signal that there is a needed change in the individuals' privacy management system (Petronio, 2013).

Petronio (2002) outlines six factors leading to privacy turbulence. These factors are: intentional rule violations, boundary rule mistakes, fuzzy boundaries, dissimilar boundary orientations, boundary definition predicaments, and privacy dilemmas. Given the myriad of factors leading to privacy turbulence, some of these factors have not been studied in depth individually. However, it is possible that they do not occur in isolation, but rather simultaneously. Each factor's definition and explanation further illustrates this simultaneous nature.

Intentional rule violations occur when a co-owner of private information purposely does not follow the established privacy rules and boundaries set in place. Examples of intentional rule violations include betrayal, spying, or a dilemma of confidentiality (Petronio, 2002). These involve intentional acts of going against privacy rules and exemplify a specific point in time when the rules were disrespected.

Boundary rule mistakes occur non-intentionally and involve the application of boundary rules that differ from the owner's intended boundary rules. Examples of this include errors of judgment, timing, and topic rules (Petronio, 2002). An error of judgment may occur if the co-owner makes a decision regarding the information that would not be supported by the owner. Timing mistakes could occur if the co-owner shares information at an earlier, later, or otherwise inappropriate time than the owner wishes. Topic rule violations occur if a co-owner is under the impression that a certain topic can be discussed within a context different from that which the owner deems appropriate.

Turbulence can also occur as a result of fuzzy privacy boundaries. A fuzzy boundary is ambiguity about the ownership of information. Petronio (2002) writes, "Turbulence arises when others see the same information as collectively owned and managed according to mutually

established rules" (190). Deception and gossip are examples of fuzzy boundaries. Information could be deceptive if the owner withholds information from another when the information is perceived by the other to be owned collectively. Gossip exemplifies how fuzzy boundaries can result in a wide range of co-owners under the belief that the information is collectively owned. For example, Child and Starcher (2016) investigate fuzzy boundaries on the social network Facebook. Boundaries are fuzzy because the owner is unable to determine who can and cannot see the revealed information. One way individuals manage fuzzy boundaries is through "vague-booking" or posting strategically ambiguous information (Child & Starcher, 2016). This helps the individual protect him or herself from having specific private information disseminated to a large audience.

Turbulence resulting from dissimilar boundary orientations occurs when individuals have differing core criteria for privacy management. The fundamental ways individuals decide what is private and public differ, causing turbulence. Boundary definition predicaments happen in two different ways: first, when public space is treated as private space and inappropriate information is disclosed. For example, if a parent chooses to discipline his or her child in a public place such as a grocery store, it may cause privacy turbulence in that the act of discipline may reveal childrearing practices that the parent wants to keep private (Petronio, 2010). Second, when an individual is pushed into a public domain, he or she is forced to redefine privacy boundaries. An example of this could be if an individual's private information is accidentally shared to a large group of people, and instead of covering up the mishap, the individual shifts privacy boundaries to include the information.

The last factor that Petronio (2002) suggests can cause privacy turbulence is a privacy dilemma. This factor demonstrates the complicated nature of privacy management. Privacy

dilemmas occur when an individual knows confidential information and the revelation or concealment of the information could lead to a breakdown of friendship, trust, or future sharing of private information.

As demonstrated, several factors may lead to privacy turbulence. It is likely that some of these factors happen simultaneously and are not separate experiences. For example, a person could experience dissimilar privacy orientation and boundary rule mistakes as part of one violation. A boundary rule mistake, if made public, could demonstrate dissimilar privacy orientation. Privacy turbulence identifies what types of factors instigate boundary breakdowns. The three elements of CPM work together to create a triangular model in which rules are formed, managed, broken, and readjusted, leading back to a reassessment of privacy ownership.

CPM online. Some research has applied communication privacy management theory to the online context. Though CPM was originally created with the offline context in mind, the theory has gained relevance in the online context with the emergence of online privacy concerns. Two areas of research regarding CPM online are family communication and blogging.

The family unit is one area where privacy research is applied. Some research investigates how parent-child privacy preferences are negotiated online. Ledbetter et al. (2010) compared privacy turbulence between parents and young adult children both at home and away from college. Children reported fewer overall privacy invasions by their parents away at college than at home, and an equal amount of privacy invasion by mobile phone at home and away at college (Ledbetter et al., 2010). Additionally, if children are friends with their parents on Facebook, it is not necessarily seen as a privacy invasion, but rather can help lessen conflict between the dyad (Kanter, Afifi, & Robbins, 2012). Child and Westermann (2013) found that parent friend requests to young adult children do not present a privacy dilemma for the young adult and they

do not change their privacy settings extensively upon receiving a friend request from a parent. This research suggests that publicly displaying family relationships online is not, in fact, as much of a privacy violation as one may assume.

Blogging behavior is another area of research applying CPM to the online context. Child and Agyeman-Budu (2010) found that bloggers with high self-monitoring skills were more private in their privacy management practices than those with low self-monitoring skills. They also interacted in a way that protected their individual ownership rights of the information they disclosed. This suggests that high self-monitoring bloggers use collective boundary rules to control the balance between private and public disclosures. Child and Agyeman-Budu also found that high self-monitors blog more frequently than low self-monitors. A blogger may also choose to alter or adapt privacy rules if their posts do not accomplish desired outcomes (Child et al., 2011). Several motives that determine if a user decides to delete, or scrub, content from blog posts include conflict management, protection of personal identity, impression management, and emotional regulation (Child et al.). This literature demonstrates the presence of privacy ownership and privacy rules in online settings.

Responses to privacy turbulence. Following privacy turbulence, an individual may reassess privacy rules or manage privacy differently. These reassessments range from directly confronting the violator to avoiding confrontation and making less permeable privacy boundaries so as to protect themselves from future violations (Steuber & McLaren, 2015). Individuals respond to privacy turbulence in a variety of ways that have both positive and negative implications for the owner and co-owner relationship. For example, emotional responses to privacy turbulence can have consequences for the relationship. The most common emotional responses are hurt, anger, and fear (McLaren & Steuber, 2013). When individuals respond to

privacy turbulence with negative emotions, like anger and distancing behaviors, there is more relational damage (McLaren & Steuber). Hesse and Rauscher (2013) go as far as asserting that privacy management overall is an emotional decision. Additionally, most individuals blame the co-owner for privacy turbulence rather than themselves (Steuber & McLaren).

