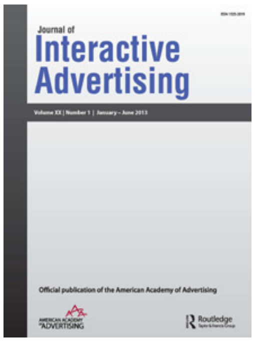
Consumers' Privacy Concern and Privacy Protection on Facebook in the Era of Big Data: Empirical Evidence from College Students

Article *in* Journal of Interactive Advertising · August 2019

DOI: 10.1080/15252019.2019.1651681

Wenjing Xie
Marist College



Journal of Interactive Advertising

Routledge
Taylor & Francis Group

ISSN: (Print) 1525-2019 (Online) Journal homepage: https://www.tandfonline.com/loi/ujia20

Consumers' Privacy Concern and Privacy Protection on Social Network Sites in the Era of Big Data: Empirical Evidence from College Students

Wenjing Xie & Kavita Karan

To cite this article: Wenjing Xie & Kavita Karan (2019): Consumers' Privacy Concern and Privacy Protection on Social Network Sites in the Era of Big Data: Empirical Evidence from College Students, Journal of Interactive Advertising, DOI: 10.1080/15252019.2019.1651681

To link to this article: https://doi.org/10.1080/15252019.2019.1651681

Accepted author version posted online: 01 Aug 2019.
Published online: 04 Sep 2019.

JOURNAL OF INTERACTIVE ADVERTISING
https://doi.org/10.1080/15252019.2019.1651681

Routledge
Taylor & Francis Group

Consumers’ Privacy Concern and Privacy Protection on Social Network Sites in the Era of Big Data: Empirical Evidence from College Students

Wenjing Xie[a] and Kavita Karan[b]

[a]School of Communication and the Arts, Marist College, Poughkeepsie, New York, USA; [b]School of Journalism, Southern Illinois University Carbondale, Carbondale, Illinois, USA

ABSTRACT

Information privacy and disclosure have been prominent issues revolving around social media. We adopted communication privacy management theory, the persuasion knowledge model, and the technology acceptance model and conducted a survey with 526 subjects and examined their privacy management on Facebook and the conditions upon which their decision to reveal or withhold private information was contingent. The results showed that consumers set up different privacy boundaries for different types of personal information. Social identity information and daily life and entertainment information tended to be shared more freely, while personal contact information was mostly withheld. Knowledge of and concern regarding technology ubiquity and companies’ business strategies involving big data were the strongest predictors of privacy protection behavior and privacy settings on Facebook. Online trust and Facebook intensity also interacted and jointly predicted privacy concerns. This study brought to researchers’ attention how big data are being used by marketers to target consumers.

KEYWORDS

Facebook; big data; ubiquity; privacy; communication privacy management

The ubiquity of mobile Internet and the era of big data are changing the ways that businesses collect and use personal data and intrude on consumers’ privacy. In marketing domains, the term *big data* refers to data from social media profiles, global positioning systems (GPS), cookies, search engines, and credit and loyalty reward cards that companies depend on to track and understand consumer behavior (Eastin et al. 2016). Big data help companies understand shoppers via digital touch points—from their online browsing and purchases to their presence on social network sites. Customer interaction management is envisaged as the key to success in the era of big data. It manages customer information across multiple touch points, including the Internet, mobile phones, social media, and offline channels (Martin and Murphy 2017). Big data analytics and social media marketing strategies provide more relevant interactions with customers, leading to more profitable and longer-lasting relationships (Uzialko 2018).

