1-2020

Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective

Mohsen Jozani
University of Texas at San Antonio

Emmanuel Wusuhon Yanibo Ayaburi
The University of Texas Rio Grande Valley, emmanuel.ayaburi@utrgv.edu

Myung Ko
The University of Texas Rio Grande Valley

Kim-Kwang Raymond Choo
University of Texas at San Antonio

Recommended Citation

Jozani, Mohsen, Emmanuel Ayaburi, Myung Ko, and Kim-Kwang Raymond Choo. 2020. "Privacy Concerns and Benefits of Engagement with Social Media-Enabled Apps: A Privacy Calculus Perspective." Computers in Human Behavior 107 (June): 106260. https://doi.org/10.1016/j.chb.2020.106260.

Examination of Social Media Enabled Apps Engagement Conundrum: A Privacy Calculus Perspective

1. Mohsen Jozani, Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, TX 78249, USA, Email: mohsen.jozani@utsa.edu
2. Emmanuel Ayaburi, Department of Information Systems, University of Texas Rio Grande Valley, Edinburg, TX 78539, USA, Email: emmanuel.ayaburi@utrgv.edu
3. Myung Ko, Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, TX 78249, USA, Email: Myung.Ko@utsa.edu
4. Kim-Kwang Raymond Choo, Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, TX 78249, USA, Email: raymond.choo@fulbrightmail.org

Privacy Concerns and Benefits of Engagement with Social Media-enabled Apps: A Privacy Calculus Perspective

ABSTRACT: Privacy threats in a social media-enabled application (app) can originate from either the institution or other app users. Although privacy in social media is well studied, the role of social (peer) privacy concerns is largely unknown and most privacy studies on mobile apps focus on initial adoption and ignore long-term behavioral outcomes. Drawing on the privacy calculus theory, this study examines the impact of both institutional and social privacy concerns on long-term user engagement with social media-enabled apps. Findings from the analysis of 354 survey responses reveal that both institutional and social privacy concerns decrease engagement. Regarding the antecedents, the perceived sensitivity of information increases institutional privacy concerns. However, social privacy concerns is influenced by the perception of risk and control. Moreover, while the impacts of social and enjoyment benefits are expectedly positive, the perception of efficiency benefits decreases engagement. These findings are further investigated and validated through a follow-up text analysis study, suggesting that users who enjoy the functionality of these apps are more likely to express social privacy concerns and minimize their engagement. This study contributes to the literature of privacy on mobile apps by unraveling the intricate dynamics of privacy concerns and benefits in the social mobile era.

KEYWORDS: privacy concerns, privacy calculus, engagement, social media-enabled apps, social mobile era

1. Introduction

In our interconnected digitalized society, individuals are increasingly willing to share their information, often publicly, to enjoy the convenience of online services (Cavusoglu et al., 2016; Trepte et al., 2020). However, such increasing levels of connectedness via smart mobile devices and social media engagement have resulted in corresponding increased risks of privacy violations (Crossler and Bélanger, 2019; Gerhart and Koohikamali, 2019; Gu et al., 2017).

Privacy is a context-dependent, multidimensional and dynamic concept that evolves with technological advancements (Acquisti et al., 2015; Hong and Thong, 2013; Smith et al., 2011; Westin, 2003). In recent years, the means of accessing the Internet has shifted from personal computers to mobile devices which account for approximately 55 percent of total Internet use in the United States in 2019 (Statcounter, 2019). Contemporary mobile (including wearable and embedded) devices have inbuilt sensors that collect data, ranging from users' social life (e.g., timestamped location data) to sleeping patterns and other geospatial data. Such data are sent to mobile device manufacturers and app developers, in exchange for enhancing user experience and offering personalized advertisements (Gal-Or et al., 2018). More than 70 percent of mobile apps reportedly share user data with third-party companies (Vallina-Rodriguez and Sundaresan, 2017). Furthermore, the trend of having multifunctional and social-media enabled apps, such as social learning, social fitness, social health, and social payment apps, has exacerbated users' privacy concerns. These issues may require a revisit of the conceptualization of privacy concerns. In the Information Systems (IS) literature, Concerns For Information Privacy (CFIP) (Smith et al., 1996) and Internet User's Information Privacy Concerns (IUIPC) (Malhotra et al., 2004) are the two widely used constructs to measure privacy concerns (Smith et al., 2011). CFIP was designed to measure information privacy in a broad sense and IUIPC is operationalized in the Internet context, focusing on e-commerce websites where: (a) users only consider the cost of disclosing information to the corresponding website and there is no third-party audience involved, and (b) information disclosure is often a one-time activity. Data disclosure in social mobile era is more

complicated as (1) publicly available user-generated content can be collected by other individuals or third-party companies with/without the consent of the user and matched with external datasets to make accurate inferences (e.g. user-generated content from Facebook can be matched with data from other social networking services, such as Grindr and Feeld dating services, to profile an individual's lifestyle and sexual orientation), (2) user interactions are augmented with various sensor data to create digital footprints or profiles, and (3) information disclosure is continuous and can vary in terms of richness and accuracy.

While the effect of privacy concerns on information disclosure in Online Social Networks (OSNs) is studied extensively, prior research has largely ignored the role of privacy concerns with regards to other individuals or peers (social privacy concerns) (Ozdemir et al., 2017). Besides, the majority of Internet users have already joined at least one OSN and access the platforms using their mobile apps (PEW Research Center, 2019) that can constantly watch the activities of their users even when the app is closed, which is different from desktop applications (Wottrich et al., 2019). These issues highlight the importance of examining the degree and intensity of OSN use. However, most mobile app privacy studies focus on app download and install (Dogruel et al., 2017; Pentina et al., 2016; Rutz et al., 2019; Wottrich et al., 2018) missing the long-term behavioral outcomes.

This study attempts to fill these gaps by considering both social and institutional privacy concerns (Ozdemir et al., 2017; Raynes-Goldie, 2010) and investigating the cost and benefit calculus of user engagement with social media-enabled apps. Specifically, this study seeks to address the following research questions:

1. What are the major antecedents of social and institutional types of privacy concerns?
2. What is the effect of social and institutional privacy concerns on users' engagement with a social media-enabled app?
3. What are the benefits that drive users to engage with a social media-enabled app?

With privacy calculus theory (Culnan and Armstrong, 1999) as the theoretical basis, this study examines the types of concerns and benefits that may affect user engagement with social media-

enabled apps and supplements a survey method with a follow-up text analysis to investigate the above research questions.

This study makes several contributions to privacy literature. First, it positions user engagement as the outcome behavior of privacy calculus. Second, it empirically validates the effect of institutional and social privacy concerns on user engagement. Third, it improves the understanding of the antecedents of privacy concerns by examining the relationship between perceived risk, control, and information sensitivity and the two dimensions of privacy concerns. Finally, it extends the benefits dimension of the privacy calculus framework by demonstrating how specific benefits may have differential impacts on user engagement.

The rest of the paper is organized as follows. Section 2 presents a review of the extant literature of information privacy, discuss the evolution of the concept in the light of recent technological developments and then explain the study context. In Section 3, the hypotheses are developed and tested using a survey approach and findings are further explored through a follow-up text analysis study. In Sections 4 and 5, the implications for research and practice are discussed respectively. Finally, Section 6 presents the conclusion and future research directions.

2. Related Literature

2.1 Privacy in a Social Mobile Era

Information privacy is defined as the ability to control information about oneself and determine when and for what purpose such information can be accessed by others (Bélanger and Crossler, 2011; Westin, 2003). Prior studies suggest that the evolution of privacy follows the advancements of information technology and its dimensions are subject to change with the evolution of markets and technologies (Malhotra et al., 2004; Smith et al., 2011).

Three contemporary eras of information privacy are discussed in the literature (Westin, 2003). The first era (1961 – 1979) is marked by the emergence of data collection, processing, and surveillance technologies when the advancements of mainframe computers and communication protocols raised concerns about individuals' privacy rights. The second era (1980 – 1989) did not

witness any fundamental privacy changes, as advancements of computers and telecommunications were incremental. Personal computers were introduced but their computation power and network access were limited. In the third era (1990 – 2010), privacy became a social and political priority as the Internet and wireless communication technologies became ubiquitous, big data tools were developed and data breach incidents, web tracking and fingerprinting, location-based services and the adoption of electronic health records compounded the challenges of balancing the needs to ensure one's privacy rights and protecting the freedom of information[1].

However, technology developments in the last decade have significantly changed the concept of privacy, and have raised unprecedented issues regarding the role of third-parties, the degree of user involvement in privacy settings, and the commercialization of user data (e.g., the Facebook–Cambridge Analytica incident). Technological advancements have also significantly increased the value of data, and hence the data collection efforts of organizations. About 90 percent of the data on the Internet today are generated after 2016 and about half of this data are generated with mobile and Internet of things (IoT) devices (Marr, 2018). Empirical analysis reveals that these devices are the major target for privacy and security violations as they lack basic security protocols (Pour et al., 2019). Moreover, using large anonymized datasets and identifying individuals or their life events is no longer computationally prohibitive (Breeden, 2014; Ebadi et al., 2019). A recent study estimates that "99.98% of Americans would be correctly re-identified in any dataset using 15 demographic attributes" (Rocher et al., 2019, p. 1). The number of social media users has also increased from 5 percent in 2005 to 72 percent in 2019 (PEW Research Center, 2019). Temporal and spatial boundaries of privacy are fading (Acquisti et al., 2015) as stored public data can even reveal people's secret affairs (Malm, 2018), and physical privacy is no longer an isolated concept, rather a subset and a function of information privacy.

[1] The interested reader is referred to Westin (2003) as well as Smith et al. (2011) for a comprehensive review of these information privacy eras.

This study argues that the significant technological developments of the last decade have changed the concept and dimensions of privacy, partly due to the increased distinct parties involved in the provision of mobile-enabled services. Additionally, with the integration of the Internet with social and mobile technologies, we may have already stepped into the fourth era of information privacy as shown in Figure 1.

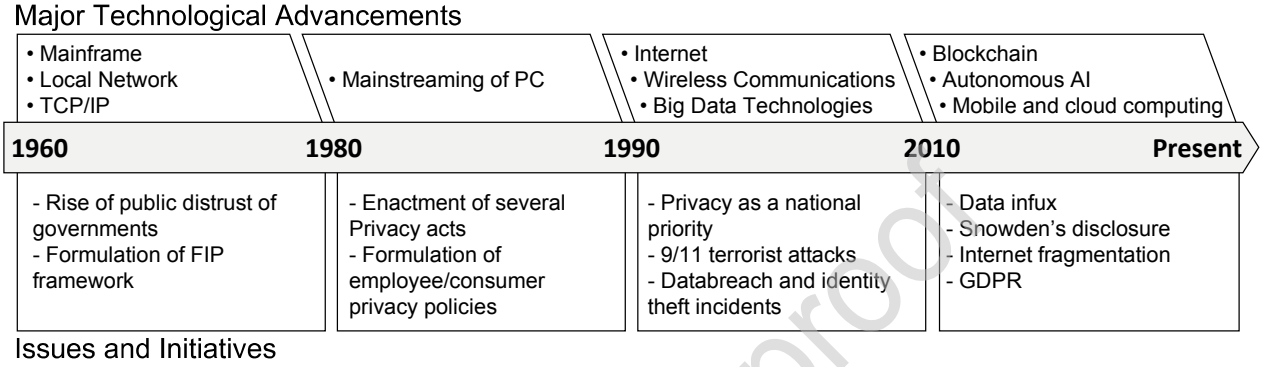


Figure 1. Eras of Information Privacy (adapted from Westin 2003; Smith et al. 2011)

The majority of positivist empirical IS studies on privacy concerns examine the phenomenon through "Antecedents-Privacy Concerns-Outcomes" (APCO) macro model (Dinev et al., 2015), and predominantly use one of the two popular constructs (CFIP or IUIPC) to measure users' information privacy concerns (Smith et al., 2011; Warkentin et al., 2016). However, as people constantly engage in social media and connect with others on mobile devices, the preceding constructs may have to be revisited.