Responses to privacy turbulence can also be positive (Child et al., 2012; McLaren & Steuber, 2015). Positive outcomes result when the owner is able to successfully confront the violator and recalibrate boundary rules (Steuber & McLaren, 2015). Recalibrating rules with the violator on any level is associated with more forgiveness and relational improvement than no recalibration (Steuber & McLaren, 2015). Thus, talking with the violator about the violation and established privacy rules can be helpful for the owner/co-owner relationship.

Online Privacy Boundary Recalibration and Outcomes

As previously demonstrated, CPM theory is a useful framework in the exploration of online privacy management practices. Less research has focused specifically on how Internet users respond to privacy turbulence. Child et al. (2011) found that scrubbing, or deleting content, is a common response to privacy turbulence for bloggers, but these results have yet to be extended to other online contexts such as social media profiles. Some research has focused on the overlap of the public/private nature of social media. For instance, information is perceived as more or less appropriate whether it is shared privately or publicly online (Bazarova, 2012). Specifically, intimate information shared publicly is perceived as less appropriate than intimate information shared privately (Bazarova, 2012). Social media also combines several different audiences and individuals perform different identities depending on the audience (Hogan, 2010). It is likely that social networking sites will reveal new insights into how individuals respond to

privacy turbulence because they blur the lines between public and private and incorporate many audiences (boyd, 2008; Vitak, 2012),

CPM contends that privacy turbulence can range from small disruptions in privacy rules to extreme privacy boundary breakdowns (Petronio, 2013). The severity of the turbulence is subject to the perception of the owner. If turbulence is more severe, the owner may take more severe ramifications. Therefore, the relational and network outcomes of the privacy turbulence may depend on its severity. Furthermore, the severity of the violation may determine how the owner chooses to recalibrate following the turbulence. Privacy recalibration refers to the active process of discussing the privacy violation with the violator. Since any amount of recalibration following privacy turbulence is associated with higher relational improvement and forgiveness in face-to-face contexts (Steuber & McLaren, 2015), it is possible that online privacy violations will also be recalibrated face-to-face. Owners set up rules around private information (Petronio, 2002; 2013), and it is possible that owners may choose to recalibrate privately face-to-face, between the owner and co-owner(s), or publicly face-to-face, where others have access to the conversation depending on the severity of the violation. Research has yet to consider the severity of the violation in face-to-face recalibration choices following privacy turbulence. Thus, two research questions address these issues.

RQ1: Is privacy turbulence severity associated with public face-to-face recalibration?

RQ2: Is privacy turbulence severity associated with private face-to-face recalibration?

If the violation occurs online, owners may also choose to discuss the event with the violator through a mediated context such as social media or text message. Communicating through social media is ingrained into everyday interaction (Debatin et al, 2009), so discussing the violation online likely happens after privacy turbulence. Since more private information is

perceived as less appropriate to share online (Bazarova, 2012), owners may also choose to discuss the violation through a private medium, such as a direct message on Facebook, or a text message. However, previous research suggests that users do not always consider the publicity of their content (Aquisti & Gross, 2006; Debatin et al., 2009), so they may recalibrate publicly online as well through a tagged status or a wall post. The amount of recalibration individuals engage in online publicly or privately may depend on the severity of the turbulence. Thus, two research questions address these issues.

RQ3: Is privacy turbulence severity associated with public mediated recalibration?

RQ4: Is privacy turbulence severity associated with private mediated recalibration?

CPM asserts that individuals adjust their privacy boundaries following privacy turbulence (Petronio, 2013). Outcomes resulting from privacy violations may include adjusting both relational privacy boundaries and network privacy boundaries. Relational privacy boundaries refer to privacy boundaries between the owner and co-owner(s) of the information. Network privacy boundaries refer to both the privacy settings in place on the social media profile that determine which individuals can or cannot see certain information, as well as how much the violator chooses to share with his or her network. Considering that social media is a masspersonal medium and includes relationships between individuals and a relationship to a networked audience, it is possible that individuals will readjustment privacy boundaries with the individual who caused the privacy turbulence as well as the network to which it was revealed.

Child et al. (2011) found that bloggers adjust, amend, change, or scrub privacy rules if they are not fulfilling desired outcomes such as impression management, identity safety or if they perceive privacy risks. This is likely the case on social media as well since individuals perform impression management through the creation of online profiles (Rosenberg & Egbert,

2011). Research suggests that personal experience determines change in privacy boundaries rather than simply knowing that something could happen (Debatin et al., 2009), suggesting that experiencing privacy violations would lead to thicker privacy boundaries. Privacy boundary thickness and thinness refers to how much is disclosed or shared with other individuals or the network, or the permeability of privacy boundaries. Hypothesis one predicts a relationship between the severity of privacy turbulence and network privacy boundary thickness.

H1: Privacy turbulence severity is positively associated with network privacy boundary thickness.

In addition to shifting network privacy boundaries, individuals may shift relational privacy boundaries following privacy turbulence. McLaren and Steuber (2013) found that privacy turbulence is either helpful or harmful for relationships and can bring people closer together or create more relational distance. Integrative communication about privacy turbulence is associated with relational improvement, while anger and distributive responses are associated with more relational distance (McLaren & Steuber). Steuber and McLaren (2015) found that individuals who experience privacy turbulence often choose not to share the same information with the violator in the future. Taken together, this research suggests that individuals adjust boundaries to be thicker or thinner, but said research does not take into account the severity of the violation. Thus, hypothesis 2 predicts a relationship between severity and relational privacy boundary thickness, but does not specify the direction of the relationship.

H2: There is a relationship between severity of privacy turbulence and relational privacy boundary thickness.

CPM and Personality

The effects of personality characteristics on communication processes have been explored, specifically in the area of communication privacy management (Bello, Brandau-Brown, & Ragsdale, 2014; Steuber & McLaren, 2015; Taddicken, 2014). Taddicken (2014) found that willingness to disclose predicted more self-disclosure on Facebook. Another study suggests that those who felt more effective confronting the violator recalibrated more than those with lower confrontation efficacy (Steuber & McLaren, 2015). Furthermore, Bello et al. (2014) tested personality traits in predicting secret revelation. Specifically, the tendency to gossip was associated with likelihood to disclose a secret (Bello at al., 2014). Steuber and McLaren (2015) assert that future research should focus on individual features that contribute to effective boundary coordination and boundary recalibration. This study tests the big 5 personality traits (extraversion, agreeableness, conscientiousness, neuroticism, and openness) as moderators between severity of privacy turbulence and outcomes. These psychological factors may reveal some important implications for how individuals communicate following privacy turbulence and are important to consider.