In the ongoing onslaught of businesses targeting consumers, questions have been raised about privacy invasion by marketers and how much data people are willing to share in exchange for benefits on social media (Limpf and Voorveld 2015). Despite the Federal Trade Commission’s warnings about the potential risks of online browsing and purchasing behavior, consumers continue to share their personal information in such trade-offs. Privacy has been a prominent problem on social media, as third parties can trace and obtain consumer information for marketing purposes (Tufekci 2008). Privacy is also challenged by the unprecedented diffusion of mobile Internet and the fast penetration of devices that can be used for accessing the Internet, such as smartphones (Okazaki and Hirose 2009). By adopting the communication privacy management (CPM) theory, the persuasive knowledge model (PKM), and the technology acceptance model (TAM), this study aims (1) to understand the status of privacy concerns and privacy protection behavior in social media advertising context; (2) to understand how consumers’ previous experiences are related to privacy concerns and privacy protection on Facebook; (3) to understand young

CONTACT Wenjing Xie ✉ wjjwxie@gmail.com School of Communication and the Arts, Marist College, 3399 North Road, Poughkeepsie, NY 12601, USA.

Color versions of one or more of the figures in the article can be found online at www.tandfonline.com/ujia.

Wenjing Xie (PhD, University of Maryland College Park) is an associate professor of communication, Communication Department, School of Communication and the Arts, Marist College.
Kavita Karan (PhD, University of London) is a professor, School of Journalism, Southern Illinois University Carbondale.

consumers' knowledge and concerns regarding technology ubiquity and advertisers' business strategies involving big data analytics; (4) to explore how consumers' trust and Facebook use interact; and (5) to provide suggestions to marketers and advertisers regarding the use of consumers' information with big data analytics.

CPM theory (Petronio 2002) has been widely used in explaining the dynamics between privacy protection and disclosure behavior in face-to-face situations. Recent studies have applied CPM theory in computer-mediated communication, but they mainly focus on privacy management in online advertising (Metzger 2007), health-related activities (Brinson, Eastin, and Bright 2019), general social media use (Child, Haridakis, and Petronio 2012), and adoption of mobile commerce activities (Eastin et al. 2016). However, privacy issues in social media advertising warrants special consideration and more research is still needed to extend CPM theory to the domain of social media advertising. First, compared with online advertising and e-commerce, social media poses special risks, such as phishing scams, to consumer privacy (Kumar, Saravanakumar, and Deepa 2016). The term *phishing* refers to attackers' attempt to obtain sensitive user information, such as passwords and financial information, by disguising themselves as a trustworthy entity in electronic communication (Ramzan 2010). Though phishing used to happen with e-mails, more attackers are now collecting personal information that people disclose on social media, and many Facebook accounts are used for phishing-type attacks through fake profiles, friend requests, and fake advertisements (Vishwanath, Harrison, and Yu 2018). Such social media spamming is more effective than e-mail spamming because the spammers can gain the trust of their victims by obtaining information about the victims' friends, personal hobbies, and shopping preferences (Karanja et al. 2018).

Second, social media advertising relies on self-disclosure of personal information, such as hobbies, birthdates, and demographics. Thus, compared to e-mail or online advertising, it is easier for third parties to collect consumer information on social media (Limpf and Voorveld 2015). Third, research shows that social media privacy settings for general social media use and advertising purposes are different (Heyman, De Wolf, and Pierson 2014). Users are granted more control over interpersonal information flow toward other users in general social media use. However, users are unable to opt out of targeted advertising, such as Facebook's ad exchange or "sponsored stories." Fourth, with users' self-disclosure of private information on social media, it is easier for advertisers to deliver personalized advertising and financial incentives, such as coupons and discount information (Ardiansyah et al. 2018), which may make consumers give up privacy protection despite high privacy concerns, a phenomenon labeled as privacy paradox (Barnes 2006).

In the social media advertising context, Facebook use is of special interest. Facebook has the highest market share among all types of social media (Smith and Anderson 2018). It is also the most popular social media advertising channel, with 93% of marketers using Facebook ads and 67% planning on increasing their use of Facebook ads in the coming year (Stelzner 2018). Despite privacy-related controversies stemming from the Facebook data breach in 2018, Facebook earnings and revenues in the last quarter of 2018 still beat estimates (Jagerson 2019). The intensive use of Facebook ensures greater opportunities for and continued interest of marketers in advertising on Facebook.

