2-2020

Effect of penitence on social media trust and privacy concerns: The case of Facebook

Emmanuel Wusuhon Yanibo Ayaburi
The University of Texas Rio Grande Valley

Daniel N. Treku
The University of Texas Rio Grande Valley

Recommended Citation

Ayaburi, Emmanuel W., and Daniel N. Treku. 2020. "Effect of Penitence on Social Media Trust and Privacy Concerns: The Case of Facebook." International Journal of Information Management 50 (February): 171–81. https://doi.org/10.1016/j.ijinfomgt.2019.05.014.

Effect of Penitence on Social Media Trust and Privacy Concerns: The Case of Facebook

Abstract

Abuse of information entrusted to organizations can result in a variety of privacy and trust concerns for consumers. In the event of violations, a social media brand or organization renders an apology – a form of social account – to alleviate users' concerns and maintain user membership and engagement with the platform. To explore the link between apology offered by a social media brand or organization and the users' trust dynamics in the brand's services, we study how organizational integrity can contribute to reducing individuals' privacy concerns whiles increasing or repairing their trust. Drawing on organizational behavioral integrity literature, our proposed research model suggests that the persuasiveness of an apology following a data breach affects users' trust or spillover trust through their perceptions of the degree of alignment between the words in the apology and the actions of the violating entity. Based on a survey of Facebook users, our findings show that persuasiveness of an apology has a significant impact on users' perceptions of the alignment between the social media brand's (i.e. Facebook) words and subsequent actions. These perceptions impact social media brand trust (i.e. users' trust in Facebook and allied services such as Instagram). We also find that, post data breach incidence, while integrity of the social media organization partially mediates the relationship between persuasive apology and users' trust, it fully mediates the relationship between the persuasive apology and the privacy concerns expressed by the users. However, users' privacy concerns do not contribute much to the repair of trust needed to maintain their membership.

Keywords: Apology, Behavioral integrity, Privacy concerns, Trust, Facebook, Social Media

1 Introduction

''Trust, like the soul, never returns once it is gone.'' by Publilius, Syrus

Trust has been echoed by leaders around the world as a key ingredient in sustaining effective organizational communication and business operations. In his 2009 State of the Union Address, former US President Barack Obama highlighted a 'deficit of trust' in business and public institutions and charged researchers and policy makers to restore trust in institutions and organizations (Good, 2013). Users' trust in institutions may be based on the type of organizations' product or service. In the case of Facebook, a popular social media brand or organization which offers communication and social network services with over 1.7 billion users (Shiau, Dwivedi, & Lai, 2018), trust may reflect the perception users have regarding the storage, usage and protection of their shared information on Facebooks' network platform.

The recent announcements of data and privacy breaches by major organizations such as Equifax and social media giant, Facebook, may have increased consumers' privacy concerns and impair consumer trust in these organizations. A reduction in user trust in organizations leads to a decrease in use of social media platforms (Antoci, Bonelli, Paglieri, Reggiani, & Sabatini, 2019). In 2014, Cambridge Analytica, a business firm based in London, UK, offering audience change behavior services, begun to inappropriately harvest Facebook users' personal information and opinions without authorization (Confessore, 2018). The unauthorized harvesting and subsequent commercialization of Facebook users' psychological profiles increased users' privacy concerns and created credibility issues for Facebook. The heightened user concerns led to Facebook's chief executive officer, Mark Zuckerberg, being summoned to testify in the United States Congress. To reassure its users and encourage them not to close their accounts, Facebook bought full-page advertisements on March 25, 2018 in seven British and three American news organizations. In each of the advertisement, Facebook as a social media brand offered an apology to its users. Despite the apology from Facebook, survey of opinions across major markets including United States and Germany suggested that users maintained low level of trust in social media, especially, Facebook over their privacy (Kahn & Ingram, 2018). The survey also suggested that some users were reconsidering their membership or nature of engagements with social media platforms.

Due to the frequent data and privacy breaches associated with digitized data, it is noteworthy that the nature and impacts on the operations of social media brands or organizations are more complex and damming compared to traditional media of communication (Miranda, Young, & Yetgin, 2016) . The complexity is also aggravated by the inherent risks and unique features of personally identifiable information shared on social media platforms or networks (Tow, Dell, & Venable, 2010). Privacy risk creates concerns for individual users and threatens the providers' business model (Weiss, 2009). This study focuses on how the dynamics of information sharing on social networks or platforms may be understood in terms of how organizations respond to breaches to shared information. Also, the study aims to understand how these breach incidents impact consumers' privacy concerns and subsequent users' information sharing behaviors on the social network. Despite the publicity of data breaches and subsequent apologies by social media platforms, Facebook users continue to disclose more information although they acknowledge concerns about how their sensitive information is being protected (Christofides, Muise, & Desmarais, 2009). Perhaps the stakeholders' efforts in trust building activities play post priori roles in users' trust in social media brands (Porter, Devaraj, & Sun, 2013). Therefore, it is important to explicate the consequential effects surrounding how the use of social network site (Facebook platform) impact trust dynamics in the social media organization or brand (Facebook), following data breach incidents or perceived violations. The effectiveness of the business communication processes, post incident activities, may depends on users' judgements of trust in the organization. Explicitly, we focus on a specific antecedent of trust-rebuilding behavior of social media platform provider in reaction to the perceptions of use/misuse of users' stored information.

The maintenance and use of platforms such as Facebook come at a cost to the user. Maintaining users' privacy is cognitively and physically costly (Jiang, Heng, & Choi, 2013). This is even exacerbated when users' trust is violated. Users need to make themselves vulnerable to trust Facebook and willingly share sensitive information in the use of the application. As the opening axiom echoes, trust is delicate and prior research suggests that repair of broken trust in business is a notoriously difficult task, effort and time involve is a lengthy process (Lount, Zhong, Sivanathan, & Murnighan, 2008). The violating entity may offer explanation, excuses, and/or penitence (apology) which are various forms of social account, in an attempt at trust rebuilding process (Simons, 2002). Individuals who have had their trust betrayed, may look for

substantive actions from the violator not merely words (Farrell & Matthew Rabin, 1996). We expect it would be no different in the case of Facebook. Trust in the services or product of the organization may be minimally affected if the words of the organization match their actions else users will consider an apology, a form of social account, as cheap talk (Dirks, Kim, Ferrin, & Cooper, 2011). The alignment between the organization or person's words and action is termed Behavioral Integrity (Simons, 2002). Behavioral integrity (BI), which is key in trust repair, is also influenced by the context in which trust is broken (Bachmann, Gillespie, & Priem, 2015). In an attempt to repair trust, explanation, excuses, and penitence (apology) rendered influence the users perception of the person's or entity's BI and subsequently the trust rebuilding process (Simons, 2002). However, does the persuasiveness of the apology by Facebook (see Appendix C) influence the trust of individual users in the social media context? In the era of ubiquitous computing, it is possible that lack of trust in a platform could have spillover effects on allied product or services by the parent organization. In the context of Facebook, the trust issues resulting from privacy concerns from the operation of Cambridge Analytica may have effects on its allied services such as WhatsApp. It has been reported that WhatsApp CEO may have quit his job because of the privacy scandal and this could create trust issues for WhatsApp users (White & Sharman, 2018). Facebook has pledged new actions to ensure user privacy on their platform and other services. However, the effectiveness of their actions has not been theoretically investigated. Knowing this, is key to developing trust repair mechanisms where the focus of extant scholarship has been on designing easy-to-use privacy and security setting based on assessment of how individuals use the application. This study seeks to explain how we can understand the psychological mechanisms of future user trust repair on social media platform following perceived information misuse of the medium of information exchange. Specifically, we seek to answer the following post data breach research questions:

RQ1: What is the effect of penitential social account (apology) on social media platforms' behavioral integrity and users' privacy concerns?

RQ2: What is the effect of behavioral integrity on the trust in the primary social media platform usage?

RQ3: What is the effect of behavioral integrity on trust in affiliate social media services of the primary social media platform?

Explicating the underlying trust repair process that lead individuals to maintain membership after infringement on their privacy is thus the central goal of the current article. There are reports in print media such as the Daily Mail (2018) that suggest that about one in ten Facebook users in America considered quitting the site after the Cambridge Analytica data breach mainly due to users developing low trust in the social media giant despite strong network effects on the platform. To answer the above research problems we draw on the concept of Behavioral Integrity at the organizational level (Simons, 2002), to develop a model that explicates the effect of apology (penitential account) on trust repair and privacy concerns. We gather data on key perceptions of Facebook users who have seen the apology offered by Facebook. Analysis of survey responses from Facebook users provide insights into the mechanism by which crisis response/communication affect trust repair. By investigating and understanding the mechanism for rebuilding trust based on the actions of the privacy violating entity, we complement prior studies such as Wang & Herrando (2019), that aim to provide social media developers and organizations the strategies that, when applied, would encourage their members to continue using social media after privacy breach. We contribute to the body of knowledge related to privacy breach management and business crisis management by providing insights for research and practice. This is important for the design of social accounts that are crucial to maintain membership of the application despite increase competition from other social media platforms. Overall, this paper offers three contributions to literature. One, our study demonstrates that the persuasiveness or appeal of an apology helps to determine whether behavioral integrity perception translate into more trust needed to maintain users on a social media platform after privacy infringement. In doing so, we help identify the conditions that facilitate the effect of trust (Robert Jr & You, 2018). Two, our findings show that privacy concerns unlike integrity is not related to the development of trust needed to maintain users' membership after privacy violations. Three, the study identifies the theoretical linkage between persuasive social account and trust spillover effects. Most firms operate multiple social media platforms; therefore, it is important to understand the effect of privacy violations on users' trust in those platforms.