Goldberg (1981) first developed a five-factor representation of personality as a general comprehensive framework for understanding personality in the English language. McRae and John (1999) provide several adjectives explaining each of the big five personality (BFI) traits. Extraversion is explained as active, assertive, energetic, enthusiastic, outgoing, and talkative. Agreeableness is characterized as appreciative, forgiving, generous, kind, sympathetic, trusting. Conscientiousness is described as efficient, organized, planful, reliable, responsible, and thorough. Neuroticism is explained as anxious, self-pitying, tense, unstable, and worrying.

Openness is described as artistic, curious, imaginative, insightful, original, and having wide interests.

The big five personality traits have been used to predict social life outcomes such as performance in school and juvenile delinquency (Pervin & John, 1999). The BFI personality traits are also useful in determining individual emotional style differences (Pervin & John, 1999). Hesse and Rauscher (2013) suggest that privacy management is an emotional decision, and some research has studied emotional responses to privacy turbulence (McLaren & Steuber, 2013; Steuber & McLaren, 2015). Since the big 5 personality traits apply to emotional styles, and privacy management involves emotion, the big 5 may help inform communication privacy management decisions. One study applied the big 5 to private disclosure on Twitter (Jin, 2013), which found a negative relationship between extraversion and the social psychological processes of self-guarded disclosure and relational privacy preference. Another study used the BFI traits to investigate Facebook activity and privacy concerns (Sumner, Byers, & Shearing, 2011) and found that individuals with higher extraversion and agreeableness were less concerned over online privacy issues. Additionally, individuals with higher neuroticism were more concerned with online privacy issues (Sumner et al.). Jin and Sumner, et al. provide evidence suggesting that personality characteristics do impact privacy management behavior. Other previous research asserts that personality characteristics may influence privacy management and are worthy of future study (Bello et al, 2014; Child et al., 2011; Steuber & McLaren, 2015; Taddicken, 2014). Thus, it is likely that the big five personality traits will be useful in predicting individuals' responses to privacy turbulence.

Privacy turbulence might result in a re-coordination of privacy boundaries for the individual or the network. Specifically, an individual may create thicker or thinner privacy

boundaries for the network and/or relationship. For example, Hesse and Rauscher (2013) found that anticipated privacy turbulence and disclosure were moderated by a lack of words for emotions, or alexithymia. Thus, personal characteristics included in the big 5 may have an influence on the relationship between severity of violation and privacy recalibration and relational and network boundary thickness.

RQ5: How do the BFI personality traits moderate the relationship between severity and a) private FtF recalibration, b) public FtF recalibration c) public online recalibration, d) private online recalibration e) relational privacy boundary thickness, f) network privacy boundary thickness?

METHOD

Participants

Participants (N = 391) were recruited through an introductory communication course and a university wide research pool, both at a large Midwestern university. Students in the communication course were offered five points of course credit in exchange for their participation in the study. Whether or not a student chose to participate in the survey had no effect on their final grade and students were offered an alternate assignment if they did not choose to participate. In order to gain credit for taking the survey, students printed a "thank you" page that indicated their completion of the survey. Participants who were part of the university research pool did not receive any compensation for their participation.

Participants had to be at least 18 years of age and identify as an active Facebook user. According to Facebook (2016), an individual is classified as an active user if they have logged in to navigate the website in the 30 days prior to the day they participate in the study. If an individual failed to meet either of these criteria, he or she was disqualified and directed out of the study. In total, 548 individuals participated in the study. Of those 548, 27 did not meet the inclusion criteria, 9 did not answer any of the survey questions, and an additional 121 respondants were excluded because they did not answer the inclusion criteria questions or if they did, they only answered a few of the survey questions. This left 391 responses for the final analysis.

The final sample was comprised of individuals between the ages of 18 and 63, with 90% of participants between the ages of 18 and 25 (M = 21.24, SD = 6.24). Adults between the ages of 18 and 29 are reportedly the age group with the highest Facebook usage (Duggan, 2015), so this participant pool is representative of the average Facebook user. The sample was 45.3% male

and 47% female. 84% were White, 2.6% were Asian, 2% African American, 1% Hispanic/Latino, .8% American Indian or Native Alaskan, 1.5% mixed and .8% other. The first five categories are the most accurate, up to date race categories used by the US Census Bureau (2013). The mixed and other options are included to encompass all race possiblities.

In addition to age, sex, and race, the demographic information measured Facebook usage. The Facebook intensity scale (FBI) developed by Ellison, Steinfeld, and Lampe (2007) was used to measure how much participants use Facebook. The eight item scale includes statements regarding Facebook habits and usage (e.g. Facebook is part of my everyday activity, or I feel out of touch when I haven't logged into Facebook for a while, etc.). Items 1-6 are rated on a Likert-type scale ranging from 1-5, with 1 being strongly disagree to 5 being strongly agree. Items 7 and 8 are open ended items that ask participants to report how many Facebook friends they have and on average how much time they have spent logged onto Facebook each day in the past week. An overall Facebook use intensity score results from the mean of the items with a higher mean indicating higher intensity of use ($M = 3.1$, $SD = .98$). Participants reported spending anywhere from 1 to 480 minutes per day using Facebook ($M = 55.02$, $SD = 62.34$) and have anywhere from 5-2600 friends ($M = 526.53$, $SD = 383.36$).

Procedures

A questionnaire was used to gather data in order to capture individual responses and reactions to an episode of privacy turbulence experienced on Facebook. The social media site Facebook was used as the context for this study because it is reported to be the most widely used among adults with 71% of adults using Facebook in comparison to only 28% using LinkdIn or Pinterest, 26% using Instagram and only 23% using Twitter (Duggan, et al., 2015).

Following IRB approval, data were collected using an online survey distributed through Qualtrics. After consenting to participate in the study, participants were asked to complete the anonymous online survey. The survey was composed of both open ended and closed questions that measured privacy turbulence, relational closeness, personality traits, recalibration, outcomes, and basic demographic information.