Individuals participate in OSNs to build social capital, improve their self-worth and self-esteem, and satisfy their enjoyment needs (Heravi et al., 2018; Krasnova et al., 2010). However, contents shared on these platforms can attract a wide range of individuals, third-party organizations and government agencies (Acquisti et al., 2015). Thus, when deciding to disclose information, users must consider the potential misuse of private information by 1) the organization operating the OSN and its partners (also known as institutional privacy concerns), and (2) other users or entities on the platform (social privacy concerns) (Raynes-Goldie, 2010).

Moreover, in the context of mobile apps, the user's information disclosure is supplemented with device-generated data (e.g., device ID, the user's location and contact list) (Crossler and Bélanger, 2019). Such data are automatically shared with the developer once users accept app permission requests (Dogruel et al., 2017). Besides, most developers share user data with third-parties for tracking and advertisement purposes; thus, enabling third-party companies to match the data from various apps and services, and make inferences about individual users (Vallina-Rodriguez and Sundaresan, 2017). Unlike traditional websites or desktop applications, mobile apps can constantly watch the activities of their users (Wottrich et al., 2019). Therefore, the dynamics of data sharing and disclosure have made privacy studies in the social mobile era more complicated than before (Barth and De Jong, 2017; Crossler and Bélanger, 2019; Wottrich et al., 2018).

2.2 Privacy Calculus Theory

As one of the most prominent information privacy research frameworks, privacy calculus theory examines the cost and benefit trade-off of information disclosure (Culnan and Armstrong, 1999; Laufer and Wolfe, 1977). Costs often entail losing one's privacy, and benefits are the context-specific gains individuals expect in exchange for the private information they provide (Jiang et al., 2013; Pentina et al., 2016). Privacy calculus theory interprets privacy in economic terms by suggesting that individuals perform a subjective cost-benefit analysis when asked to provide information in return for a product or service and disclosure happens when the individual anticipates that benefits will outweigh the risks of privacy loss (Dinev and Hart, 2006; Smith et al., 2011). The individual's outcome behavior is influenced by personality and contextual factors (Gutierrez et al., 2019) and while most prior works report a negative influence of privacy concerns on information disclosure, individuals tend to overvalue the benefits and undervalue their privacy (Dinev and Hart, 2006; Jiang et al., 2013; Xu et al., 2009). Privacy calculus is a rigorous framework to study privacy concerns in the context of social media and mobile apps (Kordzadeh and Warren, 2017; Wottrich et al., 2018) and prior studies report monetary rewards (Dogruel et al., 2017;

Gutierrez et al., 2019), personalization (Gutierrez et al., 2019; Zhao et al., 2012), enjoyment (Krasnova et al., 2010), social (Krasnova et al., 2010; Pentina et al., 2016; Trepte et al., 2020; Wang and Liu, 2019), and efficiency benefits (Krasnova et al., 2010; Pentina et al., 2016) as the major drivers of information disclosure in these contexts. Table 1 summarizes a snapshot of recent empirical privacy studies in the context of social media and mobile apps.

However, the degree of user involvement with the technology, richness, and continuity of data collection, as well as the unpredictability of privacy threats and their sources renders such binary conceptualization of behavior obsolete in the social mobile era. User assessments of costs are increasingly inaccurate as consequences are hard to anticipate and parties are difficult to hold accountable for privacy issues (Liptak, 2019; Nguyen, 2019). Additionally, privacy studies in the context of mobile apps mainly focus on app download and install intention (Gu et al., 2017; Pentina et al., 2016; Wottrich et al., 2018), and only few examine the continuation of use (Pentina et al., 2016). Industry reports indicate that many users abandon and uninstall apps shortly after downloading them, and the average user only engages with nine apps per day (McLean, 2018; Tarute et al., 2017). As a result, app developers have shifted their focus from the number of installs to the users' in-app behavior (Perro, 2018; Rutz et al., 2019). Therefore, instead of initial adoption or information disclosure, this study investigates the implications of user engagement with social media-enabled apps within the framework of privacy calculus.

Table 1. Summary of a Few Key Empirical Privacy Research on OSNs and Mobile Apps

References	Theoretical Lens	Context	Findings
(Xu, Dinev, Smith, & Hart, 2011)	Communication Privacy Management theory (CPM)	OSN, ecommerce, finance, healthcare	OSN users have higher perceived privacy control than users in other contexts.
(Cavusoglu et al., 2016)	Communication Privacy Management theory (CPM)	OSN	The addition of granular privacy control options has driven Facebook users to share more information publicly.
(Kordzadeh and Warren, 2017)	Privacy Calculus + Affective Commitment	Virtual Health Community	The disclosure of Personal Health Information is positively affected by perceived benefits and negatively affected by privacy concerns.
(Jordaan and Van	Uses and gratification theory + third-person effect	OSN	The perception of control and the number of strategies people use to control the audience of

Heerden, 2017)			their personal information predict their Facebook usage intensity.
(Trepte et al., 2020)	Privacy calculus	OSN	While privacy concerns negatively affect information disclosure on SNS?, the expected level of social support and the degree of similarity and information disclosure of other users increase an individual's self-disclosure on social media websites.
(Pentina et al., 2016)	Privacy calculus	Mobile app	Mobile app use is largely driven by perceived information and social benefits.
(Dogruel et al., 2017)	Privacy calculus	Mobile app	App users value privacy and are willing to pay a premium for better privacy. However, when faced with a choice, they often assign a higher economic value to perceived benefits than privacy-preserving measures.
(Wottrich et al., 2018)	Privacy calculus	Mobile app	This study draws a causal inference, demonstrates the trade-off in an experimental setting and shows that privacy calculus does exist in the mobile app context.
(Crossler and Bélanger, 2019)	self-efficacy theory, and the information–motivation–behavioral skills model	Mobile app	Personal motivation, privacy awareness, and privacy self-efficacy predict privacy behavior, while the role of social motivation and technology self-efficacy are not significant.
(Gutierrez et al., 2019)	Privacy calculus	Mobile advertisement	The perceived intrusiveness and privacy concerns of location-based ad messages are negative predictors of user's information disclosure while personalization of the message and monetary rewards positively impact information disclosure intention.

3. Model Development

3.1 Hypotheses and Research Model

Building on prior studies that use privacy calculus theory in social media and mobile app contexts (Dogruel et al., 2017; Gutierrez et al., 2019; Jiang et al., 2013; Pentina et al., 2016; Trepte et al., 2020; Wottrich et al., 2018), this study evaluates the costs and benefits of engagement with social media-enabled apps. Specifically, the privacy calculus framework is extended by examining the separate effects of institutional and social privacy concerns on user engagement rather than one-time information disclosure behavior, identifying the distinct antecedents of the two types of privacy concerns, and recognizing the unique benefits that are relevant within this context.

3.1.1 Risk, Control and Information Sensitivity

Over the years, several antecedents for privacy concerns have been identified but many of them were not re-evaluated (Bélanger and Crossler, 2011) as the perception of privacy is context dependent. Drawing on Communication Privacy Management (CPM) and privacy calculus theory, Xu et al., (2011) highlight the importance of perceived risk and control, and recommend researchers to further examine their findings in OSN context.

- Privacy Risk

Privacy risk is defined as the possibility and severity of losing one's personal information as a result of the opportunistic behavior of other parties (Dinev & Hart, 2006; Xu et al., 2011). Privacy risk assessment in the social media-enabled app context involves subjective evaluation of who has access to the information and what they may do with it. Privacy violations by the institution operating the platform can have severe consequences for the individual such as profiling, price discrimination and targeted ads (Crossler and Bélanger, 2019; Kordzadeh and Warren, 2017). Prior literature has shown the positive effect of privacy risk on institutional privacy concerns (Dinev & Hart, 2006; Xu et al., 2011).

In the context of social media-enabled apps, the institution is not the only potential misuser of data. IS literature is largely silent about privacy in peer relationships because the risk of data misuse by peers and third-party companies other than the immediate organization only exists in social and collaborative environments (Ozdemir et al., 2017). However, the growing popularity of social media and its integration with a variety of services, especially within mobile apps, highlight the importance of considering social privacy concerns.

Depending on users' privacy settings, their social feed can be broadcasted to a diverse range of audiences on the platform, and prior studies have shown that personal details such as individual identities, their shopping habits and the places that they visit can be tracked (Khanna, 2015; Zhang et al., 2017); thus, giving rise to privacy risks such as stalking and blackmailing. Therefore, it can be hypothesized that:

H1a: Privacy Risk is positively related to Institutional Privacy Concerns.

H1b: Privacy Risk is positively related to Social Privacy Concerns.

- Privacy Control

The risks associated with information disclosure highlight privacy control as an important predictor of privacy concerns (Dinev & Hart, 2004; Malhotra et al., 2004; Xu et al., 2011). Privacy control is the degree to which an individual believes to have control over the modification and dissemination of their personal information (Malhotra et al., 2004; Xu, Michael, & Chen, 2013). Studies suggest that although users have little control over how their data is collected and shared (Poikela et al., 2015), the use of explicit permission requests and clear privacy notifications in mobile apps can create a feeling of control and lower their privacy concerns (Malhotra et al., 2004; Widjaja et al., 2019). However, they have little power over how their data are collected and used by the OSN platform and its third-party affiliates (Crossler and Bélanger, 2019; Zarouali et al., 2018). For instance, in a recent high-profile incident, it was reported that both public and private profile data of millions of Facebook users were harvested through a mobile app by Cambridge Analytica for political purposes (Cadwalladr and Graham-Harrison, 2018).

Furthermore, OSN platforms provide users with options to control the audience of their social feed and apply more restrictive privacy settings. This perception of privacy control also lowers user's privacy concerns and drives them to disclose information in the social feed (Acquisti et al., 2015; Cavusoglu et al., 2016). Thus the following hypotheses are proposed:

H2a: Privacy Control is negatively related to Institutional Privacy Concerns.

H2b: Privacy control is negatively related to Social Privacy Concerns.