The structure of the rest of this paper is as follows: next is the discussion of literature related to this study, followed by a presentation of the theoretical framework and hypotheses development, and finally by discussion of the methodology used, and results of the study.

2 Related Literature

Recent research studies on social media have looked at social media use from trust or privacy perspective. We review prior literature on social media trust and privacy that informs this study to understand the intricate association of these important factors post data breach.

2.1 Social Media Trust

There have been calls for the resignation of Facebook's CEO by the treasurers of New York City, Rhode Island and Pennsylvania – states which have public funds invested in Facebook (Kelly, 2018). These calls have been necessitated by series of accusations levelled against Facebook. Accusations of Facebook include being a conduit for election meddling and for the spread of misinformation following the expose on Cambridge Analytica. Notably, Facebook's handling of user trust and privacy issues have been questioned. To be fair, these accusations may be perceptions users have about the about the focal medium, which is the platform provided by Facebook. However, the consequences of such perceptions cannot be underestimated. Wang & Herrando (2019) assert that the perceived misappropriation of the medium has far reaching consequences on the trust users have in using the social media. It is not surprising since user information is generated, stored and used on social media (Wang & Herrando, 2019). Therefore, for a business entity like Facebook, understanding trust dynamics in the face of accusations is always vital for their better business outcomes.

The importance of trust in building and maintaining consumer relationships in the online environment is widely examined in the Information Systems (IS) literature (e.g. Kamboj, Sarmah, Gupta, & Dwivedi, 2018). The concept of trust has been prominent among researchers with different perspectives proffered. Antoci et al., (2019) show antecedent or consequent effects of user trust on businesses or other social entities via social media platforms. Aladwani & Dwivedi (2018) focused on government's engagement with social media via trust configuration. Aside the uniqueness in the phenomenon of interest interrogated by different research works, trust-related social media studies, generally and implicitly, focus on users' information disclosures and participation/engagement with social media platforms (or social network sites) such as Facebook, Twitter and Snapchat (see Kapoor et al., 2018).

Users' trust in social media platforms have been shown to be influenced by perceived competence, benevolence and integrity (Benbasat & Wang, 2005). Users care if the social

medium, in which they are involved with, adheres to espoused set of principles or respects their interests or motivations. Information sharing and social support are some of the motivations for user engagement with social media platforms (Wang & Herrando 2019). Sustaining this engagement is necessary for business owners. To this, some studies (e.g. Lankton & McKnight, 2011) suggest that the sustenance of user motivations are dependent on their trust in the social media technology and on the organizations operating the platform, we refer to the latter as social medium brand trust. Kamboj et al.,(2018) used the term brand trust to reflect trust dynamics within organizations or entities that leverage social medium platform for its operations. A brand refers to the "name, term, sign, symbol (or combination of these) that identifies the maker or seller of a product" (Kotler & Armstrong, 2013). Consequently, we use the term social media brand to refer to the larger organization or brand such as Facebook and its affiliate services such as WhatsApp and Instagram platforms. We note that users' trust in the technology platform differs from the social media brand trust (Lankton & McKnight, 2011). Notwithstanding, each trust mechanism affects users' continuous use of the platform which may be injurious to a brand's business operations. Bonsón, Escobar, & Ratkai, (2014) found evidence that the intention to continuously use a technology or its services depends on stakeholders' satisfaction in the use of the platform. Kourouthanassis, Lekakos, & Gerakis (2015) argue that trust moderates the relationship between user satisfaction and likelihood of continuous use of the social media. Trust in the entity is negatively affected when users are victimized or experience violation of their privacy following a data breach (Näsi, Räsänen, Keipi, & Oksanen, 2017). The discussion suggests the importance of trust dynamics in research on social media engagement and its link with privacy issues. We discuss social media privacy in the next section.

There is little research on the actions taken by an entity (social media brand) and the effects of these actions following data breach incidence or perceived misappropriation of the platform. Activities bordering on the entity's attitude or in the process of re-establishing a broken trust or addressing privacy concerns which are crucial to the users' trust dynamics in the use of social media platforms (Chang, Liu, & Shen, 2017).

2.2 Social Media Privacy

Researchers have examined many aspects of privacy on social networking sites including analyses of the content that is shared on these sites (Bauer et al., 2013). Predominantly, the

constructs used to understand users' privacy are 'Concerns for Information Privacy' (CFIP) or 'Internet Users' Information Privacy Concerns' (IUIPC) (Malhotra, Sung, & Agarwal, 2004). Users weigh the costs and benefits of disclosure when they make the decision to reveal their information on social media platforms and this has been studied in literature through the lenses of Privacy Calculus framework (Jiang et al., 2013). The benefits of using social media are constantly irresistible for most users as social networking sites are taking over the traditional communication means. However, users' calculus is expected to change when they experience violation of their privacy. When violations occur, social media users may respond through such mechanisms as refusal, misrepresentation, removal, negative word-of-mouth, and complaining (Son & Kim, 2008).

Privacy concerns negatively affect users intentions to engage in social media and social commerce sites (Wang & Herrando, 2019). Online privacy concerns are highly impacted by the users' trust in the online platform (Chen, Beaudoin, & Hong, 2016). Social media platforms counter users' concerns by increasing their perception of privacy control. Platforms provide users with control for setting their privacy with the hope that it would lower their concerns (Stern & Kumar, 2014). When users do not experience privacy breach, or are psychologically distant, their attitude towards privacy choices are different (Hallam & Zanella, 2017). This implies that when users' experience violation of their privacy, their use of the social media platform will be affected due to reduction in trust. While privacy concerns are a major issue for many researchers (Külcü & Henkoğlu, 2014; Mamonov & Benbunan-Fich, 2017), little attention has been directed to the actions of the violating entity post privacy breach and how these actions influence the process of repairing the broken trust. Repairing the broken trust is important to maintaining users on the platform; as it affects their perception of the honesty and trustworthiness of the platform (Son & Kim, 2008). We argue in this study that, when social media platform owners take steps to assuage users' privacy concerns by making sure that their promised actions match their stated word, i.e. behavioral integrity, users' trust in brand's products or services (social media brand trust) will not be completely eroded. Based on the discussions, we assert that the organizational posturing following privacy violations is key to examining post incident dynamics of users' trust in the organization. Specifically, we leverage the concept of behavioral integrity as an organizational posturing lens to develop our research model.

3 Research Model and Hypotheses Development

We begin our model development by exploring the lens of organizational Behavioral Integrity and how it relates to social accounts and trust. We then add to the model, the underlying results of data breach – loss of ownership and control of users' private information –, which is rooted in their privacy concerns.

3.1 Behavioral Integrity

Behavioral integrity (BI) framework (Simons, 2002) explores the organizational posturing through employees' perception of their manager's word-deed alignment and how consequent trust dynamics inform reactionary behaviors. The framework argues that trust is a consequence of a perceived pattern of alignment between an organization's words and deeds or actions (Simons, 2002). The antecedents of users' perceptual filtering of word-deed alignment are due to organizational change stimulus (in this study context, data breaches or privacy violations). This provides a basis for a social account to be given by the organization in response to why the change incidences occurred. BI's conceptualization provides a broader perspective for studying not only the perception within internal stakeholders but also the external stakeholders who are partakers of the product and service offerings of the organization.

In this study, we focus on theorizing users' reactionary behavior in the context of repairing any broken trust as a result of perceived word-deed misalignment/alignment following a social media organization's (or brand's) social account. Following Palanski & Yammarino (2007, 2009), we define behavioral integrity as the perceived degree of consistency of the actions of social media platform provider and its words. When the actions and words of the actor are aligned, they are deemed to have behavioral integrity (Simons, 2002). The actor could be an individual, group or an organization, making behavioral integrity a concept with a multilevel approach (Klein & Kozlowski, 2000). Our study examines the actions of the social media platform provider (i.e., Facebook). Thus, behavioral integrity of Facebook refers to the word and action alignment of the company, but not the integrity of any of its employees or the industry. It is not surprising that much of the focus on trust repair research has been on the actions of an individual. However, understanding behavioral integrity of an organization is vital, because it affects the development of trust, commitment and reciprocal respect between entities (Parry & Proctor-Thomson, 2002).

Positive outcomes of behavioral integrity are adversely affected when users feel abused or violated. However, when the violating entity is transparent about the events leading to a breach or in dealing with fallouts from the breach, users may not entirely blame the organization. Transparency, a key ingredient in the process of rebuilding trust after the violation, is dependent on which social account response (apology, denial, or excuse) the entity initiates. A response should not only be timely but also considers all factors contributing to the deficit of integrity. The organization's actions could be regarded as superficial if they tackle symptoms but not the cause of deficit of trust (Gillespie & Dietz, 2009). There are several social accounts such as denial, penitence (apology), justification and excuses, used in an attempt to repair trust (Tomlinson & Mayer, 2009) and different kinds of account operate different ways (Bies, 1987). Thus, each of these social accounts has different effects on individuals' perception of organizational justice (Simons, 2002). The actions and words of organizations, following any of these social accounts, impact individuals perception of behavioral integrity and consequently transparency and trust repair (Palanski, Kahai, & Yammarino, 2011).

While denials attempt to shift blame, excuses blame external forces and justification aims to reduce the perceived level of negativity of the outcome. On the other hand, an apology, also called penitential social account, aims at internalizing blame and reassuring unlikely recurrence of the outcome (Bies, 1987; Greenberg, 1990). Based on the concept of behavioral integrity, we develop our research hypotheses that explain the effect of apology, the popular social account usually deployed by a social media entity (i.e. Facebook), on privacy concerns and trust with respect to the primary/focal/main social media services and affiliate/allied services from the same organization.