Measures

Privacy turbulence. The survey first asked participants to answer an open ended question concerning the details of a past privacy turbulent episode that happened to them on Facebook. Participants were asked to think of a time when another individual (friend, family member, acquaintance, etc.) violated their privacy on Facebook by posting content that was unintended for their whole network and to explain the violating event in detail. The prompt for the open ended question was adapted from McLaren & Steuber (2013) to include privacy turbulence within the Facebook context. A second closed question asked participants to rate the severity of the turbulent episode on a scale from 1-10 with 1 being not severe to 10 being very severe. Participants were asked to keep the situation in mind that they previously described as they answer questions regarding recalibration and privacy boundary outcomes.

Recalibration. Four Likert type items measure how individuals recalibrate following privacy turbulence. Each scale ranges from 1-7 with 1 being no discussion to 7 being a lot of discussion. The first scale asks participants to report how much they discussed the turbulent event publicly in a face-to-face context. The second scale asks how much the participant discussed the event privately in a face-to-face context. The third scale asks how much the participant discussed the event privately online using Facebook or another social media platform. The last scale asks participants how much they discussed the event publicly online using

Facebook or another social media platform. Face-to-face discussion is defined as being physically present, and online discussion is defined as being mediated in some way (text message, social networking site, etc.). Discussion of the event is deemed public if the conversation is able to be viewed or heard by others. Discussion is deemed private if the conversation can only be viewed or heard by the owner and co-owner(s). These definitions were provided to participants in the question prompts on the survey.

Outcomes. Facebook network privacy boundary outcomes and relational privacy boundary outcomes were each measured using four items that used a response set ranging from -3 to 3. Participants rated items asking how the privacy turbulence impacted both his or her relationship with their Facebook network and his or her relationship with the violator. Each item was rated on semantic differential scales that ranged from less open to more open, less willing to share private information to more willing to share private information, more guarded to less guarded, and more closed off to less closed off. Items 3 and 4 for both relational privacy and network privacy were reverse coded and averaged with the first two items to create privacy boundary outcome variables. Cronbach's alpha for network privacy was .60 and .72 for relational privacy. Following each of the privacy boundary scales, an open ended question asked participants to the explain any steps they took to implement any adjustments in privacy boundaries.

Personality. This study uses the Big Five Inventory (BFI) created by John, Donahue and Kettle (1991) and used by John, Naumann & Soto (2008) to measure the big five personality traits of openness (α=.81), conscientiousness (α=.71), extraversion (α=.81), agreeableness (α=.79), and neuroticism (α=.71). The measure consists of 44 items which measure each of the five personality traits. Items are reated on a Likert-type scale ranging from 1-5 with 1 being

strongly disagree to 5 being strongly agree. Each statement begins with “I am someone who..”. Some examples of adjectives that are rated include talkative, depressed, full of energy, etc.

RESULTS

The first four research questions asked about the relationships between the severity of privacy turbulence and face-to-face private recalibration, face-to-face public recalibration, online private recalibration, online public recalibration. Pearson correlations reveal that severity of privacy turbulence is positively correlated with private face-to-face recalibration, $r = .49$, $p < .001$, public face-to-face recalibration, $r = .35$, $p < .001$, private online recalibration, $r = .50$, $p < .001$, and public online recalibration, $r = .26$, $p < .001$. These results are consistant with research questions 1-4 which ask if there are relationships between severity and the recalibration conditions. Hypotheses one and two predict relationships between severity and network and relational privacy boundary thickness. A Pearson correlation revealed that severity of privacy turbulence was negatively associated with relational privacy boundary thickness $r = -.31$, $p < .001$, and network privacy boundary thickness $r = -.22$, $p < .001$. Because of the nature of the boundary thickness scales, a negative correlation indicates that as severity increases, the thickness of privacy boundaries increase, meaning boundaries become less permeable. These results are consistent with hypotheses one and two.

Research question 5 asked if the BFI personality traits moderate the relationships between severity and FtF private recalibration, FtF public recalibration, online public recalibration, online private recalibration, relational boundary thickness and network boundary thickness. In order to test this research question, each BFI trait was split into two categories: higher (1) and lower (0). The two categories were determined by a median split. Table 1 displays the medians, means, and standard deviations for each of the grouped personality traits. Correlations between severity and each of the six variables were run for each of the two personality trait groups in order to reveal any differences between higher and lower trait

correlation coefficients. Differences between the higher and lower groups indicate evidence that the personality trait moderates the relationship between the two correlated variables.

Table 1

BFI personality trait median splits with higher and lower group means and standard deviations

Personality Trait	Median	*M*	*SD*
Extroversion	2.88	3.54	.35
		2.50	.49
Agreeableness	3.33	3.75	.32
		2.84	.26
Conscientiousness	3.44	3.87	.37
		3.00	.27
Neuroticism	2.63	3.03	.35
		2.17	.34
Openness	2.90	3.45	.44
		2.45	.24

Considering the relationship between severity and private face-to-face recalibration, results show minimal differences between higher and lower personality trait groups for most of the personality traits. The variables with the largest gaps are agreeableness (higher: $r = .45$, $p < .001$, lower: $r = .55$, $p < .001$) and neuroticism (higher: $r = .44$, $p < .001$, lower: $r = .54$, $p < .001$). This suggests some moderation of agreeableness and neuroticism between severity and face-to-face private recalibration, but minimal moderation for the extroversion, conscientiousness and openness. Table 2 displays the complete list of correlation coefficients.

Table 2

Correlations between severity and face-to-face private recalibration for higher and lower BFI trait groups

Personality Trait	Higher	Lower
Extraversion	.50***	.48***
Agreeableness	.45***	.55***
Conscientiousness	.46***	.52***
Neuroticism	.44***	.54***
Openness	.49***	.44***

***$p<.001$

Regarding the relationship between severity and public face-to-face recalibration, results show the biggest differences between agreeableness (higher: $r = .29$, $p < .001$, lower: $r = .42$, $p < .001$), conscientiousness (higher: $r = .30$, $p < .001$, lower: $r = .39$, $p < .001$) and openness (higher: $r = .35$, $p < .001$, lower: $r = .27$, $p < .001$). This suggests some moderation of these personality traits between severity and public face-to-face recalibration. Overall, there are minimal differences for extroversion and neuroticism. Table 3 displays the complete list of correlation coefficients.