- Information Sensitivity

Information sensitivity is defined as an individual's attitude toward revealing different information while interacting with a social media-enabled app (Bansal and Gefen, 2010). The type of information requested by the institution impacts the user's privacy concerns. Individuals are more sensitive about revealing their medical records, social security number or their financial information than their shopping or eating habits (Sheehan and Hoy, 2000; Smith et al., 2011).

Information sensitivity has been shown to affect privacy concerns (Cavusoglu et al., 2016; Gu et al., 2017; Kim et al., 2019; Koohikamali et al., 2017; Xu et al., 2013). Moreover, the social feed on social media-enabled apps can reveal potentially sensitive information about the parties involved. For instance, many transactions on social P2P payment apps (e.g. Venmo) include the purchase of drugs and alcohol (Dewey, 2015) and therefore, this kind of user activity can lead to personal embarrassment if revealed which leads to the following hypotheses:

H3a: Information Sensitivity is positively related to Institutional Privacy Concerns.

H3b: Information Sensitivity is positively related to Social Privacy Concerns.

3.1.2 Engagement

Prior literature has examined several behavioral reactions as the outcome of privacy concerns and intention to disclose or disclosure behavior are the commonly used dependent variables (Smith et al., 2011). However, recent privacy studies have shifted away from disclosure intention to measure self-reported behaviors (Ozdemir et al., 2017). As a result of the technological advancements in the last decade, initial adoption or a binary information disclosure behavior may not fully capture the intricacy of users' interaction with social media-enabled apps (Hong and Thong, 2013; Kim et al., 2013). Therefore, this study proposes engagement which is defined as the degree to which thoughts, emotions, and actions of an individual are preoccupied with a particular system (Khan, 2017; O'Brien & Toms, 2008; Smith & Gallicano, 2015) as the outcome behavior of privacy calculus framework.

In a social media-enabled app (e.g. Venmo), every user activity can reveal sensitive information, such as transaction amounts and parties involved, time and location data. Thus, users may try to limit their activities because they are concerned that such information can be misused by the app company or by users such as family members, friends or other entities.

Therefore, the following hypotheses are formulated:

H4a: Institutional Privacy Concerns is negatively related to Engagement in a social media enabled app*.*

H4b: Social Privacy Concerns is negatively related to Engagement on a social media enabled app.

3.1.3 Perceived Benefits

Major benefits of users' information disclosure include monetary (Gutierrez et al., 2019), efficiency (Krasnova et al., 2010; Pentina et al., 2016), information (Bansal and Gefen, 2010; Kordzadeh and Warren, 2017; Pentina et al., 2016), personalization (Gutierrez et al., 2019; Xu et al., 2009), social (Krasnova et al., 2010) and enjoyment (Lee et al., 2010). Prior studies suggest that efficiency, social and hedonic benefits are relevant in the context of social media-enabled apps (Hsiao et al., 2016). Efficiency benefit describes user's perception regarding the usefulness, and convenience of a certain technology (Venkatesh and Brown, 2001) which can lead to higher user engagement (Kim et al., 2013; McLean, 2018). Social media-enabled apps may provide useful functionalities (Hsiao et al., 2016). For instance, mobile payment apps enable users to send and receive money quickly and conveniently. Therefore, it can be hypothesized that:

H5a: Perceived Efficiency Benefit is positively related to Engagement on a social media enabled app.

Social benefit describes the perceived rewards individuals derive from interacting with others (Jiang et al., 2013). It positively affects both user's adoption and their engagement in the mobile app context (Kim et al., 2013; Pentina et al., 2016). Social features of social media-enabled apps allow users to interact with others on the platform, and thus:

H5b: Perceived Social Benefit is positively related to Engagement a social media enabled app.

Enjoyment benefit refers to the sense of pleasure and enjoyment derived from using a certain technology (Venkatesh and Brown, 2001). Studies on mobile app engagement suggest a positive relationship between enjoyment benefits and user engagement (Kim et al., 2013; McLean, 2018). Social features of social media-enabled apps deliver fun user experience, specifically through the use of emojis and reactions. Therefore:

H5c: Perceived Enjoyment Benefit is positively related to Engagement on a social media enabled app.

3.1.4 Control Variables

Age, gender, education, privacy experience (Gu et al., 2017; Ozdemir et al., 2017), app experience (Jiang et al., 2013) and privacy settings (public or private) also impact users' privacy concerns and are included as control variables. The conceptual model of this study is illustrated in Figure 2.

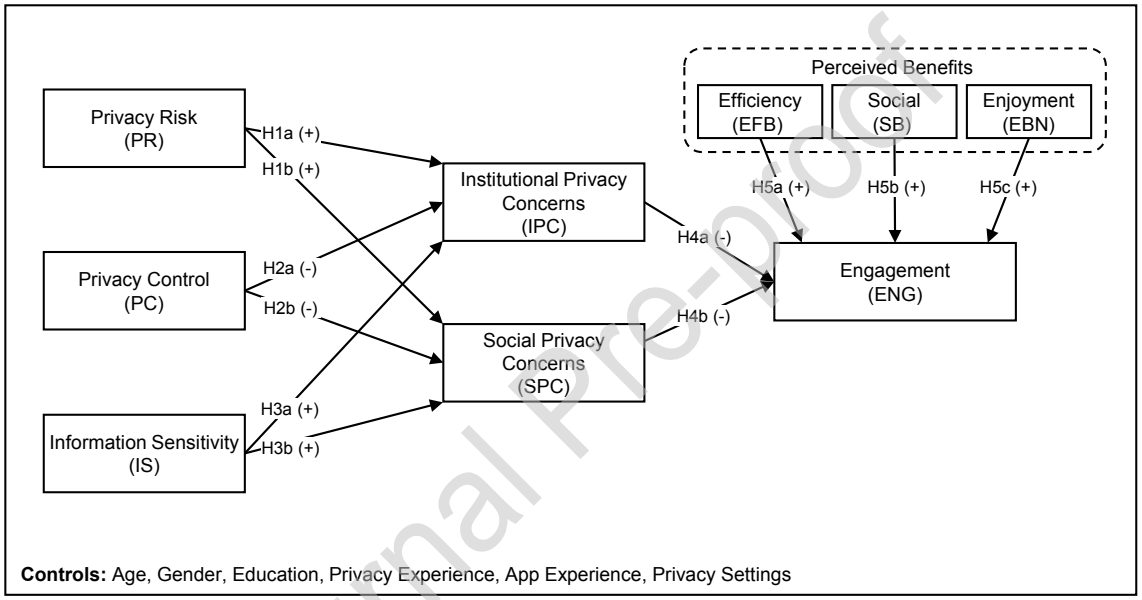


Figure 2. Conceptual Model

3.2 Methodology

3.2.1 Research Context

The popularity of OSNs has led mobile app developers to integrate social media with a variety of other services. Social media-enabled apps provide tools for users to communicate and interact with other users and friends in the context of gaming, education, fitness, health and even financial services (Hsiao et al., 2016). Prior literature suggests that the inclusion of the social aspect of apps can heighten user engagement to the point of digital addiction (Kwon et al., 2016). Venmo is a social payment app in which the P2P payment function enables mobile phone users to easily split bills and transfer money to friends and vendors, while the social features allow users to share

notes, emojis, comments, likes, and reactions to other transactions on the platform. It encourages social engagement (Lev-Ram, 2017). However, all transactions are public by default unless users deliberately change their settings either to private or friends only. To use the app, users must grant Venmo permission to access their contact list, media files, camera, and device ID, and they must provide a valid phone number, full personal information (e.g., Social Security Number, date of birth, driver's license), as well as their credit card or debit card information. The app stores user transaction information and their social activities with timestamped geolocation data. The personal and financial data collected by Venmo and the social feed of the app can reveal lifestyle, and shopping habits of the users (Khanna, 2015; Zhang et al., 2017).

3.2.2 Measurement Development

The conceptual model was tested using structural equation modeling (SEM). A questionnaire was developed using items from the literature. The final set of items used to measure each construct and the source of these measurement items are presented in Appendix I. These constructs were measured with multiple indicators coded on a seven-point Likert scale. Descriptions of these constructs are summarized in Table 2. To validate the items before testing the model, first, exploratory factor analysis (EFA) was conducted using IBM SPSS 23.0 and then the adequacy of the measurement model was assessed through confirmatory factor analysis (CFA). Finally, the SEM model and the hypotheses were tested using IBM AMOS 23.0 software package.

Table 2: Definitions of Constructs

Construct	Operational Definition
Privacy Risk (PR)	The amount of loss an individual anticipates because of the disclosure of their personal information.
Privacy Control (PC)	The degree to which an individual believes to have control over modification and dissemination of their personal information
Information Sensitivity (IS)	The perceived degree of the sensitivity of information individuals must disclose when using the system. In a social payment app, this information contains the parties, purpose, and location of the transaction.
Institutional Privacy Concerns (IPC)	The concerns individuals have about how institutions practice privacy and handle their personal information.
Social Privacy Concerns (SPC)	The concerns individuals have about access, misuse, and dissemination of their personal information by persons or entities who can access their social network.

Efficiency Benefit (EFB)	User's perception regarding the efficiency, usefulness, and convenience of a certain technology.
Social Benefit (SB)	The perceived rewards individuals derive from interacting with others.
Enjoyment Benefit (EBN)	The sense of pleasure and enjoyment derived from using a certain technology.
Engagement (ENG)	The degree to which thoughts, emotions, and actions of an individual are preoccupied with a particular system.

Sample

IRB approval was obtained prior to data collection (IRB #18-045E). Following recommendations by prior literature (Bollen, 2014; MacCallum et al., 1996), 380 respondents of actual users of the social P2P payment apps were recruited from Amazon's Mechanical Turk platform. After removing incomplete responses and those responses that failed the attention check questions, a final sample size of 354 was obtained. Table 3 summarizes the sample demographics, where approximately 62 percent of the respondents are male, and 38 percent are female.

Table 3: Demographic Characteristics of the Sample

Gender	Male (0)	219 (62%)
	Female (1)	135 (38%)
Age	1 (25 and below)	54
	2 (26 - 30)	106
	3 (31 - 35)	71
	4 (36 - 40)	48
	5 (41 - 45)	33
	6 (46 - 50)	16
	7 (51 – 55)	12
	8 (above 55)	14
Privacy Experience	Never victimized	297 (84%)
	Definitely victimized	57 (16%)

3.2.3 Measurement Model Analysis

The final EFA with 9 factors (shown in appendix II), suggests that the sample is adequate (KMO = 0.813) and the Bartlett's test of Sphericity is significant (χ^2 (378) = 6730.763, p = 0.000) suggesting the existence of a pattern relationship. The final solution resulted from the EFA was subjected to a CFA. 4 items were dropped due to low factor loadings and a measurement model with acceptable fit indices was obtained ($\chi^2_{216} = 427.001$; CFI = 0.962; TLI = 0.952; RMSEA = 0.053; SRMR = 0.0421; PClose = 0.272).