3.2 Persuasive Apology and Behavioral Integrity

Organizations employ several social accounts to repair their threatened reputation or demonstrate fairness in their relationship with their clients when they seek to restore soiled credibility. As the focus of study is on the recent actions of social media giants (such as Facebook) with respect to response to privacy invasion, we focus on the persuasiveness of penitential account (PA) also referred to as apology dimension of social account. PA are expressions of regret in which the actor accepts responsibility for the actions with acknowledgement that, the actions do not represent the true nature of the actor (Simons, 2002). The nature, time and style of delivering a PA affects perceptions of the degree of alignment

between an entity's words and actions (Bachmann et al., 2015). The persuasiveness of the PA affect users' judgement of degree of honesty or fairness in the actions of the entity as it tries to align its actions with the content of the PA or its mission statement. An apology has been reported as a powerful trust repair tool as it shows admission of responsibility, regret and desire to reconcile the relationship on the part of the violating entity (Tomlinson, Dineen, & Lewicki, 2004). In the case of Facebook, it is expected that an apology would signal an admission that their conduct was wrong and unacceptable. Social media users will therefore not expect a repeat of the violation as they judge the actions of the social media platform. This is because when the violating entity takes the blame for the deficit of trust, and deliver a timely apology it would affect users perception of their actions as being genuine, thereby increasing trust (Dirks et al., 2011; Gillespie & Dietz, 2009; Tomlinson et al., 2004). Hence, we posit that for social media users:

> **Hypothesis 1A**: Persuasive apology (penitential social account) for information misuse positively influence perceived behavioral integrity needed to maintain users' relationship with the organization (Facebook).

3.3 Persuasive Apology and Privacy Concerns

Privacy concerns are worries that users may have about the possibility of losing one's personal information entrusted to the other party in a transaction (Xu, Dinev, Smith, & Hart, 2011). These concerns involve a subjective evaluation of the information provided and the actions taken by the primary parties involved in protecting access to the information and what they may do with it. Privacy violations by a third party not involved in the primary transaction can have severe consequences including profiling, price discrimination and targeted ads (Dinev & Hart, 2006). When the primary actors involved take responsibility and promise to take steps to protect an individual after privacy invasion by a third-party, individual future concerns about another invasion may be assuaged. Consistent with the prior literature about the effect of apology, we hypothesize that:

> **Hypothesis 1B**: Persuasive apology (penitential social account) for information misuse will decrease perceived privacy concerns with the organization (Facebook).

3.4 Behavioral Integrity and Privacy Concerns

An entity is perceived to have BI when it is seen to act in the best interest of the user by protecting user private information rather than acting primarily to advance its profit-making agenda with the information. BI is relevant because it shows the commitment of an entity to fulfil its obligation. Additionally, integrity demonstrates interest of the entity in maintaining the relationship with its clients. For example, when a social media user elects to reveal private information to the platform, the user grants the platform operator certain powers and discretion in the use of the information. Social media users are anxious about how their personal information is collected and shared, and the security of their data. Previous research suggests a negative relationship between users' privacy concerns and Facebook use (Xu et al., 2011). When the actions of the operator are indeed in line with the promise not to repeat actions that led to the breach of privacy and subsequent violation of trust, the user's concerns about abuse of private information is expected to be assuaged. Increase in BI is a demonstration of the entity caring about user's feedback. Organizational actions that are reassuring will therefore be critical in alleviating the effects of any concerns. We therefore argue that:

> **Hypothesis 2**: Users' perceived behavioral integrity of the organization (Facebook) after information misuse is negatively associated with perceived privacy concerns.

3.5 Behavioral Integrity and Trust (Focal Social Media)

Violation of integrity at the organizational level leads to a substantial crisis of the organization's legitimacy. This affects stakeholders' trust in the organization and its services (Gillespie & Dietz, 2009). However, when the penitent words and deeds of the violator are aligned, an apology is seen as being sincere and not a mere cheap talk. Thus, users may perceive the entity's integrity in a positive light in the trust repair process. Users of social media may not have initial concerns about sharing information when they have not had any major negative experience. However, users generally express disquiet with complexity of privacy settings that varies greatly across different social media sites (Madden, 2012). Facebook, in particular, has been criticized for its privacy practices (Spinello, 2011). When users experience any violation of privacy on such a platform, it exacerbates their concerns and makes them pay close attention to privacy management practices of the violating entity and its services (Nissenbaum, 2004).

Users' perception of actions taken by a platform to provide security and to eliminate privacy concerns have a huge influence on users' trust in the platform or its services. Trust-repair that involves responses, diagnosis, interventions, and evaluations are effective if they are timely and

demonstrate the ability to prevent future privacy invasion (Gillespie & Dietz, 2009). Hence, with regards to users' privacy concerns and perceived behavioral integrity in an entity/focal service we expect that:

> **Hypothesis 3A**: Users' perceived behavioral integrity of the organization (Facebook) after information misuse will increase trust needed to maintain relationship with the organization's application (Facebook.com).

3.6 Behavioral Integrity and Trust Spillover Effects

Individual trust in service or product is determined by their subjective assessment of the consistency between words and actions of the service entity (Simons, 2002). The implementation of sufficient trust-repair actions promote honesty when the actions are in support of the claims in an apology (Eberl, Geiger, & Aßländer, 2015). Actions taken by the violating entity would aim to assure users that they are competent in protecting them and providing services of higher quality for all their products. Any exposure in one service would have negative effect on their other services. Thus, we expect that the violating entity would take steps to make all their services secure. Therefore, following an apology after misuse of information, we argue in this study that;

> **Hypothesis 3B**: Users perceived behavioral integrity of the organization (Facebook) will increase trust needed to maintain relationship with the organization's affiliate applications (e.g., Instagram, WhatsApp, etc.).

3.7 Privacy Concerns and Trust (Focal Social Media)

Social media privacy concerns affect use of the online platform (Chen et al., 2016). Apology could change users' attitude with respect to privacy concerns. Once trust is stimulated after an infraction, it can lead to more trust. An apology should be followed with increase privacy control for the users. This should lower privacy concerns (Stern & Kumar, 2014). Reduction in privacy concerns should translate to increase trust in the social media. This is because, the admittance of guilt by the social media platform through an apology is an indication that steps would be taken to prevent future infractions on privacy. Facebook's ability to secure user information influences the future privacy outlook. Following an apology, we expect that:

> **Hypothesis 4A**: Users' perceived privacy concerns will be negatively associated with trust needed to maintain relationship with the organization's application (Facebook.com).

3.8 Privacy Concerns and Trust Spillover Effects

The preceding discussion considers the direct effect of privacy concerns after privacy breach has been publicly announced. However, we argue here that apology has an indirect effect on concerns about other services provided by the violating entity. An attempt at understanding spillover effects of apology is essential to evaluate its overall efficacy in crisis communication management. When social media users are affected by actions of a platform, trust in the focal social medium would have carryover effects on other services by the same provider. Increase in trust in the focal social medium play an important role in how users interpret the actions of the entity in other services provided. For example, the CEO of WhatsApp, a social media platform owned by Facebook, resigned partly due to privacy concerns arising out of the Cambridge Analytica-Facebook crisis. Given that rebuilding trust is a difficult challenge and some policies affect user behavior even after they have been replaced, following an apology, we postulate that:

> **Hypothesis 4B**: Users' perceived privacy concerns with the organization (Facebook) will be negatively associated with trust in the organization's affiliate applications (e.g., Instagram, WhatsApp, etc.).

Figure 1 summarizes our hypotheses and conceptual research model

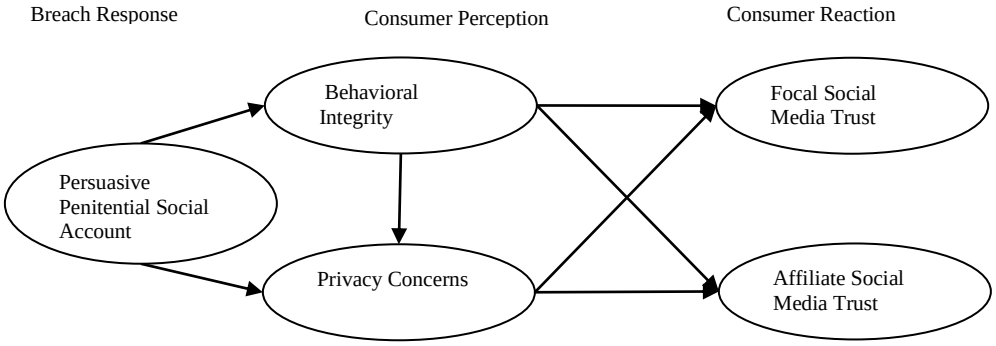

Fig. 1: Conceptual Research Model

4 Methodology

In order to empirically test the hypotheses and evaluate the proposed model in Figure 1, data was collected using a survey instrument. This methodology was selected in order to measure the perceptions of individuals (Facebook Account Holders) regarding the constructs of interest. The sub-sections that follow describe the sample and measures employed for the study.**4.1 Participants and Data Collection** We tested our conceptual model using the items presented in Appendix B. We collected data by administering a web-based questionnaire survey to Facebook

account holders using Amazon MTurk, which was deemed appropriate since our target respondents have experience of the research context. The survey was limited to users in North America to limit any confounds with respect to access to Facebook's apology. Following (Lowry, D'Arcy, Hammer, & Moody, 2016), we included attention-trap questions such as "George W. Bush is the current president of the US. T/F" and we also reverse coded PC4 and AT5 during the survey deployment. to ensure we obtain sincere responses as much as possible. A total of 432 Facebook account holders responded to an IRB Approved online survey over a three-week period in spring 2018. In the end, a sample of 411 usable questionnaires were received after dropping incomplete responses or respondents who did wrongly answer our attention question. Of the 411 respondents in the final sample, 50.6 percent were females, and 49.4 percent were males. Most of our respondents are in the 20 to 77--age range with a mean age of 36.5. The average length of users' Facebook experience was 8.6 years. To control for the potential negative effect of non-response bias on the generalizability of our result, we compared respondents of the first week to the rest of the two weeks on key indicators – age and Facebook experience. We carried out an analysis of variance (ANOVA) between respondents in week 1 and respondents in week 2-3, the f result was not significant. Thus, we are confident that our sample did not differ from the Facebook users who did not respond to the survey request MTurk.