Though previous research on social media privacy has identified factors that contribute to privacy concerns and privacy protection, consumers' knowledge of big data analytics and technology ubiquity has not received much attention. PKM, a theory that examines the role of knowledge in people's cognitive responses to mediated messages, and TAM, a model widely used to explain people's technology adoption behavior, may shed light on the understanding of consumers' privacy protection on social media in the era of big data. Based on a survey of 526 undergraduate and graduate students, this study adopts CPM theory, PKM, and TAM and aims to gain profound insights into consumers' privacy concerns and privacy management on Facebook in the era of big data.

Literature Review

Communication Privacy Management Theory

CPM theory originated from research on privacy regulation in interpersonal communication (Petronio 2002). It views disclosure as a dialectical process of revealing and withholding information and argues that disclosure has both benefits and risks (Petronio 2002; Petronio and Durham 2015). The benefits ranged from relationship development to social control. The risks of disclosure include loss of control, social status, and face. Hence, people need to consider the dialectical tension between benefits and risks and make the decision regarding withholding or disclosing private information. It provides a theoretical framework to understand how people develop rules and set up boundaries in interpersonal communication.

CPM theory proposes three processes of private information boundary management. The first process, *boundary rule formation*, refers to the process of defining boundary rules that regulate when and how to reveal personal information. According to Petronio (2002), when people withhold personal information, the information resides within their individual privacy boundary, and a personal boundary is established. However, when individuals share information with others, the information belongs to the relationship, and a collective boundary is established. When the information resides in the collective boundary, risks such as loss of control will increase. The second process is *boundary coordination*, meaning people use different strategies to control and protect private information. During this process, individuals negotiate privacy rules with partners and decide to grant or deny access to personal information. The third process is *boundary turbulence*, referring to the readjustment or recalibration of privacy management after privacy rule violation (Child, Haridakis, and Petronio 2012).

One key concept in CPM theory is boundary, which describes the transactional nature of private information management in a relationship. The boundary is "thick" when people disclose less information and gets "thinner" when the extent of disclosure increases (Petronio 2002). Moreover, CPM theory contends that there can be multiple layers of boundaries for shared information. For instance, people can establish different privacy boundaries with partners, coworkers, family, and advertisers, and disclose private information at different levels (Petronio and Durham 2015).

Application of CPM Theory in the Context of Social Media and Advertising

Though CPM theory was developed for offline communication, in recent years it has been applied to social media research (Jin 2013; Petronio and Durham 2015). First, in terms of boundary rule formation, both benefits and risks exist in the context of social media. Social media is not only a platform for social networking but also an effective channel for marketing and advertising (Khang, Ki, and Ye 2012). Nevertheless, social media use may result in unexpected consequences, such as online stalking, identity theft, and financial loss. Depending on risks and benefits, people can decide to withhold or share information with advertisers. Second, Petronio (2002) proposed that boundary coordination can be operated through the control of boundary coownership, boundary linkage, and boundary permeability. In the social media context, boundary coordination can be accepting "friend" request, posting demographics, lurking, and posting photos or videos.

Research has shown that people adopt different strategies to set up privacy boundaries to control information flow in different social, cultural, and motivational conditions (Child, Haridakis, and Petronio 2012). In the realm of online advertising, Metzger (2007) studied online consumer privacy management and found that e-commerce participants set up different boundaries around different types of information. They tended to withhold or falsify more sensitive information, such as Social Security numbers, names, and previous online purchases. Prince (2018) found that online consumers' propensity to use privacy protection from online advertisers is driven by types of personal information. Regarding general social media use, scholars have noted that social media users manage different privacy boundaries with various levels of self-censorship (Winsiewski et al. 2017). Jin (2013) found that information about daily life and entertainment was disclosed most easily on Twitter, while information about mental and physical health was most concealed. Based on these studies, it is possible that consumers use the thickest boundary to protect information related to personal safety from advertisers and adopt thinner boundaries for other types of information.