Table 3

Correlations between severity and face-to-face public recalibration for higher and lower BFI trait groups

Personality trait	Higher	Lower
Extraversion	.35***	.32***
Agreeableness	.29***	.42***
Conscientiousness	.30***	.39***
Neuroticism	.33***	.35***
Openness	.35***	.27***

***$p<.001$

Regarding the relationship between severity and private online recalibration, results suggest that conscientiousness showed the largest difference between higher conscientiousness ($r = .58$, $p < .001$) and lower conscientiousness ($r = .43$, $p < .001$), suggesting that severity and private online recalibration is somewhat moderated by conscientiousness. There were minimal differences for extraversion, agreeableness, neuroticism, and openness. Table 4 displays the complete list of correlation coefficients.

Table 4

Correlations between severity and private online recalibration for higher and lower BFI trait groups

Personality Trait	Higher	Lower
Extraversion	.53***	.50***
Agreeableness	.53***	.49***
Conscientiousness	.58***	.43***
Neuroticism	.47***	.49***
Openness	.52***	.48***

***p<.001

Considering the relationship between severity and public online recalibration, results revealed the largest differences between higher extroversion (r = .32, p < .001) and lower extraversion (r = .19, p = .008), and higher agreeableness (r = .28, p = .08) and lower agreeableness (r = .41, p < .001). This suggests that severity and public online recalibration is somewhat moderated by extraversion and agreeableness. Results revealed minimal differences between groups for conscientiousness, neuroticism, and openness. Table 5 displays the complete list of correlation coefficients.

Table 5

Correlations between severity and public online recalibration for higher and lower BFI trait groups

Personality Trait	Higher	Lower
Extraversion	.32**	.19**
Agreeableness	.28	.41***
Conscientiousness	.27***	.25***
Neuroticism	.24**	.26**
Openness	.24**	.28***

**p<.005. ***p<.001.

Regarding the relationship between severity and relational privacy boundary thickness, results reveal large differences between groups for all of the personality traits, with the largest difference being between higher conscientiousness (r = -.47, p < .001) and lower conscientiousness (r = -.07, p = .33). This suggests that each of the personality traits moderates

the relationship between severity and relational privacy boundary thickness to some degree. Table 6 displays the complete table of correlation coefficients.

Table 6

Correlations between severity and relational privacy thickness for higher and lower BFI trait groups

Personality Trait	Higher	Lower
Extraversion	-.28***	-.37***
Agreeableness	-.43***	-.13
Conscientiousness	-.47***	-.07
Neuroticism	-.19	-.46***
Openness	-.39***	-.21*

*p<.05. ***p<.001.

Regarding the relationship between severity and network privacy boundary thickness, results show relative differences between groups for each of the personality traits, with the largest difference being between higher conscientiousness (r = -.35, p < .001) and lower conscientiousness (r = .00, p = .98). This suggests that each of the personality traits are involved in moderating the relationship between severity and network privacy boundary thickness. Table 7 displays the complete table of correlation coefficients.

Table 7

Correlations between severity and network privacy thickness for higher and lower BFI trait groups

Personality Trait	Higher	Lower
Extraversion	-.17*	-.30***
Agreeableness	-.31***	-.09
Conscientiousness	-.35***	.00
Neuroticism	-.14*	-.31***
Openness	-.27***	-.18*

*p<.05. ***p<.001.

DISCUSSION

The purpose of this study was to investigate privacy turbulence and Facebook user responses and privacy boundary outcomes following privacy turbulence. The study reveals several new insights that contribute to CPM, specifically to the element of privacy turbulence. Results also provide some evidence that personality traits impact privacy turbulence outcomes. Generally, results suggest that more severe privacy turbulence is met with more recalibration and changes in network and relational privacy boundaries. There is also some evidence that the association between severity and recalibration and privacy boundaries is moderated by several of the BFI personality traits.

CPM asserts that privacy turbulence can vary from small rule violations to extreme boundary breakdowns (Petronio, 2013). This study suggests that the range of privacy turbulence also evokes more or less recalibration. Specifically, as the severity of a privacy violation increased, so did recalibration. Individuals also recalibrate in a variety of ways following a privacy violation. Specifically, the more severe a privacy violation, the more individuals recalibrate face-to-face and online both privately and publicly. Steuber and McLaren (2015) found that any amount of recalibration following privacy turbulence is associated with more forgiveness and relational improvement and that positive outcomes result when owners are able to successfully confront the violator. This suggests that a positive relationship between severity and recalibration would lead to healthier relationships. However, this study also found that as severity increased, boundary thickness also increased, suggesting that recalibration may not always result in forgiveness or relational improvement. One reason for this could be that severity of the violation was not accounted for in past research, so it is possible that if a violation is very severe, any amount recalibration is not helpful in improving relationships. Future research could

investigate how styles of recalibration differ, much like conflict styles, to see if the way an individual recalibrates impacts the permeability of privacy boundaries.

This study also revealed that in both face-to-face and online contexts, severity was more strongly associated with private recalibration than public recalibration. These findings support the idea that some types of information are deemed more or less appropriate to share publicly online. Past research suggests that publicly sharing intimate information is perceived as less appropriate than when it is shared privately (Bazarova, 2012). It is possible that discussing a privacy violation publicly may be viewed as less appropriate than discussing it in private.

CPM predicts that individuals will adjust their privacy boundaries following a turbulent episode (Petronio, 2013). Results support this prediction in that relational and boundary thickness increased as severity of privacy violation increased. Previous research has suggested that relational responses to privacy turbulence can be either positive or negative (Child et al., 2012; McLaren & Steuber, 2013; Stueber & McLaren, 2015). This study revealed that the more severe a violation, the more individuals adjust boundaries to be thicker rather than thinner. Generally, privacy violations without recalibration are met with less permeable privacy boundaries (Steuber & McLaren, 2015). As previously discussed, severe violations were also met with more recalibration, both public and private, face-to-face and online. Nevertheless, since individuals report having thicker boundaries following a severe violation, recalibration did not appear to create less permeable boundaries.

Network boundary thickness also increased with the severity of privacy violation. One reason individuals may adjust network boundaries to be thicker is to prevent any further violations from happening. Previous research suggests that Facebook users who have experienced privacy invasions online are more likely to protect personal information through

their privacy settings than those who have not experienced a privacy violation (Debatin et al., 2011). Adjusting privacy settings is one way to thicken network privacy boundaries and prevent future violations from occurring. Another way to thicken network boundaries is to delete, or scrub information (Child et al., 2011). Because Internet users are creating and managing impressions through their online profiles (Rosenberg & Egbert, 2011), they will adjust, amend, change, or scrub privacy rules if they are not fulfilling desired outcomes (Child et al., 2011). The present findings further previous research by suggesting that the severity of the privacy turbulence impacts how much individuals change privacy rules or boundaries as well as the direction that they are adjusted. Because the individuals in this study reported that more severe violations are met with thicker privacy boundaries, it is likely that privacy turbulence is not a positive experience.