Table 4 shows the composite reliability and average variance extracted (AVE) for all constructs in the research model. The values of Cronbach's alpha and composite reliabilities are all higher than the recommended 0.70 (Nunnally and Bernstein, 1994), and the values of AVE are above 0.50 (Fornell and Larcker, 1981); thus, supporting internal consistency and convergent validity. Discriminant validity was also supported because the square root of AVE of each construct (diagonal of Table 4) is higher than the correlation between that construct and any other constructs. This criterion is satisfied by all latent constructs, as shown in Table 4. Therefore, the measurement model exhibits sound reliability and validity necessary to proceed to hypothesis testing.

Table 4: Convergent and Discriminant Validity

Scales	Mean	SD	CR	α	EBN	PC	PR	SPC	SB	ENG	IPC	EFB	IS
EBN	5.086	1.119	0.866	0.860	**(0.827)**								
PC	4.683	1.355	0.911	0.910	0.380	**(0.880)**							
PR	4.481	1.319	0.864	0.861	-0.077	-0.215	**(0.826)**						
SPC	4.270	1.670	0.901	0.899	-0.241	-0.495	0.390	**(0.906)**					
SB	4.709	1.348	0.911	0.911	0.511	0.288	-0.038	-0.184	**(0.915)**				
ENG	2.933	1.636	0.901	0.900	0.336	0.260	0.131	-0.301	0.311	**(0.867)**			
IPC	6.175	1.133	0.901	0.897	0.075	-0.080	0.172	0.205	-0.037	-0.235	**(0.867)**		
EFB	6.077	1.008	0.905	0.905	0.513	0.191	-0.109	-0.011	0.321	-0.059	0.302	**(0.872)**	
IS	4.907	1.383	0.838	0.806	0.057	-0.141	0.374	0.210	0.015	0.001	0.323	0.096	**(0.854)**

Note: CR is Composite Reliability; α is Cronbach's alpha. 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 $p < 0.01$.

3.2.4 Common Method Bias

This study uses two techniques to determine if the effect of common method variance (CMV), which is a function of the methods employed to measure the independent and dependent variables, threatens the validity of the results. First, Harman's one-factor test (Podsakoff et al., 2003) was employed and all items were loaded into a non-rotated single factor to determine the number of factors necessary to account for the variance in the items. The single factor extracted accounts for 19.882 percent of the variance in the model which is far less than the 50 percent threshold, suggesting that there is no evidence of common method bias. Next, the marker variable

technique was used which is underpinned by the major assumption that the method factor has a constant effect on all measured items and as such, the lowest (or second lowest) correlation in the full correlation matrix reported in a study is an unbiased proxy for CMV (Malhotra et al., 2006). In this study, social desirability bias (Simmering et al., 2015), which is theoretically unrelated to other variables is used as the marker variable. A chi-square difference test between the baseline model and the model with the marker variable (shown in table 5) indicates that there may be evidence of common method variance. Therefore, following Podsakoff, MacKenzie, Lee, and Podsakoff, (2003) recommendations, CMB was controlled for by keeping the marker variable in the model as we move onto the Structural Equation Modeling.

Table 5: Chi-square Difference Test

Measurement Model	Chi-square	df
Baseline CFA Model	427.001	216
CFA Model Controlling for Social Desirability Bias	679.434	317
Difference	252.433***	101

Note: *** p < 0.001

3.3 Results and Discussion

The final SEM model exhibits a good fit ($\chi^2_{483} = 951.726$; CFI = 0.926; TLI = 0.914; RMSEA = 0.052; SRMR = 0.0863; PClose = 0.204) and therefore it is safe to proceed to hypothesis testing. The results are shown in Table 6.

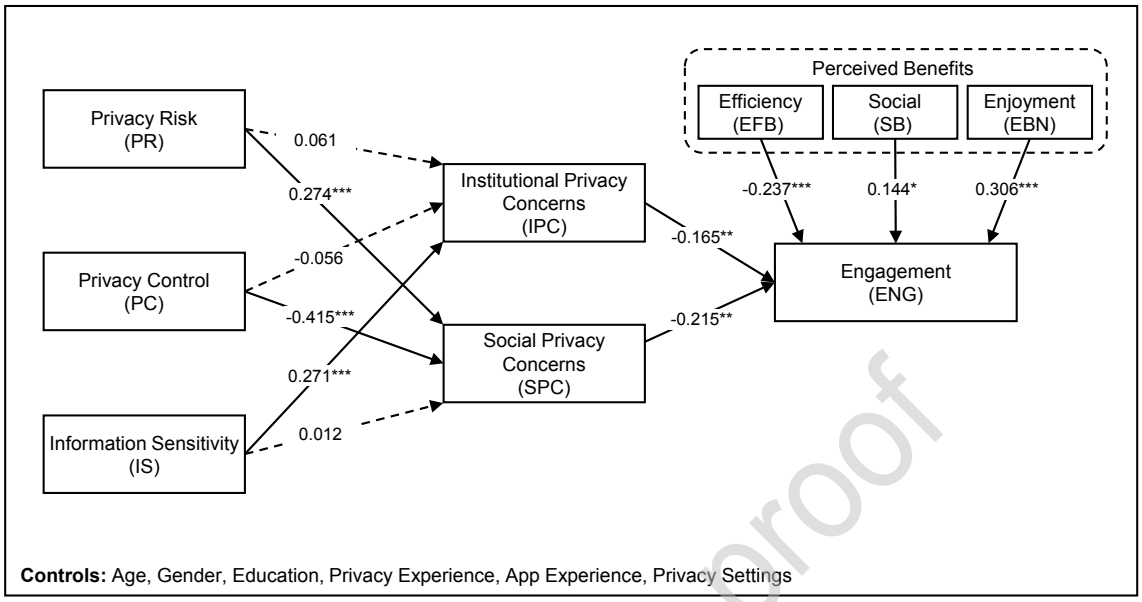
Table 6: Summary of Results

Hypothesis	Unstandardized Estimates	Standardized Estimates	P-Value	Supported?
H1a: PR ➔ IPC (+)	0.047	0.061	0.345	**No**
H1b: PR ➔ SPC (+)	0.298	0.274	0.000	**Yes**
H2a: PC ➔ IPC (-)	-0.047	-0.056	0.332	**No**
H2b: PC ➔ SPC (-)	-0.492	-0.415	0.000	**Yes**
H3a: IS ➔ IPC (+)	0.283	0.271	0.000	**Yes**
H3b: IS ➔ SPC (+)	0.018	0.012	0.817	**No**
H4a: IPC ➔ ENG (-)	-0.226	-0.165	0.003	**Yes**
H4b: SPC ➔ ENG (-)	-0.208	-0.215	0.001	**Yes**
H5a: EFB ➔ ENG (+)	-0.378	-0.237	0.000	**No** (opposite direction)
H5b: SB ➔ ENG (+)	0.171	0.144	0.017	**Yes**

H5c: EBN ➔ ENG (+)	0.438	0.306	0.000	**Yes**

Regarding the antecedent of privacy concerns, the relationship between perceived privacy risk and institutional privacy concerns (β = 0.061, p < 0.345) is not significant; thus, H1a is not supported. However, the relationship between privacy risk and social privacy concerns is significant (β = 0.274, p < 0.000), supporting H1b. While the relationship between perceived privacy control and institutional privacy concerns is not significant (β = -0.056, p = 0.332), and therefore H2a is not supported. For H2b a significant negative relationship between perceived privacy control and social privacy concerns can be observed, supporting H2b (β = -0.492, p < 0.000). This finding echoes those reported in prior studies such as Cavusoglu et al. (2016), which suggest that in the context of social media-enabled apps, the perception of control only mitigates users' concerns about the misuse of their information by others but not by the app company itself. Considering perceived information sensitivity, it has a significant positive relationship with institutional privacy concerns (β = 0.271, p < 0.000), supporting H3a. However, it is not a significant predictor of social privacy concerns (β = 0.012, p = 0.817) and H3b is not supported. Furthermore, the analysis results show that both institutional and social privacy concerns have significant negative impact on engagement, supporting H4a (β = - 0.165, p = 0.003), and H4b (β = -0.215, p = 0.001). Regarding the benefits evaluation, it was hypothesized that user's engagement is positively influenced by their perceived efficiency, social and enjoyment benefits. The analysis results indicate that two types of benefits (social and enjoyment) are positively related to engagement, supporting H5b (β = 0.171, p = 0.017), and H5c (β = 0.306, p < 0.000). The efficiency benefit is found to be significant but it is negative instead of positive (β = -0.237, p < 0.000), thus, H5a is not supported. This suggests that the efficiency benefit of the app negatively impacts engagement which is contrary to what was expected and needs further investigation (see section 3.4 for the detailed investigation). Finally, regarding the control variables, AGE (β =-0.136, p = 0.006) and PUBLIC (β =-0.330, p = 0.005) are significant, suggesting that older users as well

as those who set their privacy settings as private tend to engage less with the P2P payment apps. Figure 3 summarizes the final model.



Note: *** p < 0.001, ** p < 0.01, * p < 0.05, dotted line = not significant. Standardized coefficinets are shown.

Figure 3. Final Research Model with Results

Moreover, institutional privacy concerns positively affect social privacy concerns ($\beta = 0.124$, $p < 0.05$) and the average value of IPC (6.175) is much higher than SPC (4.270). This suggests that users are generally more concerned about the misuse of their data by companies than by other users. Also, the diversity of the study sample allows us to compare millennials with older users. The results of the post-hoc analysis (shown in appendix III) reveals that on average, millennials perceive a significantly lower level institutional privacy concerns, while their perception of social benefits of the app is significantly higher than the older generations.

The result of H5a contradicts the initial expectation and may suggest that post-technology adoption, users evaluate each benefit vis-à-vis their experience or concerns. Specifically, users who adopt the app for its efficiency benefits tend to be discouraged by its social aspect and seek to minimize their engagement by only using the app for completing transactions. To validate this conjecture and further investigate the unexpected direction of efficiency benefits relative to social

and enjoyment benefits, a follow-up text analysis study is conducted as discussed in the next subsection.

3.4 Follow-up Text Analysis Study

To corroborate the findings from the survey of the app users' perception and better understand the interplay of privacy concerns and benefits, the publicly available user review data[2] for the Venmo app from Google Play website (34,272 reviews posted between August 21, 2010, and April 21, 2018) were collected. Each review contains the review date, star rating, helpfulness rating, and review content. Non-English and less than 5-word reviews were removed. Each review was given a unique review identifier (RID) and reviews with more than one sentence were split into separate sentences. The split sentences retained the original RID and were also assigned a sentence code. At the sentence level, sentences that only contained emoticons and non-alphabetic characters as well as those with less than three characters were removed. As each review can have one or more sentences (see Figure 4), the final dataset consists of 20,392 reviews that include 38,058 sentences.