Table 1
Sample Demographics

		N
Gender	Male	203 (49.4%)
	Female	208 (50.6%)
Age	Mean	36.5
	Minimum	20
	Maximum	77
Experience using Facebook	Mean	8.6
	Minimum	1
	Maximum	12

4.2 Measures

The research model includes five constructs. Each construct was measured with multiple items adapted from the extant literature to improve content validity (Bansal & Zahedi, 2015; Chellappa & Sin, 2005; Lowry, Clay, Bennett, & Roberts, 2015; Simons, Friedman, Liu, & McLean Parks, 2007). The survey instrument was first reviewed by five doctoral students and two faculty with interest and expertise in privacy research for content and face validity. The

revised survey instrument was validated with 22 undergraduate students who are Facebook users to ascertain the readability of the items. Table 2 lists the operational definitions of the constructs.

4.2.1 Dependent Variables

Trust: Lowry et al., (2015) suggest that trust can be operationalized at different levels for the same entity; Focal Social Media Trust (FT) can be measured based on how users perceive the operator of Facebook application actions to be beneficial, favorable and not detrimental to their interest as users. To measure FT, we used five Likert scale items adapted from Lowry et al., (2015). Items presented participants with statements regarding the degree of confidence in Facebook's social media application (see Appendix B). Participants then rated their agreement with the statement ranging from 1 (strongly disagree) to 7 (strongly agree). Exploratory factor analysis (EFA) was conducted on the items and one item was dropped due to low loadings; mean = 2.74, SD= 1.25, CR= 0.917. Affiliate Social Media Trust (AT): We used Likert-scale items to measure individual trust toward other social media applications such as WhatsApp or Instagram owned by Facebook. These items were adapted from Lowry et al., (2015). These items included statements regarding the degree participants trusted or did not trust (reverse-coded) other social media applications owned by Facebook (see Table 1). We asked participants to rate their agreement with each statement from 1 (strongly disagree) to 7 (strongly agree). Again, EFA was done to assess the items, mean= 2.67, SD=1.13, CR= 0.943.

4.2.2 Independent Variable

Persuasive Penitential Social Account (PA): Four items measured users' perceptions about the authenticity, how convincing, of Facebook's apology. The Likert-scale items were adapted from Bansal & Zahedi, (2015). Participants rated how much they agreed with the statement ranging from 1 (strongly disagree) to 7 (strongly agree). Similarly, an EFA was conducted on the items, mean= 2.4, SD= 1.18, CR=0.918.

Organizational Behavioral Integrity (BI): The items measuring perception of behavioral integrity were taken from Simons et al., (2007). Facebook users were asked to rate to what degree Facebook's actions are consistent with words they espouse post the privacy breach announcement. The measurement was a Likert-type scale of strongly disagree to strongly agree and EFA was conducted. One item was dropped because of low factor loading, mean= 2.71, SD= 1.25, CR= 0.934.

Privacy Concerns (PC): Four items measured users' level of concern over loss of privacy as a result of information disclosure to Facebook. The items were taken from Xu et al., (2011). Sample items include "following the privacy breach announcement, I am sensitive about giving out information on Facebook". EFA was done on items, mean = 1.93, SD=1.05, CR0.864.

Control Variables: We used several control variables to reduce the possibility of alternative explanations. We controlled for gender and experience using Facebook's social media application.

Table 2
Variable Operational Definition

Construct	Definition	Reference
Behavioral Integrity (BI)	The degree to which an entity such as Facebook's actions are consistent with words, they espouse	(Simons et al., 2007)
Persuasive Penitential Social Account (PA)	Users' perceptions about how convincing and authentic Facebook's apology is.	(Bansal & Zahedi, 2015)
Privacy Concerns (PC)	The concerns individuals have about access, misuse and dissemination of their personal information or over loss of privacy as a result of information disclosure to Facebook	(Chellappa & Sin, 2005) (Xu et al., 2011)
Trust	The degree to which a Facebook user's expectations, assumptions, or beliefs that Facebook's actions will be beneficial, favorable, or not detrimental	(Lowry et al., 2015)

5 Data Analysis and Results

5.1 Assessment of Measurement Validation

The measurement and the structural models were tested using structural equation modeling. Component-based partial least squares (PLS) approach was used to evaluate the psychometric properties of measurement scales and to test the research hypotheses proposed in this study. The PLS, as a component-based approach, is appropriate for this study because it focuses on prediction of data and is well suited for exploratory models and theory development. The Smart-PLS 3.0 software package (Ringle, Wende, & Becker, 2015) was used for the estimations. The measurement quality of reflective constructs was assessed by examining the reliability, and discriminant validity (see Table 3) of the measurement model (Fornell & Larcker, 1981). Since the measures of all constructs had adequate reliability and validity assessments, all the measurement items of these constructs were kept for testing the structural model. Subsequently, we estimated the structural model to test the research hypotheses. Appendix B shows the questionnaire items, as well as the descriptive statistics of all the constructs, including means, standard deviations, and the level of each item's contribution to the overall factor.

First, to ensure the individual item reliability and convergent validity of constructs, we examined factor loadings of individual measures on their respective underlying constructs, as well as the average variance extracted (AVE). All of the measurement item loadings on respective constructs were above the recommended minimum value of 0.7, indicating that at least 50 percent of the variance was shared with the construct (Chin, Marcolin, & Newsted, 2003) (see Appendix A). The AVE values for all reflective constructs were greater than the minimum recommended value of 0.50 (see diagonal of Table 3), indicating that the items satisfied convergent validity. Second, to ensure the discriminant validity of constructs in the research model, the square root of the average variance extracted (AVE) for each construct was compared with the other correlation scores in the correlation matrix. The square root of the AVE for each construct in the model, as reported in the diagonal of the correlation of constructs matrix in Table 3, was larger than the corresponding off diagonal correlations of the constructs to their latent variables. We also performed confirmatory factor analysis and examined the cross loadings of the items on other constructs and found that, as recommended, all of the measurement item loadings on the intended constructs were above 0.7 and were at least 0.1 less on their loadings on other constructs (Straub, Boudreau, & Gefen, 2004) (See Appendix B). To confirm the scale reliability and internal consistency of the constructs in the research model, we calculated the composite reliability (Fornell & Larcker, 1981). A composite reliability values of 0.7 or greater is considered acceptable (Nunnally, Bernstein, & Berge, 1967; Nunnally et al., 1967); as reported in Appendix B, the composite reliability values for all of the constructs in the research model were greater than 0.80, demonstrating that all constructs had adequate reliability assessment scores.

If the independent and dependent variables in a study are not obtained from different sources and are not measured in different contexts, common method bias can be a potential threat to the study (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003). This study employed two techniques to estimate if the effect of common method variance (CMV) – which is a function of the methods employed to measure the independent and dependent variables – was a threat to the validity of the study results. In the first approach, Harman's single factor test was conducted (Podsakoff et al., 2003). All items were loaded onto a single factor in an exploratory factor analysis without rotation. The test showed that the factor that accounted for largest variance extracted 39.78%, providing evidence that common method bias was not present based on this test. Common

method bias is considered an issue when one single factor accounts for the majority (0.50) of the covariance among the variables. The second approach employed was the marker variable approach. In this study, Blue attitude (Simmering, Fuller, Richardson, Ocal, & Atinc, 2015) was used as the marker variable, as it was assumed to be theoretically unrelated to other variables in the study. The correlations between Blue Attitude and PA, BI, PC, AT and FT were are 0.19, 0.23, 0.03, 0.21 and 0.28 respectively. These correlations are lower than the recommended threshold (0.3). This provides evidence that our results are not threatened by common method bias in the measurement of our dependent and independent variables.

Table 3
Discriminant Validity

Construct	AT	BI	FT	PA	PC
Allied Services Trust (AT)	0.877				
Behavioral Integrity (BI)	0.626	0.882			
Focal Social Media Trust (FT)	0.704	0.853	0.858		
Penitential Account (PA)	0.582	0.808	0.777	0.861	
Privacy Concerns (PC)	-0.148	-0.189	-0.190	-0.169	0.784

Note: Diagonal elements in brackets are the square root of the Average Variance Extracted (AVE). Off-diagonal elements are the correlations among latent constructs all with p<0.01

To validate these items before testing the model, we conducted a Confirmatory Factor Analysis (CFA) using Mplus 7.11 (Muthén & Muthén, 2005) software. This co-variance-based SEM estimation allows us to obtain model fit indices to assess the adequacy of the measurement model. The results of the CFA analysis (see Appendix D) in Mplus show that our measurement model exhibited sound psychometric properties (CFI=0.993, TLI=0.992, RMSEA= 0.047 and Chi/dff = 1.9).