H1: Consumers will set up different privacy boundaries for different types of personal information on Facebook to prevent marketers' data collection, with information related to personal safety being more private than other types of information.

Previous Experience

CPM theory predicts that information disclosure is contingent upon certain rules, conditions, and factors (Petronio 2002), and previous experience is one such factor. Previous experience refers to feedback from personal experiences associated with the targeted maladaptive or adaptive responses (Nisbett and Ross 1980). Heuristics and biases research suggest that people make judgments of perceived vulnerability and behavioral decisions based on limited information and cognitive abilities; heuristics underlie such judgments (Tversky and Kahneman 1974). As an individual's cumulative experience of events, prior experiences would affect his or her heuristics and behavioral decisions. The easier it is to retrieve an event, the greater the chance that the individual thinks similar events will occur again in the future. Based on heuristics research, scholars found that people use previous experiences to predict future circumstances (Nisbett and Ross 1980).

Research has shown that previous positive Internet and e-commerce experiences decrease consumers' online risk perceptions and increase willingness for self-disclosure (Metzger 2007). Online shopping often offers many incentives and has become commonplace. Consumers who often shop on the Internet are likely to share their personal information for these benefits (Youn 2009). As an increasing number of social media users are migrating to mobile phones, mobile Internet and mobile apps are turning out to be an effective way of marketing (Brinson, Eastin, and Bright 2019). Previous positive mobile shopping experiences might help consumers reduce perceptions of online risks. Therefore, frequent mobile shoppers may be more willing to trade personal information for convenience, discounts, and other benefits.

> **H2a:** People who shop frequently via their mobile phones are less likely to set their Facebook information to private.

Nevertheless, CPM theory proposes that if the privacy rule is violated, people may experience privacy boundary turbulence and redefine boundary ownership rights and readjust the information revealed to others (Eastin et al. 2016; Petronio 2002). Heuristics research also suggests that previous negative life events are positively associated with perception of vulnerability to risks (Tversky and Kahneman 1974). Research has demonstrated that negative experiences from past online disclosures heighten consumers' online risk perceptions (Yang and Liu 2014), decrease consumers' willingness to disclose information in subsequent transactions (Metzger 2007), and increase advertising avoidance on the Internet (Yang and Liu 2014).

> **H2b:** People with negative online experiences are more likely to protect privacy on Facebook from advertisers and set information to private.

Persuasion Knowledge Model and Knowledge of Business Strategies

CPM theory argues that people's privacy management may depend on intrapersonal and contextual factors (Petronio 2002), and scholars suggested knowledge is one of the intrapersonal factors (Liu et al. 2017; Youn 2009). PKM offers a theoretical perspective in understanding the cognitive process of responses to commercial messages and the role of knowledge in privacy management (Brinson and Eastin 2016). PKM studies how consumers perceive marketers' efforts and strategies to persuade them and how they cope with such business strategies (Friestad and Wright 1994). According to this model, consumers are repeatedly exposed to persuasion messages such as advertisements. Over time, consumers can develop persuasion knowledge about the tactics marketers use in their persuasion attempts, which will help them identify how, when, and why marketers try to persuade them and how to adaptively respond to these persuasion attempts (Friestad and Wright 1994). PKM posits that the more persuasion knowledge about the marketing attempts the consumers have, the more likely they are to develop skepticism and reject the promotion (Friestad and Wright 1994). In the modern age of big data, consumers' persuasion knowledge can accumulate from multiple sources, including observations of marketers' persuasion attempts and other consumers' online comments (Brinson and Eastin 2016).

Echoing PKM, researchers have found that the ad message in nontraditional advertising, such as advertorials, reduces consumers' ability to identify the ad and the perceived persuasive intent (Attaran, Notarantonio, and Quigley 2015). Studies also have extended PKM to online shopping, in-game shopping, and native advertising (Jung and Heo 2019; Nelson, Keum, and Yaros 2004) and found that as online gamers are knowledgeable about the in-game advertisements, they tend to install ad blocking software or ignore product placement messages. Liu et al. (2017) found that people with more privacy knowledge change Facebook privacy settings more frequently. Smit, Noor, and Voorveld's (2014) study discovered that people with different levels of privacy concerns and privacy coping strategies differ in their knowledge of technologies, such as cookies and big data analytics.