The last research question asked if the BFI personality traits influence the relationships between severity and the outcome variables. Past research has called for the investigation of personality trait influences on the privacy management process (Bello et al, 2014; Steuber & McLaren, 2015; Taddicken, 2014) and this study has found that the Big Five personality traits of extroversion, agreeableness, conscientiousness, neuroticism, and openness have some impact on the relationships between the severity of privacy violation and the various privacy turbulence outcomes.

Extraversion impacted the relationship between severity and public online recalibration, as well as relational and network privacy boundary thickness. Severity and public online recalibration was more strongly associated for the more extraverted group than the less extraverted group. Because extraverted individuals are characterized as assertive and outgoing (McRae & John, 1999), it is possible that the more extraverted group views recalibrating publicly

online after a privacy violation as an appropriate avenue for conversation. Previous research has suggested that more extraverted individuals have less relational privacy preferences (Jin, 2013; Sumner et al., 2011), suggesting that these individuals may not consider the publicity of the recalibration to be a problem, and see the conversation as a social opportunity. Extraversion also moderated severity and both relational and network privacy boundary thickness. The less extroverted group was more associated with thicker privacy boundaries for both the relationship and the network, while the more extroverted individuals still adjusted privacy boundaries to be thicker, but not as much as the less extraverted group. This difference was specifically large for network privacy boundaries, suggesting that individuals who are more extroverted may be more relaxed about what information they make available to their network through their social media profile. This suggests that severe violations do not affect privacy boundary thickness as much for more extroverted individuals.

Agreeableness affected the relationship between severity and both public face-to-face and public online recalibration, as well as both relational and network privacy boundary thickness. For both public recalibration conditions, the less agreeable group was more strongly associated with FtF and online public recalibration than those with higher agreeableness. Because agreeableness is characterized as being appreciative, forgiving, generous, kind, sympathetic and trusting (McRae & John, 1999), those who are less agreeable may not consider how public recalibration will affect the violators feelings. However, more agreeable individuals did not appear to recalibrate significantly more in private contexts than less agreeable individuals. It is possible that more agreeable individuals recalibrate less all together because of their trusting, forgiving nature. These findings are somewhat puzzling and deserve more investigation.

Severity and relational privacy boundary thickness were also moderated by agreeableness, with a stronger association between the two variables for the more agreeable group than the less agreeable group. This is surprising considering that individuals who are more agreeable usually enact more forgiveness and trust (McRae & John, 1999). It is possible that these individuals value relationships more, and therefore view severe violations as a threat to the integrity of the relationship. Network privacy boundary thickness was also moderated by agreeableness, with a stronger association between the two variables for the more agreeable group than the less agreeable group. These findings are not consistant with previous research which suggests that higher agreeableness is met with lower concern for online privacy (Sumner et al, 2011). If individuals had lower concern for privacy, it would make sense for individuals to adjust boundaries to be less permeable instead of more permeable. The impact of agreeableness on privacy turbulence response deserves further investigation.

Conscientiousness impacted private online recalibration and privacy boundary thickness. More conscientious individuals recalibrated more privately online than less conscientious individuals. These findings suggest that conscientiousness affects the amount of private online recalibration more than any of the other recalibration methods. Additionally, conscientiouseness substantially moderated severity and privacy boundary thickness, both relational and network. Specifically, more conscientious individuals adjusted boundaries to be much thicker than less conscientious individuals. Conscientious individuals are planful, responsible, and thorough (McRae & John, 1999). More conscientious individuals may feel that thickening privacy boundaries is an act of responsibility or thoroughness in preventing further violations. This may also be the case for private online mediated recalibration.

The BFI trait of neuroticism affected the relationship between severity and both relational and network privacy thickness. However, less neurotic individuals changed their boundaries to be much thicker than more neurotic individuals, suggesting that more neurotic individuals are less concerned about changing privacy boundaries following privacy turbulence. These findings do not agree with previous research. Hazel, Keaten and Kelly (2014) found that neuroticism was positively associated with fear of negative evaluation and Sumner et al (2011) found that higher levels of neuroticism were associated with more concern for online privacy. It is possible that, in this case, more neurotic individuals fear that making thicker privacy boundaries would reflect negatively upon them and they would be judged by the violator and their social media network since neurotic individuals tend to be more anxious and worrying (McRae & John, 1999).

Openness had the most impact on both relational and network privacy boundary thickness. The higher openness group was more associated with boundary thickness than the lower openness group, suggesting that more open individuals adjust boundaries to be thicker following a severe privacy violation. These findings are not consistant with previous research which finds that more openness is associated with less fear of negative evaluation (Hazel et al, (2014) and that more openness is associated with more disclosure on Twitter (Jin, 2013). This finding is puzzling and deserves further research concerning how openness impacts privacy management.

Surprisingly, the five BFI traits did not have much of any impact on the relationship between severity and private face-to-face recalibration. Each of the BFI traits revealed only small differences between the higher and lower trait groups. This suggests that these persoanlity traits do not impact face-to-face discussion about online privacy turbulent episodes. It is possible that

severity was the biggest influence on how much face-to-face recalibration is necessary following a privacy violation.

Broadly, this study contributes to existing CPM research by discovering that the severity of privacy turbulence can impact how individuals react and change privacy boundaries. Knowing how personality can affect outcomes, especially in relational boundary thickness, can help increase empathy in relationships. When individuals understand how aspects of their personality affect the way they communcate, they can foster more undersanding and empathy within a relationship. Furthermore, personality characteristics can affect the relationship between severity of turbulence and reactions to the turbulence. Knowing that severity of privacy turbulence alters how individuals react to the privacy turbulence opens up new avenues for future research.

Limitations and Future Research

Though this study suggests some new insight into privacy management and privacy turbulence online, it also has some limitations. The survey design presented some problems, specifically regarding the performance of the boundary thickness measures. The purpose of these measures was to gage how individuals change or alter their privacy boundaries following a severe privacy turbulent incident. However, the network boundary thickness measure had relatively low reliability (α=.60) due to unknown factors. One possible explanation is that the wording may have been misinterpreted, or the scale (-3 to 3) was confusing to participants. Future measurement of this concept should alter wording and/or scale type to increase validity and reliability.