5.2 Structural Model Testing and Results

As proposed in our research methodology, the measurement of the structural model was estimated using the PLS approach to structural equation modeling. The PLS algorithm and the bootstrapping re-sampling method with 411 cases and 1,000 re-samples were used to estimate the structural model. The results of the model estimation, including standardized path coefficients, significance of the paths based on a two-tailed t-test, and the amount of variance explained (R2), are presented in Figure 2. Based on the significant path coefficients (Table 4), most of our hypotheses involving behavioral integrity were supported ($p < 0.01$). Approximately

65 percent of the variance is explained for behavioral integrity by the perceived persuasiveness or appeal of the apology. While behavioral integrity and privacy concerns constructs explain 39 percent of the variance in trust in affiliate social media product, they explain 73 percent of the variance in the focal social media (Facebook).

We conducted model robustness checks for multicollinearity. Variance inflation factor (VIF) values of perceived trust in affiliate social media (1.037), Trust in Facebook (1.037), perceived privacy concerns (2.881), and behavioral integrity (1.000) were at satisfactory levels as they were below the recommended threshold of 5 (Hair, Black, Babin, & Anderson, 2010). Thus, indicating multicollinearity was not a serious threat to the robustness of our results.

In support of Hypothesis 1a, persuasiveness of the apology has a significant positive impact on perception behavioral integrity ($b = 0.82$, $p<0.01$). Hypothesis 2 states that the persuasiveness of the apology is negatively related to privacy concerns perception. This hypothesis was not supported ($b = -0.02$, $p >0.05$). The results may provide insight as to why social media users such as Facebook account holders are still using social media and disclosing their private information despite the announcement of the privacy invasion by Cambridge Analytica. However, in support of hypothesis 2, the results show that behavioral integrity is negatively associated with social media users' privacy concerns ($b = -0.18$, $p<0.05$). Hypotheses 3a and 4a predicted a significant effect of behavioral integrity on trust in focal social media (Facebook) and affiliated social media respectfully. These hypotheses were supported ($b = 0.88$, $p<0.01$ and $b=0.63$, $p<0.001$ respectfully). Results indicate that when behavioral integrity perception is high, individuals have high trust in the social media platform and its allied services. Our last set of hypotheses (H3b and 4b) were not supported ($b = -0.03$, $p>0.05$ and $b=-0.03$, $p>0.05$ respectfully). This suggests that privacy concerns did not play important role in social media users' trust after an apology was offered. The results are summarized in Table 4 below. The results provide richer information on the distinctive effect of privacy concerns.

Table 4
Hypothesis Testing Results Using PLS

Hypotheses	Path Coefficient	t-statistic	P-Value	Supported/Not supported
H1a	0.820	42.534	0.000	Supported
H1b	-0.018	0.200	0.824	Not Supported
H2	-0.184	2.067	0.039	Supported
H3a	0.879	63.495	0.000	Supported
H3b	0.631	16.754	0.000	Supported
H4a	-0.025	0.983	0.326	Not Supported
H4b	-0.026	0.717	0.473	Not Supported
Controls				Significant/Not significant

Experience → FT	-0.040	1.744	0.085	Significant
Experience → AT	-0.010	0.403	687	Not significant
Gender → FT	0.000	0.007	0.995	Not significant
Gender → AT	0.059	1.538	0.124	Not significant

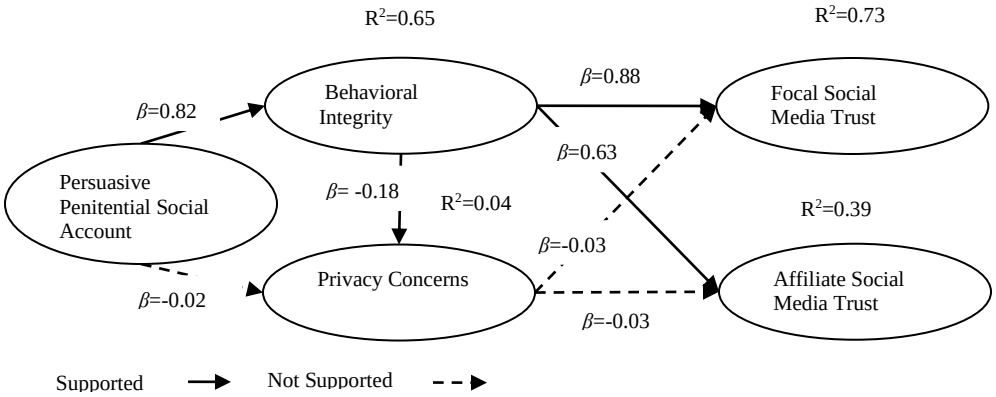

Fig 2: Research Model with results

Table 5
Summary of Hypotheses

	Hypotheses Statement	Supported/Not Supported
H1a	Persuasive apology (penitential social account) for information misuse positively influence their perceived behavioral integrity needed to maintain relationship with the organization (Facebook).	Supported
H1b	Persuasive apology (penitential social account) for information misuse will decrease perceived privacy concerns with the organization (Facebook).	Not supported
H2	Users' perceived behavioral integrity of the organization (Facebook) after information misuse is negatively associated with perceived privacy concerns.	Supported
H3a	Users' perceived behavioral integrity of the organization (Facebook) after information misuse will increase trust needed to maintain relationship with the organization's application (Facebook.com).	Supported
H3b	Users' perceived behavioral integrity of the organization (Facebook) after misuse of information will increase trust needed to maintain relationship within the organization's affiliate applications (e.g., Instagram, WhatsApp, etc.).	Supported
H4a	Users' perceived privacy concerns will be negatively associated with trust needed to maintain relationship with the organization's application (Facebook.com).	Not supported
H4b	Users' perceived privacy concerns with the organization (Facebook) will be negatively associated with trust in the organization's affiliate applications (e.g., Instagram, WhatsApp, etc.).	Not supported

5.3 Post-hoc Analysis – Mediation Effects

We further investigated hypotheses H1a, H3a & b to assess the extent to which penitential account affect trust in Facebook and its allied services, and privacy concerns. We conducted a Sobel test for mediation following the recommendation of (Hair Jr, Anderson, Tatham, & William, 1995) using equation 1 to examine the significance of the indirect path.

$$\text{z-value} = \beta_a * \beta_b / \text{SQRT}(\beta_b^2 * SE_a^2 + \beta_a^2 * SE_b^2) \quad (1)$$

We included two additional paths that examine the direct effects of penitential account to our two dependent variables. Both direct path (PA -> FT, β=0.22, p=0.00) and indirect path (PA -> BI -> FT, β =0.58, p=0.00) were significant for Focal social media trust. Thus, suggesting that organizational behavioral integrity partially mediate the effect of penitential account on focal social media trust. Similarly, organizational integrity was found to partially mediate the effect of penitential account on affiliate social media trust (PA -> AT, β =0.17, p=0.0.03; PA -> BI -> AT, β =0.41, p=0.00). With respect to privacy concerns, the indirect effect (PA -> BI -> PC, β =-0.151, p=0.045) of penitential account on privacy concerns was significant while the direct effect (PA -> PC, β =-0.02, p=0.85) was found to be insignificant. This suggest that organization behavioral integrity fully mediates the relationship between social penitential account and privacy concerns post privacy breach announcement.

6 Discussion

This study sets out to answer questions regarding post privacy violation crisis management in social media context, understanding what underlies management effort to reduce users' privacy concerns, increase trust and maintain users of their social media platforms. Our conceptual model suggested a two-stream process of penitential social account's (apology) influence on rebuilding violated trust. We postulated that the persuasiveness of an apology affects the building of trust through confidence increment in the behavioral integrity of the violating entity and reduction in users' privacy concerns. The estimation results underline the significant influence of behavioral integrity on trust repair in the focal social media platform and allied services or products. An entity such as Facebook has built a solid reputation over the past decade and admitting they were complacent requires great strength of magnanimity and acceptance of vulnerability. Our mixed results demonstrate that apology has mixed results, confirming findings in prior literature that apology may lead to unintended results (Stamato, 2008). Offering an apology could serve to gain credibility and generate confidence. In the context of this study, it was found that the persuasiveness of the apology positively influences users' confidence in the degree of the alignment between the violating organizations words and deeds. This is consistent with actions of business leader which suggest that an apology followed by an action plan that is honest, gives users the impression that the entity is in control of the process of reestablishing credibility (Sterling, 2017). Apologies reflect an entity's ethical domain and affect their

behavioral integrity (Ghoshal, 2005; Lee & Tiedens, 2001). However, in crisis communication, apology may not lead to the ultimate results (Coombs & Holladay, 2008). An apology makes an entity vulnerable and does not lead to the elimination of suspicion. In the context of this study, the estimation results show that although the persuasiveness or appeal of apology could lead to increase behavioral integrity, it does not influence users concerns about access, misuse and dissemination of their personal information on the social platform. The mediating role of behavioral integrity further explain the underlying mechanism that link the persuasive power of an apology to the process of rebuilding trust and alleviating concerns. Alleviation of users concerns has the added advantage of encouraging users to opt into protective services usually offered after privacy violation.

The insignificance of persuasiveness of an apology as a predictor of privacy concerns and privacy concerns as a predictor of both forms of trust was unexpected. Privacy concerns are complex and entity/context-specific (Kehr, Kowatsch, Wentzel, & Fleisch, 2015). Privacy in the social media era is more complex because of the involvement of multiple parties and the nature of data disclosure. One possible explanation for the insignificance could be, after active presence on social media, users may care less about exercising their control of privacy. This leads to inconsistency between user behavior and their beliefs or concerns about privacy. Thus, the finding is consistent with privacy paradox literature (Brandimarte, Acquisti, & Loewenstein, 2013). Despite potential privacy violations, social media have become an indispensable part of life for millions of people decreasing the likelihood of complete degradation in trust (Dinev & Hart, 2006). Although, social media users may consider their exposure to the platform in the calculus of their privacy concerns, it does not affect their future outlook of the firm (Gutierrez, O'Leary, Rana, Dwivedi, & Calle, 2019). Some individuals' response to privacy threats through mental disengagement as a coping response (Jung & Park, 2018). This confirms why majority of Facebook and other social media users including Instagram users visit these platforms daily.