> **H3:** Knowledge of companies' business strategies using big data technologies will be positively related to consumers' **(a)** concerns regarding private information being collected by advertisers and **(b)** privacy protection behavior on Facebook.

> **H4:** Concern about data breaches in the era of big data will be positively related to consumers' **(a)** privacy concerns and **(b)** privacy protection behavior on Facebook.

Technology Acceptance Model and Ubiquity of Technologies

As one of the basic theories in psychology, TAM (Davis, Bagozzi, and Warshaw 1989) provides insights into consumer online behavior. It builds on the fundamental assumption that one's attitude and behavioral intention lead to actual behavior. The original TAM proposed that perceived usefulness and perceived ease of use were the two most important factors predicting technology use (Davis, Bagozzi, and Warshaw 1989). Enhancements to TAM integrated more factors into this model, including social influence (Venkatesh and Davis 2000; Venkatesh and Bala 2008), privacy (Choi 2018), and perceived risks (Pavlou 2003). TAM has been applied in predicting consumers' intentions and behaviors, including using information systems, privacy concerns, and information-sharing behavior in e-commerce and mobile commerce (m-commerce) transactions (Choi 2018; Pavlou 2003). Based on TAM, Gupta and Chennamaneni (2018) found that older social media users' privacy concerns led to more privacy protection in online interactions.

> **H5:** Consumers' privacy concerns regarding information being collected by advertisers using big data technologies will be positively related to **(a)** the adoption of privacy protection behavior and **(b)** privacy settings on Facebook.

More recently, scholars integrated perceived ubiquity of technologies into TAM. Ubiquity refers to the idea that technologies have been integrated into our physical living environment (Hallnäs and Redström 2002). Weiser (1991) proposed the concept of ubiquitous computing, where computers are no longer the tools for work but are devices available anywhere, at any time. In the ultimate ideal situation of ubiquitous computing, computers or other devices would "disappear" and become a part of the user (Hallnäs and Redström 2002). In recent years the unprecedented growth of social media, GPS use, and the Internet of Things (IOT) has pushed the boundary of ubiquity even further (Thielst 2011; Tucker 2014). CPM predicts that various contextual factors may influence privacy control. Previous research applying CPM has examined contextual factors such as network diversity (Beam et al. 2018), ease of use, and perceived benefits (Pavlou 2003). However, technology ubiquity has received limited attention. Okazaki, Li, and Hirose (2009) argued that ubiquity is a unique feature of social media and mobile Internet, enabling consumers to search for information in any place, at any time. Thus, it is reasonable to include ubiquity of technologies as a construct in our research and to link it with CPM.

Research has revealed that consumers' perceptions of ubiquity of technologies could have direct or indirect effects on the adoption of m-commerce (Choi 2018). However, scholars also have pointed out that ubiquity may increase consumers' concerns about the intrusion of privacy by ubiquitous technologies. For instance, Westin (2003) argued that privacy was not an issue when information technologies were in a newer stage. Nonetheless, with the arrival of the Internet and advances in ubiquitous mobile technologies, the public has become aware of the threat to privacy as marketers, advertisers, and other third parties can easily access consumer's personal information. Research has shown how the advent of GPS-based mobile phones and location-based services have provoked consumer privacy concerns (Okazaki, Li, and Hirose 2009).

> **H6:** Consumers' knowledge about technology ubiquity will be positively related to their **(a)** privacy concerns regarding information being collected by advertisers and **(b)** privacy protection behavior.

> **H7:** Consumers who are concerned about technology ubiquity will **(a)** be more concerned regarding private information being collected by advertisers and **(b)** take more privacy protection measures on Facebook.