In testing the moderation of personality between privacy turbulence severity and the various outcomes, the mean differences between the higher and lower personality trait groups were minimal. This suggests that the individuals who were placed in the higher group did not

score that much differently than those placed in the lower group, and vice versa. The minimal mean difference between groups is one possible explanation as to why the results revealed some marginal differences between correlation coefficients for higher and lower personality types. Future research may want to compare upper and lower quartiles, instead of using a median split, in order to reveal more accurate differences between higher and lower personality trait groups. This study did not compare quartiles because the sample size was not large enough. However, considering the marginal mean difference between the two groups, there were some correlations that did differ significantly, suggesting that personality is an important factor to consider in studying responses to privacy turbulence.

Previous research suggests that social media sites, like Facebook, are places where individuals merge many different audiences in one place and therefore must manage their privacy goals more carefully (boyd, 2008; Vitak, 2012). This context collapse then increases the possibility of privacy violations occurring online. However, many of the participants in this sample reported never having experienced a privacy violation on Facebook. This suggests that privacy turbulence does not occur as often as expected in this context. One possible explanation is that Facebook users believe that they are able to control their private information and manage privacy rules effectively, avoiding privacy breakdowns. It is also possible that those who reported not having experienced a privacy violation already had thick privacy boundaries to begin with, which would protect them from any chance of a privacy violation occurring. Users may also consider privacy violations a flaw in impression management strategy rather than a flaw in privacy management and may respond quickly by scrubbing content without perceiving the violation as a loss of privacy control.

One implication that emerges from these findings is that the definition and importance of privacy likely varies across individuals. As users rely on Facebook more and more for social interaction, it is possible that the blurred lines between private and public spheres may be warping the definition of privacy. For example, users may not consider privacy a valid concern on social media, but rather they may be more concerned with how others respond to their content, or whether or not it meets their social needs or personal goals. Future research should investigate how users define privacy and privacy turbulence online and how their definitions impact their responses to it.

The current study assumes that social media interactions are more permanent than face-to-face interactions. This permanence results in context collapse, which can increase privacy turbulence because of the de-contextualization of content (boyd, 2007; Vitak, 2012). However, this ignores the idea that face-to-face interaction can also be very permanent, specifically if it is public or has permanent repercussions for the individual. Similarly, social media content is thought of as being permanent, but users have the ability to hide information from their profiles, which challenges the permanent aspect of the Internet. The permanence of the interaction is likely determined by the perception of the individual. This perceived permanence may impact how private information is managed online and is another possible avenue for future research.

The specific ways in which individuals respond to privacy turbulence online have not been investigated extensively and deserve further research. This study found that individuals recalibrate in various ways, but did not include which types of violations lead to which modes of recalibration. If individuals do recalibrate, what kinds of messages or reactions are used to recalibrate? This study focused on recalibration and boundary thickness as separate outcome variables, but did not test how these two variables interact with each other. Future research

should investigate whether or not more recalibration leads to more permeable boundaries, since recalibration is found to enact more forgiveness and relational improvement (Steuber & McLaren, 2015).

Another possible avenue for future research should explore other factors that influence privacy management. This study suggested that some personality traits impact privacy turbulence outcomes, but it is possible that personality traits may influence other aspects of the privacy management process such as privacy control. It is also possible that other individual factors, such as privacy orientation, may influence the privacy management process.

Overall, this research contributes several key findings to CPM and Internet privacy research. First, it extends CPM to the online context and suggests that individuals who experience online privacy turbulence adjust privacy boundaries with both their network and the violator following the turbulent event. This research also revealed that the severity of a privacy violation impacts how individuals respond and that they discuss the event with the violator in different ways, both in public/private and mediated/face-to-face. Findings also suggest that the BFI personality traits impact how individuals respond to privacy turbulence. As society continues to operate online just as much as offline, it is important to understand how individuals respond to privacy turbulence online and how individual factors influence these responses. This study aimed to investigate some of the factors that may impact privacy turbulence outcomes.

REFERENCES

Acquisti, A., & Gross, R. (2006). *Imagined communities: Awareness, information sharing, and privacy on the Facebook*. Proceedings from Privacy Enhancing Technologies Workshop, Cambridge, UK.

Bazarova, N. N. (2012). Public intimacy: Disclosure interpretation and social judgment on Facebook. *Journal of Communication, 62.* 815-832. doi:10.1111/j.1460-2466.2012.01664.x

Bello, R. S., Brandau-Brown, F. E., & Ragsdale, J. D. (2014). A profile of those likely to reveal friends' confidential secrets. *Communication Studies*, *65*(4), 389-406. doi:10.1080/10510974.2013.837082

Bernstein, M., Bakshy, E., Burke, M., & Karrer, B. (2013). Quantifying the invisible audience in social networks. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 21–30). New York, NY: ACM. doi:10.1145/2470654.2470658

boyd, D. (2008). *Taken out of context: American teen sociality in networked publics*. (Doctoral dissertation). University of California, Berkeley, Berkeley, CA.

Child, J. T. & Agyeman-Budu, E. A. (2010) Blogging privacy management rule development: The impact of self-monitoring skills, concern for appropriateness, and blogging frequency. *Computers in Human Behavior, 26*, 957-963. doi:10.1016/j.chb.2010.02.009

Child, J. T., Petronio, S., Agyeman-Budu, E. A., Westermann, D. A. (2011). Blog scrubbing: Exploring triggers that change privacy rules. *Computers in Human Behavior, 27*, 2017-2 027. doi:10.1016/j.chb.2011.05.009

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*, 1-8. 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

Craig, E., & Wright, K. B. (2012). Computer-mediated relational development and maintenance on Facebook. *Communication Research Reports*, *29*(2), 119-129. doi:10.1080/08824096.2012.667777

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*, 83-108. doi:10.1111/j.1083-6101.2009.01494.x

Duggan, M., Ellison, N. B., Lampe, C., Lenhart, A., & Madden, M. (2015, Jan 9). Social media update 2014. Pew Research Center. Retrieved from http://www.pewinternet.org/2015/01/09/social-media-update-2014/

Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook "friends:" Social capital and college students use of online social network sites. *Journal of Computer-Mediated Communication, 12*, 1143-1168. doi: 10.1111/j.1083-6101.2007.00367.x

Facebook Newsroom (2016). *Stats.* Retrived from http://newsroom.fb.com/company-info/

Fogel, J. & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior, 25,* 153-160. doi:10.1016/j.chb.2008.08.006

Goldberg, L. R. (1981). Language and individual differences: The search for universals in personality lexicons. In L. Wheeler (Ed.), *Review of Personality and Social Psychology*: Vol. 2 (pp. 141-165). Beverly Hills, CA: Sage.