User ID	Review ID	Sentence	Labels			
			Y1	Y2	Y3	Y4
U1001	RID1001	X1	0	0	1	1
		X2	1	0	0	0
		X3	0	0	0	0
		X4	0	1	1	0

Figure 4. Multiple Labels for Each of the Sentences of a Review

3.4.1 Text Classification

Text classification is the automatic process of assigning labels to documents based on the existence of certain characteristics, words, and phrases (Law et al., 2017). It is widely popular in social media studies (Ghani et al., 2019) and has been used in IS literature to detect Internet abuse in the workplace (Chou et al., 2010), classify public sentiments in microblogs (Liu & Chen,

[2] This study does not meet the definition of human subject research per federal regulations and is exempt from IRB review since (a) data is publicly available, and (b) unit of analysis is each review text rather than the individual (National Institutes of Health, 2016; Office for Human Research Protections, 2016).

2015), discover product defects from user reviews (Law et al., 2017), detect corporate fraud from social media data (Dong, Liao, & Zhang, 2018), measure brand personality (Hu et al., 2019) and consumer repurchase intention (Zhou et al., 2019).

- Data Labeling

The purpose of this analysis is to investigate the relationship between the three benefits (i.e., efficiency, social, and enjoyment) and app engagement. Therefore, based on keywords and word combinations that signify each of the three aspects, a labeling protocol was developed (Appendix IV). Users may express their likes and dislikes of certain aspects in the same sentence. For instance, *"works well, but I personally don't like the transactions showing up in a "public" fashion".* As a result, positive and negative labels were created for each aspect. Each sentence was classified using a binary label ("1" = present, and "0" = absent). Then, 4,000 of the total 34,272 sentences (10.5 percent of the entire dataset) were randomly selected and manually labeled according to the labeling protocol. Since positive efficiency was represented more than other aspects, the oversampling technique recommended by Charte et al. (2015) was used to create a balanced training set.

- Training and Validating Classifiers

This study reports four common metrics for multi-label classifiers including Hamming Loss, Precision, Recall, and F_1 Score. Following the approach of Wainer & Cawley (2017), 5-fold cross-validation with 80 percent training and 20 percent test data was performed and the performance of three classification models, namely, multi-label Naïve Bayes, multi-label SVM, and multi-label Logistic Regression were compared. As shown in Table 7, SVM outperformed the other two classification models, in terms of Hamming Loss and F_1 Scores. Thus, the SVM classification model was chosen to predict the labels for the remaining 34,058 sentences. Once the final dataset was labeled by SVM, the output was visually inspected for misclassifications.

Table 7: Performance Scores for All Three Classification Models

Performance Metrics	Classification Model		
	Naïve Bayes	SVM	Logistic Regression
Hamming Loss	0.064	**0.019**	0.051
Precision (macro)	**0.981**	0.953	0.979
Precision (micro)	**0.980**	0.953	0.977
Recall (macro)	0.535	**0.902**	0.635
Recall (micro)	0.524	**0.896**	0.628
Macro F_1	0.679	**0.924**	0.763
Micro F_1	0.683	**0.924**	0.764

After labels for individual sentences were generated, each aspect was aggregated at the review level to understand the overall opinion. Figure 5 shows the three phases of the user review classification process.

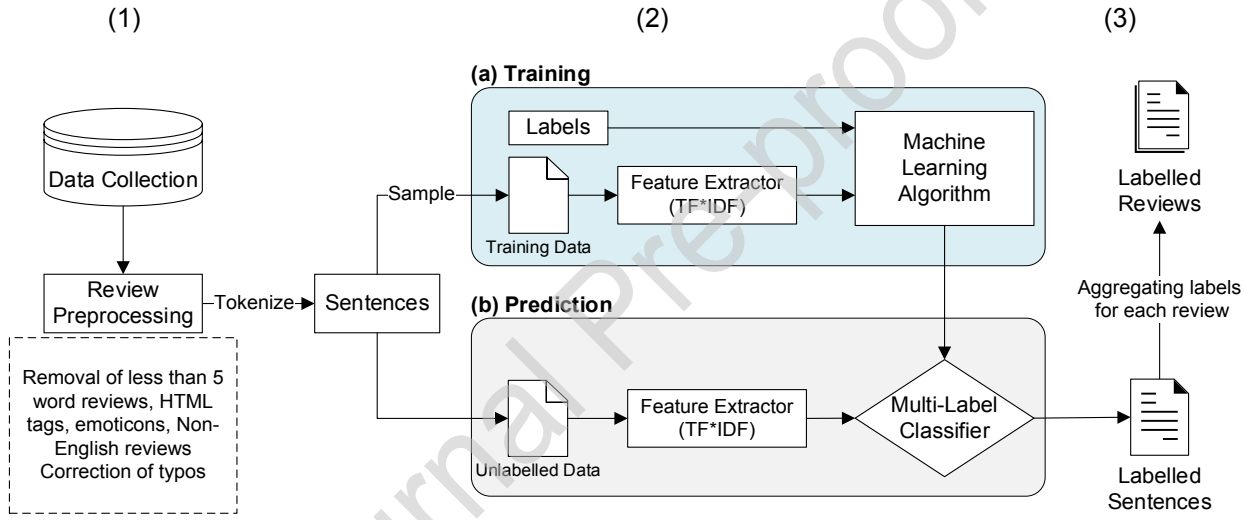


Figure 5. Classification Process of User Reviews

3.4.2 Results and Discussion

The labeling process resulted in 20,738 labels for 20,392 reviews, which represent the total number of times each aspect is discussed in the reviews. Positive efficiency was the most discussed aspect (80 percent) and negative social (10.5 percent), which signifies social privacy concerns, was the second most mentioned aspect. A co-occurrence matrix was computed to examine the relationship between aspects. This technique is often used to understand the associations and similarities between entities (Matsuo and Ishizuka, 2004). The co-occurrence matrix (Table 8) shows that positive efficiency and negative social appeared together 523 times,

the highest co-occurrence score in the matrix. However, high frequency of co-occurrences can be accidental and therefore it is necessary to test for significance of the differences (Bordag, 2008). To achieve this, the log-likelihood measure was used which describes the association between two labels by comparing their separate occurrences to their co-occurrences (Manning et al., 1999). Log-likelihood is suitable for this study because it is robust to sparsity and generates easily interpretable results. As shown in Table 9, the pairwise co-occurrences of positive efficiency with all the other aspects are significant; thus, providing evidence to reject the null hypothesis of label independence and suggesting that the interdependence is strongest for negative efficiency and negative social respectively.

Table 8: The Co-occurrence Matrix

	Positive Efficiency	Positive Social	Positive Fun	Negative Efficiency	Negative Social
Positive Efficiency	16,619				
Positive Social	100	107			
Positive Enjoyment	355	35	466		
Negative Efficiency	199	2	16	1352	
Negative Social	523	0	26	108	2,194

Table 9: Pairwise Log-Likelihood Measures for Positive Efficiency

	Terms	**Log-Likelihood Score**
Positive Efficiency	Negative Efficiency	1097.74880***
	Negative Social	462.20472***
	Positive Social	57.19032***
	Positive Enjoyment	49.89225***

***p<0.001

Typically, reviews are the presentation of users' interests and concerns (Goes et al., 2014) and the co-occurrence of positive and negative efficiency aspects can be interpreted as people who mention a positive efficiency aspect of the app are also highly likely to discuss a negative efficiency aspect. For instance, a user states that: "*Simple and easy to use. Wish it didn't take so long to transfer funds to account*". Furthermore, the strong relationship between *positive efficiency* and *negative social* suggests that people who enjoy the functionality of the app are more likely to express social privacy concerns (i.e. *negative social*) and as a result, they minimize their engagement, which corroborates the findings from the analysis of the survey response.

To further explore the findings, the average count of the five aspects over time was plotted as shown in Figure 6. The figure indicates that the trends for efficiency aspects are changing over time, while the social and enjoyment aspects are relatively constant. This is consistent with prior studies and suggests that the efficiency aspect is a more objective concept related to the actual quality of the app while social and enjoyment aspects are more subjective (Sen and Lerman, 2007).

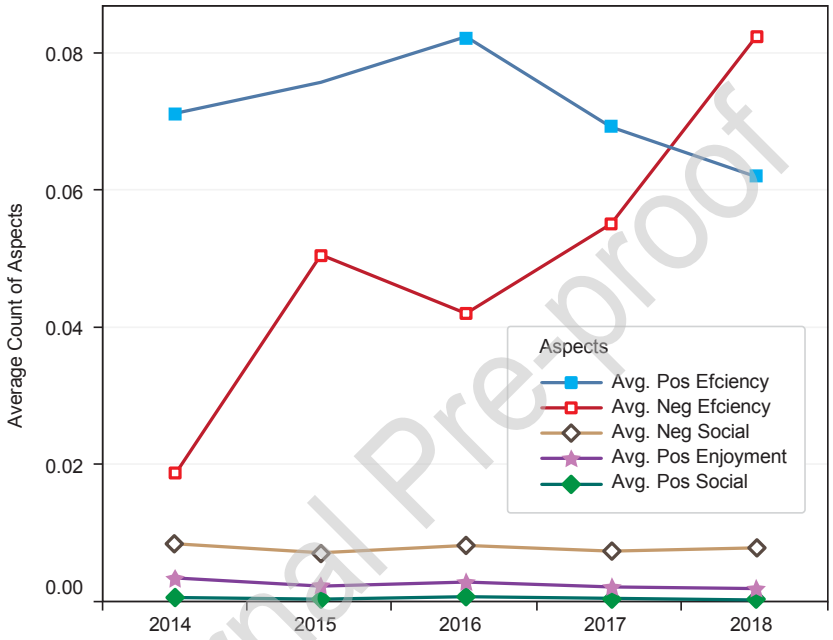


Figure 6. Average Counts of Aspects Over Time

Regarding the negative relationship between efficiency benefits and engagement, prior studies have also reported contradictory findings. While McLean (2018) reports a positive relationship between utilitarian and app engagement, this relationship was not significant in other studies (Hsiao et al., 2016; Tarute et al., 2017). In any context, the values of privacy and its benefits are subjective and vary between individuals (Crossler and Posey, 2017). However, in the context of this study, individuals who are attracted to the usefulness of the app are likely to have higher concerns for privacy and therefore, they are less likely to engage with a social media-enabled app.

4. Implications for Research

Prior studies on users' information disclosure or online platform usage have employed the privacy calculus as an appropriate investigative lens across several contexts. With privacy calculus as the theoretical basis, the current study investigates user engagement in social media-enabled apps and extends both costs and benefits dimensions of privacy calculus to explain users' engagement behavior.

- **A Dual Perspective on Privacy Concerns and their Antecedents**

Privacy in the social mobile era is more complex because of the involvement of multiple parties and the nature of data disclosure. Privacy control which is generally considered a key factor influencing privacy concerns was shown to only significantly affect social privacy concerns, not affecting institutional privacy concerns. As users share their private information, they assign different cost values and different antecedents to their institutional and social privacy concerns. Users' perceptions of privacy risk and control are entity/context-specific (Kehr et al., 2015) and despite being aware of the risk of sharing information on OSNs, they may have a false sense of control in managing the audience of their social network (Brandimarte et al., 2013).