7 Implications

7.1 Implications for Research

The results of our study have implications for research and practice. We demonstrate that apology works on restoring violated trust and reducing users' concerns through behavioral integrity, in the context of social media. Prior research (e.g. Bansal & Zahedi 2015) suggest that,

the type of social account affects repaired trust. Our results demonstrate the intricate process through which penitential social account affect trust repair. It does so through violated users' perception of the degree of alignment between words and actions of the violating entity.

Additionally, consistent with prior research (Bansal & Zahedi, 2015), privacy concerns have no effect on users repaired trust. However, users' concerns are heavily influenced by their perceptions of the entity's behavioral integrity. This may explain why we do not observe any decreasing trend in the use of social media despite the sensational nature of the recent discovery of privacy violations on Facebook. When an apology increases users' perception of the entity's integrity, it may reduce any privacy concerns and dampen its effect on the trust repair process. It may cause users' not to attribute any blame to the violating entity, thus making concerns about privacy inconsequential to their trust rebuilding process.

To the best of our knowledge, this is the first study that has investigated the spillover effects of violated trust. We postulate that when users experience any violation from using an organization's service or product, it might affect users' trust in other services provided by the same organization. The estimation results, indeed, show that words and actions of an organization with respect to a product/service affect users' perception of other services provided. In this study's context, we suggest that users' perception of behavioral integrity of Facebook and their privacy concerns would have a spillover effect on their perception about other affiliate social medium brands such as WhatsApp and Instagram. Thus, behavioral integrity affects an entity and possibly its portfolio of products and services. This is consistent with prior findings that posit that corporate integrity image and provision of sufficient information influence consumers' judgment about a firm's and its services (Xie & Peng, 2009).

Finally, our theorizing of 'breach response–consumer perception–consumer reaction' explicitly contributes to the causal-chain framework of social media research, which essentially consider put forth by (Ngai, Tao, & Moon (2015). In a systematic review of theories and conceptual frameworks employed by social media studies Ngai et al., (2015) report how this framework expresses the different inter-relationships of antecedents, mediators, moderators and outcome dimensions and constructs that link to causes and results of user behavior in the social media adoption. Notably the context of application may reposition the constructs. In our response-perception-reaction framework, we see how breach response which qualifies as outcome variable is operationalized as an input variable. We have also explained the mediating

role of constructs backed by strong empirical assessments which strengthens the validity of causal-chain (Ngai et al., 2015) in our arguments.

7.2 Implication for Design of Trust Repair Mechanisms

We utilized the context of Facebook as a social media brand or organization which is one of the top three most targeted contexts for social media research (Kapoor et al., 2018). Thus, our findings offer key insights for practice. The results highlight the effects of ex-ante apology in crisis communication for business leaders. Managers should consider the persuasiveness or appeal of their messages following a crisis on recipients' judgement of the entity's actions and reactions. The nature as well as the medium of crisis communication play crucial roles in rebuilding violated trust (Schultz, Utz, & Göritz, 2011). Although, an organization may choose channels (such as the Washington Post) to offer an apology, it is equally important that whatever items that are spelled out in an apology statement should be such that they are actionable in the eyes of the victim and the organization must be seen to be executing those actions. Such a behavior by the organization, although may not alleviate users' concerns, would restore trust in the organization's services. This would enable users to maintain relationship with the organization. When a privacy breach occurs, it appears the focus of organizations is to reassure victims of the security of their technologies and limited scope of the impact. However, the results indicate that the degree of alignment between the words of organizations and subsequent actions is key to ensuring users do not terminate their membership of the social media platform. The alignment which is an indication of the organization's BI contribute to fair information practices promoted by Federal Trade Commission (FTC) as effective communication for concerned parties in this era of increased user data collection. Regarding privacy concerns, our results it suggests that companies may need to intensively analyze customers' perception about the company actions and privacy concerns. Privacy concerns are key to using technology including social media (Wang & Herrando, 2019). Our findings imply that social media users' privacy behaviors are intricately tied to the words and actions of the social media platform and not statements issues after discovery of privacy violations. Thus, managers need to take various privacy concerns and their related affects into account when developing customer strategies. For example, when users have their private information inappropriately gathered and used, an apology may be interpreted as only in compliance with response to regulatory requirements.

However, the social media platform operates on users' trust and may need to take a different approach to users whose main concern is actions taken to restore trust.

The results of our study also suggest that managers need to make considerable efforts to mitigate loss of trust in their allied services. Most social media platforms enjoy the network effects resulting from operating multiple social media platforms. Convincing media users that company cares about fairness in dealing with their data collected on its platforms is critical for the success of the businesses model (Jung & Park, 2018). When the platform offers an apology for data breach on one of its services, the actions stated in the apology must be seen to lead to protecting users' data on all their services. For example, social media platform's public relations activities following a data breach must be comprehensive and should affect all services being offered.

8.0 Conclusion

Our study provided a theoretical background into investigating the mechanism of trust repair following a breach in the social media context. This study considers the effect of apology following data breach, on trust repair in social media context. Using survey responses of actual users of Facebook who have read Facebook's Apology, we found that behavioral integrity plays a critical as intervening factor between the persuasiveness of an apology and trust. Additionally, we found that while behavioral integrity affects privacy concerns, users' privacy concerns that not impact trust in the social media context. Our finding open avenue into post data breach crisis communication research, with potential for enlightening practitioners regarding mechanism for maintain users after crisis.

8.1 Limitations and Future Research Directions

Like all studies of this nature, this study is not without limitations. We only examined the effect of one dimension of social account (penitential/apology). Future research can investigate the relative effect of this strategy against others such as denial or no response. Additionally, we relied on responses from users' memory recall of the penitential account. Although we showed them a copy of the apology, recall may not be as accurate as when events are fresh in the minds of respondents. The timing of a response has been suggested to play a critical role in trust repair (Gillespie & Dietz, 2009). Future research is required to examine the appropriate timing of an apology and its effectiveness in trust repair. We do acknowledge that trust is not stationary but changes overtime. Therefore, it will be interesting to see to the extent to which social media trust

change after apology has been offered. We plan to explore these dynamics in the future as we expand this research. Future studies may also explore the civility or incivility effects on the trust dynamics following penitential accounts. Antoci et al. (2019) report that participants exposed to civil Facebook interactions are more trusting whereas participants who experience online incivility in their use of social media showed no changes in their behavior regarding trust. Such an endeavor may advance theory on apriori factors that eventually contribute to the level of post-data-breach trust dynamics in users following an apology.

Despite the limitations, our research contributes to the literature on ethics and crisis communication. We show that the degree of persuasiveness of an apology does not only influence the focal product/service but also has profound spillover effect on other services offered by the same entity. Additionally, we considered and investigated organizational level behavioral integrity. We explicated the effect of organizational level behavioral integrity in business crisis communication.

References

Aladwani, A. M., & Dwivedi, Y. K. (2018). Towards a theory of SocioCitizenry: Quality anticipation, trust configuration, and approved adaptation of governmental social media. *International Journal of Information Management*, *43*, 261–272.

Antoci, A., Bonelli, L., Paglieri, F., Reggiani, T., & Sabatini, F. (2019). Civility and trust in social media. *Journal of Economic Behavior & Organization*, *160*, 83–99.

Bachmann, R., Gillespie, N., & Priem, R. (2015). Repairing Trust in Organizations and Institutions: Toward a Conceptual Framework. *Organization Studies*, *36*(9), 1123–1142.

Bansal, G., & Zahedi, F. M. (2015). Trust violation and repair: The information privacy perspective. *Decision Support Systems*, *71*, 62–77.

Bauer, L., Cranor, L. F., Komanduri, S., Mazurek, M. L., Reiter, M. K., Sleeper, M., & Ur, B. (2013). *The post anachronism: the temporal dimension of Facebook privacy*. 1–12.

Benbasat, I., & Wang, W. (2005). Trust in and Adoption of Online Recommendation Agents. *Journal of the Association for Information Systems*, *6*(3), 72–101.

Bies, R. J. (1987). The predicament of injustice: The management of moral outrage. In L. L. Cummings & B. M. Staw (Eds.), *Research in Organizational Behavior* (Vol. 9, pp. 289–319). Greenwich, CT: JAI Press.

Bonsón, E., Escobar, T., & Ratkai, M. (2014). Testing the inter-relations of factors that may support continued use intention: The case of Facebook. *Social Science Information*, *53*(3), 293–310.

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced Confidences: Privacy and the Control Paradox. *Social Psychological and Personality Science*, *4*(3), 340–347.

Chang, S. E., Liu, A. Y., & Shen, W. C. (2017). User trust in social networking services: A comparison of Facebook and LinkedIn. *Computers in Human Behavior*, *69*, 207–217.

Chellappa, R. K., & Sin, R. G. (2005). Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma. *Information Technology and Management*, *6*(2–3), 181–202.

Chen, H., Beaudoin, C. E., & Hong, T. (2016). Teen online information disclosure: Empirical testing of a protection motivation and social capital model. *Journal of the Association for Information Science and Technology*, *67*(12), 2871–2881.

Chin, W. W., Marcolin, B. L., & Newsted, P. R. (2003). A partial least squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation study and an electronic-mail emotion/adoption study. *Information Systems Research*, *14*(2), 189–217.