Trust and Facebook Intensity

According to CPM theory, people believe their personal information is protected by privacy boundaries. When experiencing privacy turbulence, their trust in privacy co-owners will be lost. Thus, privacy concerns will increase, and new privacy management rules will be developed (Metzger 2007). Trust is viewed as a psychological state in which people expect another party to perform an action predictably, fulfill responsibilities, and behave fairly. In marketing research, trust is a crucial antecedent for active participation in e-commerce as it is an effective way to reduce uncertainty (Pavlou 2003). When advertiser information is lacking, trust can reduce consumers' privacy concerns (Bleier and Eisenbeiss 2015) and perceived risk in mobile advertising (Okazaki, Li, and Hirose 2009) but increase participation in online and mobile commercial transactions (Eastin et al. 2016).

Furthermore, research suggests that other factors may act in conjunction with trust in influencing consumer cognition and behavior. For instance, Bleier and Eisenbeiss (2015) found that trust interacts with ad personalization on perceived usefulness of banner ads and privacy concerns. Research also has demonstrated that people who are frequent social media users report higher levels of privacy concerns and are more likely to have private social media profiles. The reason is that those who actively use social media are more familiar with the online marketing environment and are more aware of the online risks associated with disclosure of private information (Lewis, Kaufman, and Christakis 2008). Could the relationship between trust in advertisers and privacy concerns or privacy protection behavior depend on variations in Facebook use?

> **RQ1:** Will trust and Facebook intensity interact and jointly predict consumers' **(a)** privacy concerns and **(b)** privacy protection behavior on Facebook?

Method

Sample

A survey with 526 students in a large Midwestern university in the United States was conducted in fall 2015. An online survey was created on the university server. To ensure the representativeness of the sample, a complete name and e-mail list of all enrolled students was obtained from the university. Using a systematic sampling method, an e-mail invitation with a link to the survey was sent to 6,100 students, which accounted for one-third of the student population of the university. College students were chosen for this survey because statistics show that people between ages 18 and 29 constitute the largest group of social media users (Greenwood, Perrin, and Duggan 2016). Meanwhile, due to the lack of awareness of the business models of social media, many college students disclose private data on Facebook (Chang and Heo 2014).

The average age of the sample was 24.21 (*SD* = 5.92). Females and males comprised 59% and 41% of the sample, respectively. Whites comprised the highest percentage of the sample (68.4%), followed by Asians (12.7%), and Hispanics (7.0%). The average household income was between $40,000 and $49,999.

Measurement

Demographics included gender, age, house income, and education.

Facebook Intensity

Facebook intensity was measured using Ellison, Steinfield, and Lampe's (2007) Facebook intensity scale. The scale includes six closed-ended statements, such as "Facebook is part of my everyday activity" (1 = *Strongly disagree* and 5 = *Strongly agree*). A Facebook intensity score was computed by calculating the mean of the six items, *M* = 2.84, *SD* = 1.04, Cronbach's α = .93.

Mobile Shopping Experience

Mobile shopping experience was measured through two questions adapted from Metzger's (2007) study. The respondents were asked how often they shopped on their mobile phone last year and how often they received coupons and sales information on their mobile phone. The answers ranged from 1 (*Never*) to 5 (*Very frequently*). A new index was created by averaging answers to these two questions (*M* = 2.45, *SD* = 1.25, Cronbach's α = .81).

Previous Online Negative Experiences

Previous online negative experiences were measured using eight questions adapted from Kang's (2015) study. The respondents were asked if they had had important personal information, such as identification card number or bank account, stolen, had an e-mail or social media account taken over/hacked by others, and so on. The answers were based on a five-point Likert scale, from 1 (*Never*) to 5 (*Very frequently*). Answers to these questions were averaged (*M* = 1.35, *SD* = .48, Cronbach's α = .82).