- **Elaborating the Relative Influence of Enjoyment, Social and Efficiency Benefits**

This study also contributes to the understanding of the relationships between perceived benefits and user engagement with social media-enabled apps. According to prior literature, the general perception of benefits increases the user's likelihood of information disclosure (Wottrich et al., 2018). However, the findings of the present study indicate that specific benefits may have negative impact on user's engagement behavior. Although social, hedonic, and efficiency benefits in isolation may increase user engagement, the interplay of these benefits may not be appealing in certain contexts.

A further post hoc analysis based on age groups reveals that millennials engage more with the app than the older generations as they have lower perceived institutional privacy concerns, and higher social benefits. The older generation who are efficiency-driven users are more likely to perceive high social privacy concerns and limit their engagement with such apps. The opposite

direction of the effect of the different types of benefits suggests that users may perform a complex cost and benefit analysis when they decide to use the app. In the era of social mobile technology, the consideration of privacy is not straightforward and requires an intricate analysis of the overall effect of each separate factor.

5. Implications for Practice

The always-connected-always-carried-around nature of smartphones can lead to unprecedented privacy issues as evidenced by the recent privacy scandals (Wottrich et al., 2019). The findings from this study reinforce the need for privacy advocates and practitioners to move beyond adoption and focus on the privacy implications of user engagement with mobile apps as developers strive for an active user base and consider engagement as a key metric of success (Rutz et al., 2019).

Policy makers should seek to increase user awareness regarding both institutional and social aspects of privacy and caution users about the perception of control and how it may not protect their information if the threat arises from the institution that provides the app. Moreover, app developers should practice transparency in their data protection policies and provide adequate privacy-protecting measures and privacy controls to minimize the risk of repeating past privacy scandals and safeguard sensitive user data.

6. Conclusion and Future Research Directions

Privacy concerns are highly context-dependent (Kokolakis, 2017; Xu et al., 2011a) and the privacy research in the context of mobile apps is scarce (Kokolakis, 2017; Pentina et al., 2016). Prior literature suggests that acquiring needed information and satisfying one's social needs are the primary reasons for disclosing sensitive information on mobile apps, which echo with the privacy calculus framework (Pentina et al., 2016; Zafeiropoulou et al., 2013). The unique integration of social and user activity data makes social media-enabled apps an interesting context to examine privacy, especially the two types of social and institutional privacy concerns. This study reveals

different antecedents for these two types of privacy concerns. Regarding the research questions/study hypotheses, while the effect of information sensitivity on institutional privacy concerns is positive and significant (H3a), privacy risk positively and privacy control negatively impact social privacy concerns (H1b and H2b). Moreover, both institutional and social privacy concerns negatively impact user engagement (H4a and H4b), with social privacy concerns being the stronger predictor. Lastly, while the effects of social and enjoyment benefits were significant and positive as theorized (H5b and H5c), the efficiency benefit negatively affects user engagement (H5a). This study contributes to the literature of privacy on mobile apps by investigating the effects of both institutional and social privacy concerns on user engagement and identifying the distinct antecedents of these two types of privacy concerns.

Future investigation of this study should be extended to other demographics (e.g., baby boomers and elderly users) and possibly users from different countries and cultures to strengthen the generalizability of the results reported in this study. While this study supplemented survey results with a follow-up text analysis of user reviews, future research may want to examine users' in-app behaviors or other social media-enabled apps as user perceptions of functionality and information sensitivity could be different in the context of other social media-enabled apps. The current study focuses on the various benefits and expands the view of privacy concerns on app users' engagement. Future research could also consider other antecedents such as trust, usability, and self-efficacy in examining factors that are relevant to privacy calculus in the context of social mobile technologies.

References

Acquisti, A., Brandimarte, L., Loewenstein, G., 2015. Privacy and human behavior in the age of information. Science 347, 509–514.

Bansal, G., Gefen, D., 2010. The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. Decision support systems 49, 138–150.

Barth, S., De Jong, M.D., 2017. The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature review. Telematics and informatics 34, 1038–1058.

Bélanger, F., Crossler, R.E., 2011. Privacy in the digital age: a review of information privacy research in information systems. MIS quarterly 35, 1017–1042.

Bollen, K.A., 2014. Structural equations with latent variables. John Wiley & Sons.

Bordag, S., 2008. A comparison of co-occurrence and similarity measures as simulations of context, in: International Conference on Intelligent Text Processing and Computational Linguistics. Springer, pp. 52–63.

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

Breeden, J., 2014. Worried about security? Beware the mosaic effect [WWW Document]. GCN. URL https://gcn.com/articles/2014/05/14/fose-mosaic-effect.aspx (accessed 10.21.18).

Cadwalladr, C., Graham-Harrison, E., 2018. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The guardian 17, 22.

Cavusoglu, H., Phan, T.Q., Cavusoglu, H., Airoldi, E.M., 2016. Assessing the impact of granular privacy controls on content sharing and disclosure on Facebook. Information Systems Research 27, 848–879.

Charte, F., Rivera, A.J., del Jesus, M.J., Herrera, F., 2015. Addressing imbalance in multilabel classification: Measures and random resampling algorithms. Neurocomputing, Recent Advancements in Hybrid Artificial Intelligence Systems and its Application to Real-World Problems 163, 3–16.

Chou, C.H., Sinha, A.P., Zhao, H., 2010. Commercial Internet filters: Perils and opportunities. Decision Support Systems 48, 521–530.

Crossler, R.E., Bélanger, F., 2019. Why Would I Use Location-Protective Settings on My Smartphone? Motivating Protective Behaviors and the Existence of the Privacy Knowledge–Belief Gap. Information Systems Research 30, 995–1006.

Crossler, R.E., Posey, C., 2017. Robbing Peter to Pay Paul: Surrendering Privacy for Security's Sake in an Identity Ecosystem. Journal of the Association for Information Systems 18.

Culnan, M.J., Armstrong, P.K., 1999. Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. Organization science 10, 104–115.

Dewey, C., 2015. Why would anyone in her right mind use Venmo? Washington Post.

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

Dinev, T., Hart, P., 2004. Internet privacy concerns and their antecedents - measurement validity and a regression model. Behaviour & Information Technology 23, 413–422.

Dinev, T., McConnell, A.R., Smith, H.J., 2015. Research commentary—informing privacy research through information systems, psychology, and behavioral economics: thinking outside the "APCO" box. Information Systems Research 26, 639–655.

Dinev, T., Xu, H., Smith, H.J., Hart, P., 2013. Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. European Journal of Information Systems 22, 295–316.

Dogruel, L., Joeckel, S., Vitak, J., 2017. The valuation of privacy premium features for smartphone apps: The influence of defaults and expert recommendations. Computers in Human Behavior 77, 230–239.

Ebadi, N., Lwowski, B., Jaloli, M., Rad, P., 2019. Implicit Life Event Discovery From Call Transcripts Using Temporal Input Transformation Network. IEEE Access 7, 172178–172189.

Fornell, C., Larcker, D.F., 1981. Structural equation models with unobservable variables and measurement error: Algebra and statistics. Journal of marketing research 382–388.

Gal-Or, E., Gal-Or, R., Penmetsa, N., 2018. The role of user privacy concerns in shaping competition among platforms. Information Systems Research 29, 698–722.
Gerhart, N., Koohikamali, M., 2019. Social network migration and anonymity expectations: What anonymous social network apps offer. Computers in Human Behavior 95, 101–113.
Ghani, N.A., Hamid, S., Targio Hashem, I.A., Ahmed, E., 2019. Social media big data analytics: A survey. Computers in Human Behavior 101, 417–428.
Goes, P.B., Lin, M., Au Yeung, C., 2014. "Popularity Effect" in User-Generated Content: Evidence from Online Product Reviews. Information Systems Research 25, 222–238.
Gu, J., Xu, Y.C., Xu, H., Zhang, C., Ling, H., 2017. Privacy concerns for mobile app download: An elaboration likelihood model perspective. Decision Support Systems 94, 19–28.
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.
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.
Hann, I.H., Hui, K.L., Lee, S.Y.T., Png, I.P.L., 2007. Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach. Journal of Management Information Systems 24, 13–42.
Hays, R.D., Hayashi, T., Stewart, A.L., 1989. A five-item measure of socially desirable response set. Educational and psychological measurement 49, 629–636.
Heravi, A., Mubarak, S., Choo, K.K.R., 2018. Information privacy in online social networks: uses and gratification perspective. Computers in Human Behavior 84, 441–459.
Hong, W., Thong, J.Y., 2013. Internet privacy concerns: An integrated conceptualization and four empirical studies. Mis Quarterly 275–298.
Hsiao, C.H., Chang, J.J., Tang, K.Y., 2016. Exploring the influential factors in continuance usage of mobile social Apps: Satisfaction, habit, and customer value perspectives. Telematics and Informatics 33, 342–355.
Hsieh, J.J.P.A., Rai, A., Keil, M., 2008. Understanding Digital Inequality: Comparing Continued Use Behavioral Models of the Socio-Economically Advantaged and Disadvantaged. MIS Quarterly 32, 97–126.
Hu, Y., Xu, A., Hong, Y., Gal, D., Sinha, V., Akkiraju, R., 2019. Generating Business Intelligence Through Social Media Analytics: Measuring Brand Personality with Consumer-, Employee-, and Firm-Generated Content. Journal of Management Information Systems 36, 893–930.
Jiang, Z., Heng, C.S., Choi, B.C.F., 2013. Privacy Concerns and Privacy-Protective Behavior in Synchronous Online Social Interactions. Information Systems Research 24, 579–595.
Jordaan, Y., Van Heerden, G., 2017. Online privacy-related predictors of Facebook usage intensity. Computers in Human Behavior 70, 90–96.
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. Information Systems Journal 25, 607–635.
Khan, M.L., 2017. Social media engagement: What motivates user participation and consumption on YouTube? Computers in Human Behavior 66, 236–247.
Khanna, A., 2015. Venmo'ed: Sharing your payment data with the world. Technology Science 2015102901.
Kim, D., Park, K., Park, Y., Ahn, J.H., 2019. Willingness to provide personal information: Perspective of privacy calculus in IoT services. Computers in Human Behavior 92, 273–281.

Kim, Y.H., Kim, D.J., Wachter, K., 2013. A study of mobile user engagement (MoEN): Engagement motivations, perceived value, satisfaction, and continued engagement intention. Decision Support Systems 56, 361–370.

Kokolakis, S., 2017. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & security 64, 122–134.

Koohikamali, M., Peak, D.A., Prybutok, V.R., 2017. Beyond self-disclosure: Disclosure of information about others in social network sites. Computers in Human Behavior 69, 29–42.

Kordzadeh, N., Warren, J., 2017. Communicating Personal Health Information in Virtual Health Communities: An Integration of Privacy Calculus Model and Affective Commitment. Journal of the Association for Information Systems 18.

Krasnova, H., Spiekermann, S., Koroleva, K., Hildebrand, T., 2010. Online social networks: Why we disclose. Journal of information technology 25, 109–125.

Kwon, H.E., So, H., Han, S.P., Oh, W., 2016. Excessive Dependence on Mobile Social Apps: A Rational Addiction Perspective. Information Systems Research 27, 919–939.

Laufer, R.S., Wolfe, M., 1977. Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory. Journal of Social Issues 33, 22–42.