Christofides, E., Muise, A., & Desmarais, S. (2009). Information Disclosure and Control on Facebook: Are They Two Sides of the Same Coin or Two Different Processes? *Cyber Psychology & Behavior*, *12*(3), 341–345.

Confessore, N. (2018). Cambridge Analytica and Facebook: The Scandal and the Fallout So Far. *The New York Times*. Retrieved from https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

Coombs, W. T., & Holladay, S. J. (2008). Comparing apology to equivalent crisis response strategies: Clarifying apology's role and value in crisis communication. *Public Relations Review*, *34*(3), 252–257.

Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research*, *17*(1), 61–80.

Dirks, K. T., Kim, P. H., Ferrin, D. L., & Cooper, C. D. (2011). Understanding the effects of substantive responses on trust following a transgression. *Organizational Behavior and Human Decision Processes*, *114*(2), 87–103.

Eberl, P., Geiger, D., & Aßländer, M. S. (2015). Repairing Trust in an Organization after Integrity Violations: The Ambivalence of Organizational Rule Adjustments. *Organization Studies*, *36*(9), 1205–1235.

Farrell, J., & Rabin, M. (1996). Cheap Talk. *The Journal of Economic Perspectives*, *10*(3), 103–118.

Fornell, C., & Larcker, D. F. (1981). Structural equation models with unobservable variables and measurement error: Algebra and statistics. *Journal of Marketing Research*, 382–388.

Ghoshal, S. (2005). Bad Management Theories Are Destroying Good Management Practices. *Academy of Management Learning & Education*, *4*(1), 75–91.

Gillespie, N., & Dietz, G. (2009). Trust Repair after an Organization-Level Failure. *The Academy of Management Review*, *34*(1), 127–145.

Good, C. (2013, February 12). *Things Obama Always Says*. Retrieved from https://abcnews.go.com/Politics/things-obama-sotu-speech-predictions/story?id=18470162

Greenberg, J. (1990). Looking fair vs. being fair: Managing impressions of organizational justice. In L. L. Cummings & B. M. Staw (Eds.), *Research in Organizational Behavior* (Vol. 12, pp. 111–157). Greenwich, CT: JAI Press.

Gutierrez, A., O'Leary, S., Rana, N. P., Dwivedi, Y. K., & Calle, T. (2019). Using privacy calculus theory to explore entrepreneurial directions in mobile location-based advertising: Identifying intrusiveness as the critical risk factor. *Computers in Human Behavior*, *95*, 295–306.

Hair, J., Black, W., Babin, B., & Anderson, R. (2010). *Multivariate Data Analysis*.

Hair Jr, J. F., Anderson, R. E., Tatham, R. L., & William, C. (1995). *Multivariate data analysis with readings*. New Jersy: Prentice Hall.

Hallam, C., & Zanella, G. (2017). Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. *Computers in Human Behavior*, *68*, 217–227.

Jiang, Z. (Jack), Heng, C. S., & Choi, B. C. F. (2013). Research Note —Privacy Concerns and Privacy-Protective Behavior in Synchronous Online Social Interactions. *Information Systems Research*, *24*(3), 579–595.

Jung, Y., & Park, J. (2018). An investigation of relationships among privacy concerns, affective responses, and coping behaviors in location-based services. *International Journal of Information Management*, *43*, 15–24.

Kahn, C., & Ingram, D. (2018). Americans less likely to trust Facebook than rivals on personal data. *Reuters*. Retrieved from https://www.reuters.com/article/us-usa-facebook-poll/americans-less-likely-to-trust-facebook-than-rivals-on-personal-data-reuters-ipsos-poll-idUSKBN1H10K3

Kamboj, S., Sarmah, B., Gupta, S., & Dwivedi, Y. (2018). Examining branding co-creation in brand communities on social media: Applying the paradigm of Stimulus-Organism-Response. *International Journal of Information Management*, *39*, 169–185.

Kapoor, K. K., Tamilmani, K., Rana, N. P., Patil, P., Dwivedi, Y. K., & Nerur, S. (2018). Advances in Social Media Research: Past, Present and Future. *Information Systems Frontiers*, *20*(3), 531–558.

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus: Privacy calculus: dispositions and affect. *Information Systems Journal*, *25*(6), 607–635.

Kelly, H. (2018, October 17). Public Funds Back Plan to Replace Mark Zuckerberg as Facebook Chairman [News Report]. Retrieved October 22, 2018, from CNN Business website: https://www.cnn.com/2018/10/17/tech/facebook-shareholder-public-fund-proposal/index.html

Klein, K. J., & Kozlowski, S. W. J. (2000). *Multilevel theory, research, and methods in organizations: Foundations, extensions, and new directions*. San Francisco, CA, US: Jossey-Bass.

Kotler, P., & Armstrong, G. (2013). *Principles of marketing* (16th global). Pearson Education.

Kourouthanassis, P., Lekakos, G., & Gerakis, V. (2015). Should I stay or should I go? The moderating effect of self-image congruity and trust on social networking continued use. *Behaviour & Information Technology*, *34*(2), 190–203.

Külcü, Ö., & Henkoğlu, T. (2014). Privacy in social networks: An analysis of Facebook. *International Journal of Information Management*, *34*(6), 761–769.

Lankton, N. K., & McKnight, D. H. (2011). What does it mean to trust Facebook?: examining technology and interpersonal trust beliefs. *ACM SIGMIS Database*, *42*(2), 32.

Lee, F., & Tiedens, L. Z. (2001). Who's Being Served? "Self-Serving" Attributions in Social Hierarchies. *Organizational Behavior and Human Decision Processes*, *84*(2), 254–287.

Lount, R. B., Zhong, C.-B., Sivanathan, N., & Murnighan, J. K. (2008). Getting Off on the Wrong Foot: The Timing of a Breach and the Restoration of Trust. *Personality and Social Psychology Bulletin*, *34*(12), 1601–1612.

Lowry, P. B., Clay, P., Bennett, R. B., & Roberts, T. L. (2015). Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust. *Information Systems Journal*, *25*(3), 193–273.

Lowry, P. B., D'Arcy, J., Hammer, B., & Moody, G. D. (2016). "Cargo Cult" science in traditional organization and information systems survey research: A case for using nontraditional methods of data collection, including Mechanical Turk and online panels. *The Journal of Strategic Information Systems*, *25*(3), 232–240.

Madden, M. (2012, February 24). Privacy management on social media sites. *Pew Research Center Internet & Technology*.

Malhotra, Naresh K., Sung, S. K., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research*, *15*(4), 336–355.

Mamonov, S., & Benbunan-Fich, R. (2017). Exploring factors affecting social e-commerce service adoption: The case of Facebook Gifts. *International Journal of Information Management*, *37*(6), 590–600.

Miranda, S. M., Young, A., & Yetgin, E. (2016). Are social media emancipatory or hegemonic? Societal effects of mass media digitization. *MIS Quarterly*, *40*(2), 303–329.

Muthén, L. K., & Muthén, B. O. (2005). Mplus: Statistical analysis with latent variables: User's guide (Version 7.11). Los Angeles.

Näsi, M., Räsänen, P., Keipi, T., & Oksanen, A. (2017). Trust and victimization: A cross-national comparison of Finland, the U.S., Germany and UK. *Research on Finnish Society*, *10*, 13.

Ngai, E. W. T., Tao, S. S. C., & Moon, K. K. L. (2015). Social media research: Theories, constructs, and conceptual frameworks. *International Journal of Information Management*, *35*(1), 33–44.

Nissenbaum, H. (2004). Privacy as Contextual Integrity. *Washington Law Review*, *79*, 39.

Nunnally, J. C., Bernstein, I. H., & Berge, J. M. T. (1967). *Psychometric theory* (Vol. 226). New York: McGraw-Hill.

Palanski, M. E., Kahai, S. S., & Yammarino, F. J. (2011). Team Virtues and Performance: An Examination of Transparency, Behavioral Integrity, and Trust. *Journal of Business Ethics*, *99*(2), 201–216.

Palanski, M. E., & Yammarino, F. J. (2007). Integrity and Leadership: Clearing the Conceptual Confusion. *European Management Journal*, *25*(3), 171–184.

Palanski, M. E., & Yammarino, F. J. (2009). Integrity and leadership: A multi-level conceptual framework. *The Leadership Quarterly*, *20*(3), 405–420.

Parry, K. W., & Proctor-Thomson, S. B. (2002). Perceived Integrity of Transformational Leaders in Organisational Settings. *Journal of Business Ethics*, *35*, 75–96.

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, *88*(5), 879–903.

Porter, C. E., Devaraj, S., & Sun, D. (2013). A test of two models of value creation in virtual communities. *Journal of Management Information Systems*, *30*(1), 261–292.

Publilius, S. (2018). *Quotable Quote*. Retrieved from https://www.goodreads.com/quotes/503006-trust-like-the-soul-never-returns-once-it-is-gone

Ringle, C. M., Wende, S., & Becker, J.-M. (2015). *SmartPLS 3. Bönningstedt: SmartPLS*. Retrieved from http://www.smartpls.com

Robert Jr, L. P., & You, S. (2018). Are you satisfied yet? Shared leadership, individual trust, autonomy, and satisfaction in virtual teams. *Journal of the Association for Information Science and Technology*, *69*(4), 503–513.

Schultz, F., Utz, S., & Göritz, A. (2011). Is the medium the message? Perceptions of and reactions to crisis communication via twitter, blogs and traditional media. *Public Relations Review*, *37*(1), 20–27.

Shiau, W.-L., Dwivedi, Y. K., & Lai, H.-H. (2018). Examining the core knowledge on facebook. *International Journal of Information Management*, *43*, 52–63.