Knowledge about Business Strategies Using Big Data Analytics

This was measured through questions adapted from previous studies (Liu et al. 2017; Youn 2009). The respondents were asked how knowledgeable they were about companies' business strategies, such as data mining, customer profiling, tracking cookies, biometrics, and cloud computing (1 = *Not knowledgeable at all*; 5 = *Very much knowledgeable*). Answers to these questions were averaged (*M* = 2.86, *SD* = .84, Cronbach's α = .88).

Knowledge about Technology Ubiquity

This was measured through questions from Madden's (2014) study. The respondents were asked how much they knew about the ubiquitous technologies that were used for marketing purposes, including (a) social media, (b) mobile technology, (c) the IOT, and (d) GPS on five-point Likert scale ranging from 1 (*Not knowledgeable at all*) to 5 (*Very much knowledgeable*). The answers to these questions were averaged (*M* = 2.26, *SD* = .72, Cronbach's α = .90).

Concern about Technology Ubiquity

Concern about technology ubiquity was measured through questions from Kang's (2015) study. The

Table 1. Factor analysis of consumers' privacy setting on Facebook.

	Factor Loadings[a]		
Variables	Social Identity Information	Contact Information	Daily Life and Entertainment
Photos or videos they upload	.810		
Photos or videos in which they are tagged	.807		
Notes in which they are tagged	.802		
Facebook wall	.790		
Facebook profile page	.772		
Notes they write	.757		
Cell phone number		.847	
Email address		.835	
Birthday			.682
Personal interests such as books, movie, music, etc.			.678
Relationship status			.609
Percent variance explained	49.331	11.508	9.216
Eigenvalue	4.901	1.606	1.199
Cronbach's α	.886	.839	.710

[a] Varimax rotation method was used for the final solution.

respondents were asked how social media, IOT, mobile devices, and GPS increased their concerns about the privacy of personal data being collected by advertisers, ranging from 1 (*Not at all*) to 4 (*Very much*).[1] A new index was created by averaging answers to these questions ($M = 2.58$, $SD = .89$, Cronbach's α = .87).

Concerns about Data Breaches

Concerns about data breaches was measured through questions adapted from Kessinger and Berger's (2014) study, asking how data breaches at retailers (such as supermarkets) and financial institutions (such as banks) increased their privacy concerns, ranging from 1 (*Not at all*) to 4 (*Very much*) ($M = 2.63$, $SD = 1.01$, Cronbach's α = .91).

Trust

Trust was measured through questions adapted from Pavlou's (2003) study. The respondents were asked how much they agreed with the following statements: "Advertisers on Facebook are trustworthy," "Advertisers on Facebook can keep promises and commitments," and "Advertisers on Facebook can keep my best interests in mind," all measured on a four-point Likert scale, ranging from 1 (*Not at all*) to 4 (*Very much*). Answers to these questions were averaged ($M = 2.98$, $SD = .86$, Cronbach's α = .81).

Privacy Concerns about Advertisers' Data Collection

This was measured through questions from previous studies (Bleier and Eisenbeiss 2015). The measurement asked respondents how much they agreed with the statements "It bothers me that advertisers or marketers are able to track information about me on Facebook" and "I am concerned that advertisers or marketers have too much information about me." Items were rated on four-point Likert-type scale, ranging from 1 (*Strongly disagree*) to 4 (*Strongly agree*). Answers to these questions were averaged ($M = 2.92$, $SD = .94$, Cronbach's α = .86).

Privacy Protection Behavior

Privacy protection behavior was measured through questions adapted from previous studies (Kang, Brown, and Kiesler 2013; Zureik and Stalker 2010). The respondents were asked if they did the following things on Facebook for the purpose of protecting their privacy from advertisers or marketers: clearing cookies and browse history; setting their browser to disable or turn off cookies; purposely giving incorrect or misleading information; using services such as VPN, and so on. The answers ranged from 1 (*Never*) to 5 (*Very frequently*). A new index was built by averaging the answers ($M = 2.84$, $SD = .88$, Cronbach's α = .82).