Law, D., Gruss, R., Abrahams, A.S., 2017. Automated defect discovery for dishwasher appliances from online consumer reviews. Expert Systems with Applications 67, 84–94.

Lee, C.S., Goh, D.H.L., Chua, A.Y.K., Ang, R.P., 2010. Indagator: Investigating perceived gratifications of an application that blends mobile content sharing with gameplay. Journal of the American Society for Information Science & Technology 61, 1244–1257.

Lev-Ram, M., 2017. PayPal's CEO on Venmo: Don't Mess Up the "Special Magic" [WWW Document]. Fortune. URL https://fortune.com/2017/11/17/dan-schulman-paypal-venmo/ (accessed 11.30.19).

Lim, J.S., Hwang, Y., Kim, S., Biocca, F.A., 2015. How social media engagement leads to sports channel loyalty: Mediating roles of social presence and channel commitment. Computers in Human Behavior 46, 158–167.

Liptak, A., 2019. The FTC is reportedly divided about how to hold Facebook accountable for privacy lapses [WWW Document]. The Verge. URL https://www.theverge.com/2019/5/4/18529490/federal-trade-commission-fine-facebook-divided-mark-zuckerberg-punishment-report (accessed 12.14.19).

MacCallum, R.C., Browne, M.W., Sugawara, H.M., 1996. Power analysis and determination of sample size for covariance structure modeling. Psychological Methods 1, 130–149.

Malhotra, N.K., Kim, S.S., Agarwal, J., 2004. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. Information systems research 15, 336–355.

Malhotra, N.K., Kim, S.S., Patil, A., 2006. Common Method Variance in IS Research: A Comparison of Alternative Approaches and a Reanalysis of Past Research. Management Science 52, 1865–1883.

Malm, S., 2018. Hushand divorces wife after seeing her with another man on Google Maps | Daily Mail Online [WWW Document]. URL https://www.dailymail.co.uk/news/article-6264139/Husband-divorces-wife-seeing-cuddling-man-Google-Maps.html (accessed 11.27.19).

Manning, C.D., Manning, C.D., Schütze, H., 1999. Foundations of statistical natural language processing. MIT press.

Marr, B., 2018. How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read [WWW Document]. Forbes. URL https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/ (accessed 10.21.18).

Mathwick, C., Malhotra, N., Rigdon, E., 2001. Experiential value: conceptualization, measurement and application in the catalog and Internet shopping environment☆11☆This article is

based upon the first author's doctoral dissertation completed while at Georgia Institute of Technology. Journal of Retailing 77, 39–56.
Matsuo, Y., Ishizuka, M., 2004. Keyword extraction from a single document using word co-occurrence statistical information. Int. J. Artif. Intell. Tools 13, 157–169.
McLean, G., 2018. Examining the determinants and outcomes of mobile app engagement-A longitudinal perspective. Computers in Human Behavior 84, 392–403.
National Institutes of Health, 2016. Definition of Human Subjects Research [WWW Document]. URL https://grants.nih.gov/policy/humansubjects/research.htm (accessed 12.2.19).
Nguyen, N., 2019. People On Venmo Are Being Harassed With A Flood Of Payment Requests [WWW Document]. BuzzFeed News. URL https://www.buzzfeednews.com/article/nicolenguyen/venmo-request-spam (accessed 12.13.19).
Norberg, P.A., Horne, D.R., Horne, D.A., 2007. The privacy paradox: Personal information disclosure intentions versus behaviors. Journal of Consumer Affairs 41, 100–126.
Nunnally, J.C., Bernstein, I.H., 1994. The Assessment of Reliability, in: Psychometric Theory. McGraw-Hill, Blacklick, Ohio, USA, pp. 248–292.
O'Brien, H.L., Toms, E.G., 2008. What is user engagement? A conceptual framework for defining user engagement with technology. Journal of the American society for Information Science and Technology 59, 938–955.
Office for Human Research Protections, 2016. Human subject regulations decision charts.
Ozdemir, Z.D., Smith, H.J., Benamati, J.H., 2017. Antecedents and outcomes of information privacy concerns in a peer context: An exploratory study. European Journal of Information Systems 26, 642–660.
Pentina, I., Zhang, L., Bata, H., Chen, Y., 2016. Exploring privacy paradox in information-sensitive mobile app adoption: A cross-cultural comparison. Computers in Human Behavior 65, 409–419.
Perro, J., 2018. Mobile Apps: What's A Good Retention Rate? http://info.localytics.com/blog/mobile-apps-whats-a-good-retention-rate.
PEW Research Center, 2019. Demographics of Social Media Users and Adoption in the United States. Pew Research Center: Internet, Science & Tech. URL https://www.pewresearch.org/internet/fact-sheet/social-media/ (accessed 11.27.19).
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, 879–903.
Poikela, M., Schmidt, R., Wechsung, I., Möller, S., 2015. FlashPolling privacy: the discrepancy of intention and action in location-based poll participation, in: Adjunct Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2015 ACM International Symposium on Wearable Computers. ACM, pp. 813–818.
Pour, M.S., Mangino, A., Friday, K., Rathbun, M., Bou-Harb, E., Iqbal, F., Shaban, K., Erradi, A., 2019. Data-driven Curation, Learning and Analysis for Inferring Evolving IoT Botnets in the Wild, in: Proceedings of the 14th International Conference on Availability, Reliability and Security, ARES '19. ACM, New York, NY, USA, pp. 6:1–6:10.
Raynes-Goldie, K., 2010. Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. First Monday 15.
Rocher, L., Hendrickx, J.M., De Montjoye, Y.A., 2019. Estimating the success of re-identifications in incomplete datasets using generative models. Nature communications 10, 1–9.
Rutz, O., Aravindakshan, A., Rubel, O., 2019. Measuring and forecasting mobile game app engagement. International Journal of Research in Marketing 36, 185–199.
Sen, S., Lerman, D., 2007. Why are you telling me this? An examination into negative consumer reviews on the web. Journal of interactive marketing 21, 76–94.

Sheehan, K.B., Hoy, M.G., 2000. Dimensions of Privacy Concern among Online Consumers. Journal of Public Policy & Marketing 19, 62–73.
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, 473–511.
Smith, B.G., Gallicano, T.D., 2015. Terms of engagement: Analyzing public engagement with organizations through social media. Computers in Human Behavior 53, 82–90.
Smith, H.J., Dinev, T., Xu, H., 2011. Information Privacy Research: An Interdisciplinary Review. MIS Quarterly 35, 989–1016.
Smith, H.J., Milberg, S.J., Burke, S.J., 1996. Information privacy: measuring individuals' concerns about organizational practices. MIS quarterly 167–196.
Statcounter, 2019. Desktop vs Mobile vs Tablet Market Share United States Of America [WWW Document]. StatCounter Global Stats. URL https://gs.statcounter.com/platform-market-share/desktop-mobile-tablet/united-states-of-america (accessed 11.27.19).
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, 248–273.
Tarute, A., Nikou, S., Gatautis, R., 2017. Mobile application driven consumer engagement. Telematics and Informatics 34, 145–156.
Trepte, S., Scharkow, M., Dienlin, T., 2020. The privacy calculus contextualized: The influence of affordances. Computers in Human Behavior 104, 106115.
Vallina-Rodriguez, N., Sundaresan, S., 2017. 7 in 10 smartphone apps share your data with third-party services. The Conversation.
Venkatesh, V., Brown, S.A., 2001. A Longitudinal Investigation of Personal Computers in Homes: Adoption Determinants and Emerging Challenges. MIS Quarterly 25, 71–102.
Wainer, J., Cawley, G., 2017. Empirical Evaluation of Resampling Procedures for Optimising SVM Hyperparameters 35.
Wang, X., Liu, Z., 2019. Online engagement in social media: A cross-cultural comparison. Computers in Human Behavior 97, 137–150.
Warkentin, M., Johnston, A.C., Walden, E., Straub, D.W., 2016. Neural Correlates of Protection Motivation for Secure IT Behaviors: An fMRI Examination. Journal of the Association for Information Systems; Atlanta 17, 194–215.
Westin, A.F., 2003. Social and political dimensions of privacy. Journal of social issues 59, 431–453.
Widjaja, A.E., Chen, J.V., Sukoco, B.M., Ha, Q.A., 2019. Understanding users' willingness to put their personal information on the personal cloud-based storage applications: An empirical study. Computers in Human Behavior 91, 167–185.
Wottrich, V.M., Reijmersdal, E.A. van, Smit, E.G., 2019. App Users Unwittingly in the Spotlight: A Model of Privacy Protection in Mobile Apps. Journal of Consumer Affairs 53, 1056–1083.
Wottrich, V.M., van Reijmersdal, E.A., Smit, E.G., 2018. The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns. Decision support systems 106, 44–52.
Xu, F., Michael, K., Chen, X., 2013. Factors affecting privacy disclosure on social network sites: an integrated model. Electronic Commerce Research 13, 151–168.
Xu, H., Bélanger, F., 2013. Information systems journal special issue on: Reframing privacy in a networked world. Information systems journal 23, 371–375.
Xu, H., Dinev, T., Smith, J., Hart, P., 2011a. Information privacy concerns: Linking individual perceptions with institutional privacy assurances. Journal of the Association for Information Systems 12, 1.

Xu, H., Luo, X. (Robert), Carroll, J.M., Rosson, M.B., 2011b. The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. Decision Support Systems 51, 42–52.

Xu, H., Teo, H.H., Tan, B.C., Agarwal, R., 2009. The role of push-pull technology in privacy calculus: the case of location-based services. Journal of Management Information Systems 26, 135–174.

Zafeiropoulou, A.M., Millard, D.E., Webber, C., O'Hara, K., 2013. Unpicking the Privacy Paradox: Can Structuration Theory Help to Explain Location-based Privacy Decisions?, in: Proceedings of the 5th Annual ACM Web Science Conference, WebSci '13. ACM, New York, NY, USA, pp. 463–472.

Zarouali, B., Poels, K., Ponnet, K., Walrave, M., 2018. "Everything under control?": Privacy control salience influences both critical processing and perceived persuasiveness of targeted advertising among adolescents. Cyberpsychology: Journal of Psychosocial Research on Cyberspace 12.

Zhang, X., Tang, S., Zhao, Y., Wang, G., Zheng, H., Zhao, B.Y., 2017. Cold hard E-cash: Friends and vendors in the Venmo digital payments system, in: Eleventh International AAAI Conference on Web and Social Media.

Zhao, L., Lu, Y., Gupta, S., 2012. Disclosure intention of location-related information in location-based social network services. International Journal of Electronic Commerce 16, 53–90.

Zhou, Q., Xu, Z., Yen, N.Y., 2019. User sentiment analysis based on social network information and its application in consumer reconstruction intention. Computers in Human Behavior 100, 177–183.