Simmering, M. J., Fuller, C. M., Richardson, H. A., Ocal, Y., & Atinc, G. M. (2015). Marker Variable Choice, Reporting, and Interpretation in the Detection of Common Method Variance: A Review and Demonstration. *Organizational Research Methods*, *18*(3), 473–511.

Simons, T. (2002). Behavioral Integrity: The Perceived Alignment Between Managers' Words and Deeds as a Research Focus. *Organization Science*, *13*(1), 18–35.

Simons, T., Friedman, R., Liu, L. A., & McLean Parks, J. (2007). Racial differences in sensitivity to behavioral integrity: Attitudinal consequences, in-group effects, and "trickle down" among Black and non-Black employees. *Journal of Applied Psychology*, *92*(3), 650–665.

Son, & Kim. (2008). Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model. *MIS Quarterly*, *32*(3), 503-529.

Spinello, R. A. (2011). Privacy and Social Networking Technology. *International Review of Information Ethics*, *16*, 41-6.

Stamato, L. (2008, August). Should Business Leaders Apologize? Why, When And How An Apology Matters. *Ivey Business Journal*, *72*(4), 1–8.

Sterling, K. (2017, November 6). Why You Should Never Write "I'm Sorry" to Consumers and Clients. *Inc.Com*.

Stern, T., & Kumar, N. (2014). Improving privacy settings control in online social networks with a wheel interface: Improving Privacy Settings Control in Online Social Networks with a Wheel Interface. *Journal of the Association for Information Science and Technology*, *65*(3), 524–538.

Straub, D., Boudreau, M.-C., & Gefen, D. (2004). Validation guidelines for IS positivist research. *The Communications of the Association for Information Systems*, *13*(1), 380–427.

Tomlinson, E. C., Dineen, B. R., & Lewicki, R. J. (2004). The Road to Reconciliation: Antecedents of Victim Willingness to Reconcile Following a Broken Promise. *Journal of Management*, *30*(2), 165–187.

Tomlinson, E. C., & Mayer, R. C. (2009). The Role of Causal Attribution Dimensions in Trust Repair. *The Academy of Management Review*, *34*(1), 85–104.

Tow, W. N. F. H., Dell, P., & Venable, J. (2010). Understanding information disclosure behaviour in Australian Facebook users. *Journal of Information Technology*, *25*(2), 126–136.

Wang, Y., & Herrando, C. (2019). Does privacy assurance on social commerce sites matter to millennials? *International Journal of Information Management*, *44*, 164–177.

Weiss, S. (2009). Privacy threat model for data portability in social network applications. *International Journal of Information Management*, *29*(4), 249–254.

White, J. B., & Sharman, J. (2018, April 30). *Billionaire WhatsApp co-founder Jan Koum quits amid Facebook privacy scandal*. Retrieved from https://www.independent.co.uk/news/business/jan-koum-whatsapp-leaving-cofounder-facebook-privacy-a8330256.html

Xie, Y., & Peng, S. (2009). How to repair customer trust after negative publicity: The roles of competence, integrity, benevolence, and forgiveness. *Psychology & Marketing*, *26*(7), 572–589.

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances. *Journal of the Association for Information Systems*, *12*(12), 798–824.

Appendix A – Items loadings and cross-loadings

Items loadings and cross-loadings

	AT	BI	FT	PA	PC
AT1	0.896	0.585	0.641	0.552	-0.156
AT2	0.813	0.476	0.571	0.431	-0.107
AT3	0.891	0.568	0.619	0.496	-0.153
AT4	0.897	0.561	0.625	0.538	-0.144
AT5	0.883	0.545	0.629	0.524	-0.081
BI1	0.542	0.871	0.721	0.699	-0.159
BI2	0.542	0.896	0.753	0.726	-0.155
BI4	0.535	0.891	0.758	0.720	-0.149
BI5	0.589	0.871	0.778	0.705	-0.204
FBT2	0.552	0.667	0.812	0.586	-0.079
FBT3	0.652	0.777	0.878	0.676	-0.215
FBT4	0.638	0.784	0.892	0.748	-0.172
FTB5	0.566	0.691	0.846	0.648	-0.175
PA1	0.536	0.726	0.700	0.930	-0.147
PA2	0.509	0.736	0.711	0.905	-0.166
PA3	0.360	0.477	0.469	0.666	-0.085
PA4	0.568	0.795	0.754	0.914	-0.166
PC1	-0.129	-0.123	-0.143	-0.126	0.744
PC2	-0.106	-0.114	-0.106	-0.100	0.779
PC3	-0.094	-0.172	-0.170	-0.166	0.833
PC4	-0.133	-0.172	-0.164	-0.128	0.778

Appendix B– Items, Composite Reliability (CR), Factor Loadings

Items	Construct and Items	Mean	Std	Loading
	Persuasive Penitential Social Account (PA): CR=0.918			
PA1	The apology by Facebook is sincere	2.41	1.16	0.930
PA2	The extent to which I believe the apology of Facebook is high	2.57	1.25	0.906
PA3	The apology from Facebook is very professional	2.07	1.06	0.619
PA4	I believe that Facebook's apology is genuine	2.55	1.24	0.945
	Behavioral Integrity (BI): CR=0.934			
BI1	There is a match between Facebook's words and actions	2.63	1.22	0.856
BI2	Facebook delivers on promises	2.71	1.22	0.893
BI3	Facebook practices what it preaches	2.81	1.27	-
BI4	Facebook does what they say they will do	2.67	1.22	0.918
BI5	Facebook conduct business by the same values they espoused	2.78	1.24	0.878
BI6	I am certain Facebook will keep their promise after their apology	2.66	1.32	0.878
	Privacy Concerns (PC): CR=0.864			
PC1	I am sensitive about giving out information on Facebook	1.76	0.96	0.706
PC2	I am concerned about anonymous information (information collected automatically but which cannot be used to identify me, such as my computer or operating system) that is collected about me	2.08	1.11	0.796
PC3	I am concerned about how my personally unidentifiable information (information that I have voluntarily given out but cannot be used to identify me, e.g., postal code, age range, sex) will be used by Facebook	2.10	1.11	0.873
PC4	I am concerned about how my personally identifiable information (information that I have voluntarily given out and can be used to identify me as an individual, e.g., name, shipping address, credit card) will be used by Facebook	1.78	1.00	0.739
	Focal Social Media Trust: CR=0.917			
FT1	I believe Facebook has high honor.	2.85	1.35	-
FT2	I can expect Facebook to treat me in a consistent and predictable fashion.	2.53	1.14	0.763
FT3	Facebook is always reliable and truthful.	3.01	1.36	0.892
FT4	In general, I believe Facebook's motives and intentions are good.	2.66	1.26	0.900
FT5	I do think Facebook treats me fairly.	2.65	1.15	0.812
	Affiliate Social Media Trust: CR=0.943			
AT1	I believe social media platform such as Instagram and WhatsApp have high honor.	2.76	1.15	0.909
AT2	I can expect social media platform such as Instagram and WhatsApp to treat me in a consistent and predictable fashion.	2.45	1.09	0.779
AT3	Social media platform such as Instagram and WhatsApp are always reliable and truthful.	2.9	1.16	0.895
AT4	In general, I believe social media platform such as Instagram and WhatsApp motives and intentions are good.	2.64	1.13	0.901
AT5	I do think social media platform such as Instagram and WhatsApp treat me fairly.	2.61	1.10	0.881
	Control Variables Gender: Male……Female…….. Age (please enter your age in years):_____			

	Education The highest degree of education I have received till date: High school…….. Bachelor's Degree…….. Graduate…… Experience How long have you been using Facebook…….. Have you used Instagram….WhatsApp….			

Appendix C – Sample Facebook Apology

A26 THE WASHINGTON POST · SUNDAY, MARCH 25, 2018

ADVERTISEMENT

ADVERTISEMENT

We have a responsibility to protect your information. If we can't, we don't deserve it.

You may have heard about a quiz app built by a university researcher that leaked Facebook data of millions of people in 2014. This was a breach of trust, and I'm sorry we didn't do more at the time. We're now taking steps to make sure this doesn't happen again.

We've already stopped apps like this from getting so much information. Now we're limiting the data apps get when you sign in using Facebook.

We're also investigating every single app that had access to large amounts of data before we fixed this. We expect there are others. And when we find them, we will ban them and tell everyone affected.

Finally, we'll remind you which apps you've given access to your information – so you can shut off the ones you don't want anymore.

Thank you for believing in this community. I promise to do better for you.

Mark Zuckerberg

Facebook Apology from the Washington Post

Appendix D: CFA for research model

	Estimate (Est.)	S.E.	Est./S.E.
AT1	0.909	0.012	78.757
AT2	0.779	0.021	36.719
AT3	0.895	0.012	72.532
AT4	0.901	0.013	70.212
AT5	0.881	0.012	71.724
BI1	0.856	0.018	47.446
BI2	0.893	0.012	75.519
BI3	0.918	0.01	91.61
BI4	0.878	0.014	64.644
BI5	0.878	0.013	65.46
FBT2	0.763	0.022	35.344
FBT3	0.892	0.013	67.988
FBT4	0.900	0.011	78.992
FTB5	0.812	0.018	43.978
PA1	0.930	0.009	101.448
PA2	0.906	0.011	80.246
PA3	0.619	0.034	18.142
PA4	0.945	0.009	108.168
PC1	0.706	0.037	18.898
PC2	0.796	0.031	25.39
PC3	0.873	0.028	31.318
PC4	0.739	0.036	20.382
Fit Indices			
X^2/diff	377.44/199 = 1.9		
CFI	0.993		
TLI	0.992		
RMSEA	0.047		