Hazel, M., Keaten, J., & Kelly, L. (2014). The relationship between personality temperament, communication reticence, and fear of negative evaluation. *Communication Research Reports, 4*(31), 339-347. doi: 10.1080/08824096.2014.963219

Hesse, C., & Rauscher, E. A. (2013). Privacy tendencies and revealing/concealing: The moderating role of emotional competence. *Communication Quarterly*, *61*(1), 91-112. doi:10.1080/01463373.2012.720344

Hogan, B. (2010). The presentation of self in the age of social media: Distinguishing performances and exhibitions online. *Bulletin of Science, Technology, & Society, 30*(6), 377-386. doi: 10.1177/0270467610385893

Jin, S. A., (2013). Peeling back the multiple layers of Twitter's private disclosure onion: The roles of virtual identity discrepancy and personality traits in communication privacy management on Twitter. *New Media and Society, 15*(6), 813-833. doi: 10.1177/1461444812471814

John, O. P., Donahue, E. M., & Kentle, R. L. (1991). The big five inventory—Versions 4a and 54. Berkeley, CA: University of California, Berkeley, Institute of Personality and Social Research.

John, O. P., Naumann, L. P., & Soto, C. J. (2008). Paradigm shift to the integrative Big Five trait taxonomy: History, measurement, and conceptual issues. In O. P. John, R. W. Robins, & L. A. Pervin (Eds.), *Handbook of personality: Theory and research* (pp. 114-158). New York, NY: Guilford Press.

John, O. P., & Srivastava, S. (1999). The Big-Five trait taxonomy: History, measurement, and theoretical perspectives. In L. A. Pervin & O. P. John (Eds.), *Handbook of personality: Theory and research* (Vol. 2, pp. 102–138). New York: Guilford Press.

Kanter, M., Afifi, T., & Robbins, S. (2012). The impact of parents "friending" their young adult child on Facebook on perceptions of parental privacy invasions and parent-child relationship qulity. *Journal of Communication, 62*, 900-917. doi:10.1111/j.1460-2466.2012.01669.x

Kennedy-Lightsey, C. D., Martin, M. M., Thompson, M., Himes, K. L., & Clingerman, B. Z. (2012). Communication privacy management theory: Exploring and ownership between friends. *Communication Quarterly*, *60*(5), 665-680. doi:10.1080/01463373.2012.725004

Knowles, M. (2012, September 25). PSA uses 'Psychic' to demonstrate dangers of sharing personal info online. *Yahoo! News*. Retrieved from https://www.yahoo.com/news/blogs/trending-now/psa-uses-psychic-demonstrate-dangers-sharing-personal-online-174017116.html

Ledbetter, A. M., Heiss, S., Sibal, K., Lev, E., Battle-Fisher, M., & Shubert, N. (2010). Parental invasive and children's defensive behaviors at home and away at college: Mediated communication and privacy boundary management. *Communication Studies, 61*(2). 184-204. doi: 10.1080/10510971003603960

Lenhart, A. (2015, August 6). Teens, technology and friendships. *Pew Research Center.* Retrieved from http://www.pewinternet.org/2015/08/06/teens-technology-and-friendships/

McLaren, R. M., & Steuber, K. R. (2013). Emotions, communicative responses, and relational consequences of boundary turbulence. *Journal of Social and Personal Relationships, 30*(5), 606-626. dio:10.1177/0265407512463997

McRae. R.R., & John O. P. (1999). An introduction to the five factor model and its applications. *Jounral of Personality, 60,* 175-215.

O'Sullivan, P. B. (2005, May). *Masspersonal communication: Rethinking the mass interpersonal divide.* Paper presented at the annual meeting of the International Communication Association, New York.

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

Petronio, S. (2010). Communication privacy management theory: What do we know about family privacy retulation? *Journal of Family Theory & Review*, *2*. 175-196. doi:10.1111/j.1756-2589.2010.00052.x

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. & Durham, W. T. (2015). Communication privacy management theory: Significance for interpersonal communication. In D. O. Braithwaite (Ed.,) *Relationship-Centered Theories of Interpersonal Communication* (pp. 335-347). Thousand Oaks, CA: SAGE Publications Inc.

Rosenberg, J., & Egbert, N. (2011). Online impression management: Personality traits and

concerns for secondary goals as predictors of self-presentation tactics on Facebook. *Journal Of Computer-Mediated Communication*, *17*(1), 1-18. doi:10.1111/j.1083-6101.2011.01560.x

Steuber, K. R. & McLaren, R. M. (2015). Privacy recalibration in personal relationships: Rule usage before and after an incidient of privacy turbulence. *Communication Quarterly, 63*(3), 345-364. doi: 10.1080/01463373.2015.1039717

Stutzman, F., Capra, R., & Thompson, J. (2010). Factors mediating disclosure in social network sites. *Computers in Human Behavior, 27*, 590-598. doi:10.1016/j.chb.2010.10.017

Sumner, C., Byers, A., & Shearing, M. (2011). Determining personality traits & privacy concerns from facebook activity. *Black Hat Briefings*, *11*, 197-221. Retrieved from https://media.blackhat.com/bh-ad-11/Sumner/bh-ad-11-Sumner-Concerns_w_Facebook_WP.pdf

Taddicken, M. (2014). The 'Privacy Paradox' in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal Of Computer-Mediated Communication*, *19*(2), 248-273. doi:10.1111/jcc4.12052

Venetis, M. K., Greene, K., Magsamen-Conrad, K., Banerjee, S. C., Checton, M. G., & Bagdasarov, Z. (2012). “You can't tell anyone but …”: Exploring the use of privacy rules and revealing behaviors. *Communication Monographs*, *79*(3), 344-365. doi:10.1080/03637751.2012.697628

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

Waters, S. & Ackerman, J. (2011). Exploring privacy management on Facebook: Motivations and percieved consequences of voluntary disclosure. *Journal of Computer-Mediated Communication, 17*, 101-111. doi:10.1111/j.1083-6101.2011.01559.x