Appendix I: Survey Instruments

Title	Construct	Reference
IS	**Information Sensitivity**	
ISN_1	I do not feel comfortable with the type of information P2P payment apps request from me.	(Dinev et al., 2013)
ISN_2	I feel that P2P payment apps gather highly personal information about me.	
ISN_3	The information I provide to P2P payment apps is very sensitive to me.	
PC	**Privacy Control**	
PC_1	I believe I have control over who can get access to my personal information collected by P2P payment apps.	(Malhotra et al., 2004; Xu and Bélanger, 2013)
PC_2	I think I have control over what personal information is released by P2P payment apps.	
PC_3 (Dropped)	I believe I have control over how personal information is used by P2P payment apps.	
PC_5	I believe I can control my personal information provided to P2P payment apps.	
PR	**Privacy Risk**	
PR_1	In general, it would be risky to give personal information to P2P payment apps.	(Malhotra et al., 2004; Xu et al., 2011b)
PR_2	There would be high potential for privacy loss associated with giving personal information to P2P payment apps.	
PR_3	Personal information could be inappropriately used by P2P payment apps.	
PR_4 (Dropped)	Providing P2P payment apps with my personal information would involve many unexpected problems.	
SPC	**Social Privacy Concerns**	
SPC_1R (Reversed)	I am not concerned that the personal information I share on P2P payment apps could be misused by other users.	(Jiang et al., 2013; Malhotra et al., 2004)
SPC_2R (Reversed)	I am not concerned that the transaction information I share on P2P payment apps could be misused by other users.	
SPC_3 (Dropped)	I believe that leaving my personal information public on P2P payment apps could threaten my privacy.	
SPC_4 (Dropped)	I believe that leaving my transaction information public on P2P payment apps could threaten my privacy.	
SPC_5 (Dropped)	I am concerned that any user on P2P payment apps may access my personal information.	
SPC_6 (Dropped)	I am concerned that any user on P2P payment apps may access my transaction information.	
IPC	**Institutional Privacy Concerns**	
IPC_1	P2P payment app companies should disclose the way the data are collected, processed, and used.	(Malhotra et al., 2004)
IPC_2	A good P2P payment app privacy policy should have a clear and conspicuous disclosure.	
IPC_3	It is very important to me that I am aware and knowledgeable about how my personal information will be used.	
EFB	**Efficiency Benefits**	

EFB_1	Making and receiving payments from P2P payment apps is a convenient way to manage my time.	(Mathwick et al., 2001)
EFB_2	Making and receiving payments from the app makes my life easier.	
EFB_3	Making and receiving payments from the app fits with my schedule.	
SB	**Social Benefits**	
SB_1	To make a good impression on other people	(Jiang et al., 2013)
SB_2	To have a good reputation among other people	
SB_3 (Dropped)	To add to my uniqueness	
Title	**Construct**	**Reference**
ENB	**Enjoyment Benefits**	
EBN_1	I find using P2P payment apps to be enjoyable.	(Hsieh et al., 2008)
EBN_2	The actual process of using P2P payment apps is pleasant.	
EBN_3	I have fun using P2P payment apps.	
ENG	**Engagement**	
ENG1	I post likes and comments on other's transactions on P2P payment apps.	(Khan, 2017; Lim et al., 2015; Smith and Gallicano, 2015)
ENG2	I express my feelings about transactions on P2P payment apps.	
ENG3 (Dropped)	I interact with others socially on P2P payment apps.	
ENG4	Anything related to P2P payment apps grabs my attention.	
ENG5 (Dropped)	I spend a lot of time on P2P payment apps.	
SDB	**Social Desirability Bias**	
SDB_1	I am always courteous even to people who are disagreeable. I am always courteous even to people who are disagreeable.	(Hays et al., 1989)
SDB_2	No matter who I'm talking to, I'm always a good listener.	
SDB_3	I am always willing to admit it when I make a mistake.	
SDB_4	I have never intensely disliked anyone.	
SDB_5	I would never think of letting someone else be punished for my wrongdoings.	

Control Variables

AGE	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**	**(6)**	**(7)**	**(8)**
	25 and below	36 – 30	31 – 35	36 – 40	41 – 45	46 – 50	51 – 55	Above 55
EDU	**(1)**		**(2)**		**(3)**		**(4)**	
	High school or less		Some college		Undergraduate/bachelor's degree		Graduate	
GENDER	**(0)**				**(1)**			
	Male				Female			
TIME	How long have you been using P2P payment apps?							
	(1)	**(2)**	**(3)**	**(4)**	**(5)**			
	Less than a month	Less than 6 months	6 months to 1 year	1 to 2 years	More than 2 years			
VICT	When it comes to the privacy invasion of information, my experience could be characterized as:							
	(1)			**(2)**				
	Never victimized			Definitely victimized				
PUBLIC	What is the privacy settings on the P2P payment app that you use?							
	(1)	**(2)**	**(3)**	**(4)**				
	Public (everyone can see my transactions)	Friends (my friends can see my transactions)	Private (only I can see my transactions)	I don't know my privacy settings				

Appendix II: Item loadings and cross-loadings

	ENG	PC	EFB	IPC	PR	SB	EBN	ISN	SPC
ENG_A_2	0.95	-0.02	0.00	0.04	-0.05	-0.10	-0.04	0.00	0.04
ENG_A_1	0.89	-0.01	0.01	0.07	0.06	0.00	-0.11	-0.07	-0.10
ENG_A_4	0.88	-0.02	0.02	0.02	0.02	-0.01	-0.07	-0.11	0.01
ENG_A_6	0.67	-0.05	-0.03	-0.08	-0.03	0.00	0.15	0.11	-0.02
ENG_A_5	0.60	0.06	0.03	-0.01	-0.01	0.15	0.14	0.06	0.07
PC_4	0.03	0.96	0.00	0.03	-0.04	0.00	-0.07	0.02	0.01
PC_5	-0.08	0.88	-0.01	0.01	-0.01	-0.02	0.05	-0.03	0.03
PC_1	0.02	0.82	0.02	-0.02	0.07	0.00	0.00	-0.02	-0.07
EFB_3	-0.03	0.01	0.92	-0.02	0.00	0.07	-0.05	0.02	0.02
EFB_1	0.04	-0.03	0.86	-0.03	0.06	-0.04	0.03	-0.06	-0.04
EFB_2	0.00	0.02	0.83	0.01	-0.07	-0.05	0.06	0.06	0.03
IPC_2	-0.01	-0.05	-0.03	0.97	0.00	0.06	0.01	-0.03	-0.06
IPC_1	0.00	0.01	0.03	0.87	-0.02	-0.04	-0.01	-0.01	0.01
IPC_3	0.06	0.07	-0.04	0.77	0.04	-0.03	0.06	0.10	0.08
PR_2	-0.01	0.00	-0.02	-0.08	0.91	0.01	0.06	-0.03	0.05
PR_1	-0.01	0.04	-0.05	0.00	0.89	0.00	0.00	0.00	-0.05
PR_3	0.01	-0.04	0.09	0.15	0.66	0.05	-0.05	0.06	0.01
SB_1	-0.04	-0.04	-0.05	0.03	0.01	0.95	0.03	-0.03	0.01
SB_2	-0.02	0.00	0.06	0.00	0.05	0.94	-0.07	-0.02	-0.02
SB_3	0.22	0.08	-0.04	-0.13	-0.09	0.44	0.07	0.13	0.03
EBN_1	-0.01	-0.04	0.00	0.02	-0.01	-0.03	0.93	-0.04	0.01
EBN_2	-0.10	-0.02	0.06	0.07	0.02	0.01	0.80	-0.01	-0.05
EBN_3	0.13	0.07	0.00	-0.04	0.01	0.00	0.70	-0.01	0.00
ISN_2	-0.08	-0.01	0.01	0.00	-0.07	0.04	-0.05	0.93	-0.05
ISN_3	0.01	-0.01	0.02	0.18	0.03	-0.02	0.00	0.72	0.01
ISN_1	0.06	-0.01	-0.04	-0.19	0.23	-0.11	-0.01	0.51	0.02
SPC_1R	-0.01	0.02	0.02	0.00	-0.02	-0.02	-0.01	-0.02	0.91
SPC_2R	-0.01	-0.05	-0.01	0.03	0.04	0.02	-0.02	-0.02	0.86

Appendix III: T-test Analysis

In order to account for the variation in responses due to age differences, the dataset was split in two groups: (a) millennials, and (b) older generations. In our questionnaire, age is recorded as a

categorical variable. Those who reported their age as 35 and below are considered millennials (N = 231), and the rest as older generations (N = 123). The results of an independent samples t-test suggests that while millennials report a lower average Institutional privacy concerns, they perceive higher social benefits in using social media enabled apps.

Group Statistics

Variable	Age group	N	Mean	Std. Deviation	Std. Error Mean
IPC	Millennial	231	6.0765	1.13505	.07468
	Older	123	6.3604	1.10932	.10002
SB	Millennial	231	4.8268	1.33037	.08753
	Older	123	4.4878	1.35723	.12238

Independent Samples Test

Variable	Levene's Test		t-test for Equality of Means						
	F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% CI	
								Lower	Upper
IPC	2.820	.094	-2.259	352	.025	-.28395	.12571	-.53118	-.03672
SB	.029	.866	2.267	352	.024	.33903	.14954	.04493	.63314

Appendix IV: Labeling Protocol

This protocol was used for labeling and preparing the sample dataset used for training the classification model. The protocol provides a definition, keyword dictionary, and examples for labeling the data.

Aspect	Guideline	
Efficiency Positive / Negative	Describes a reviewer's opinion about functionality and efficiency of Venmo.	
	Keywords: easy, convenience, convenient, handy, fast, works, quick, simple, useful, free, no fee, sufficient, user friendly, instant, immediate, immediately, slow, wait, complicated, confusing, long, longer, time, delay, forever.	
	Examples	
	Positive	**Negative**
	"Works great for splitting up things amongst friends."	*"Don't ever expect instant transfer to work."*
Social Positive / Negative	Describes reviewer's opinion about the social aspect of Venmo.	
	Keywords: social, social media, private, privacy, public, see, seeing, comment, like, follow, invasive,	
	Examples	
	Positive	**Negative**

	"It's awesome I love reading the public comments, lol."	*"Don't like how you can see friends activity, I feel it's an invasion of privacy."*
Fun Positive	Describes reviewer's opinion about the fun and entertaining aspect of Venmo.	
	Keywords: fun, funny, enjoy, cool, cute, amusing, exciting, dull	
	Examples	
	Positive	**Negative**
	"Super handy, and using emojis is fun."	---

Mohsen Jozani: Conceptualization, Methodology, Validation, Data Curation, Writing - Original Draft, Writing - Review & Editing; **; Emmanuel Ayaburi**: Conceptualization, Methodology, Validation, Data Curation, Writing - Review & Editing, Supervision; **Myung Ko**: Conceptualization, Methodology, Validation, Writing - Original Draft; **Kim-Kwang Raymond Choo**: Conceptualization, Methodology, Writing - Review & Editing, Supervision

1. Privacy risk is positively related to social privacy concerns
2. Privacy control is negatively related to social privacy concerns
3. Information sensitivity is positively related to institutional privacy concerns
4. Institutional privacy concerns are negatively related to engagement
5. Social privacy concerns are negatively related to engagement