Privacy Settings

Privacy settings were measured through adapting questions from Chang and Heo's (2014) study. The respondents were asked how public or private they set series of personal information on Facebook to prevent advertisers' collection of their personal data. The answer choices included 1 = *Open to the public*, 2 = *Open to my friends and friends' friends on Facebook*, and 3 = *Only open to myself*, with larger value meaning higher levels of privacy. A principal component analysis was conducted with varimax rotation method,[2] and three factors were extracted (Table 1). Following Jin (2013), the first factor was named privacy setting of social identity information, including profile page, photos, videos, wall, and notes. It accounted for 44.56% of the variances (eigenvalue = 5.43; $M = 2.00$, $SD = .36$). The second factor, privacy setting of contact information,

Table 2. Hierarchical regression models predicting privacy concern with advertisers and marketers and privacy protection behavior on Facebook.

	Privacy Concern		Privacy Protection Behavior[b]	
Predictors	β	*t*	β	*t*
Step 1: Demographics				
Male	−.095	−1.781	−.007	−.138
Age	.060	.984	.146	2.353*
Education	.112	1.819	−.039	−.616
Household income	−.088	−1.649	−.014	−.250
ΔR^2	.047**		.018	
Step 2: Experiences				
Mobile shopping experience	−.031	−.278	.020	.374
Negative personal experience	.045	.385	.118	1.907*
ΔR^2	.002		.015	
Step 3: Knowledge				
Knowledge of business strategies	−.035	−.556	.193	3.206***
Knowledge of technologies	.128	1.969*	.293	4.871***
ΔR^2	.012		.157***	
Step 4: Sources of concern				
Concern of data breaches	.098	1.559	.135	2.229*
Concern of technology ubiquity	.249	3.875***	.095	1.578*
ΔR^2	.099***		.038***	
Step 5				
Facebook intensity	−.108	−1.987*	−.120	−1.913*
Trust	−.129	−2.496**	−.111	−2.286**
ΔR^2	.029**		.030**	
Step 6				
Trust × Facebook intensity[a]	.128	2.579*	—	
ΔR^2	.016*			
Total R^2	.205		.258	

[a]The interaction term is based on the centered values of trust and Facebook intensity to avoid the problem of multicollinearity.
[b]Neither privacy concern nor the interaction term between trust and Facebook intensity was significant in predicting privacy protection behavior. Thus, they were removed from the final model.
*$p < .05$; **$p < .01$; ***$p < .001$.

including cell phone number and e-mail address, accounted for 14.60% of the variances (eigenvalue = 1.61; *M* = 2.49, *SD* = .56). The third factor was privacy setting for daily life and entertainment information, including birthday, relationship status, and personal interest, and accounted for 10.9% of the variances (eigenvalue = 1.61; *M* = 2.02, *SD* = .49). Three new factors were formed by multiplying the item scores and their factor loadings.

Results

Setting Different Privacy "Boundaries"

To test hypothesis 1, paired-samples *t* tests were run to compare respondents' privacy settings for different types of information.[3] The results showed that respondents set personal contact information (*M* = 2.49, *SD* = .56) to private, while leaving social identity information (*M* = 2.00, *SD* = .36) (*t* (426) = 18.99, *p* < .001) and daily life and entertainment information (*M* = 2.02, *SD* = .49) (*t* (464) = 17.93, *p* < .001) more accessible. Hypothesis 1 was supported.

Predicting Privacy Concern

To test hypotheses 2 through 7 and answer research question 1, a series of hierarchical regression analyses were run. For privacy concerns, Table 2 showed that respondents who were more concerned (β = .249, *p* < .001) or knowledgeable about technology ubiquity (β = .128, *p* < .05) were more concerned with their private information being collected by the advertisers on Facebook, supporting hypotheses 6a and 7a. Both Facebook intensity (β = −.108, *p* < .05) and online trust (β = −.129, *p* < .01) negatively predicted privacy concerns. The interaction between Facebook intensity and online trust was also significant, β = .128, *p* < .05 (research question 1). Figure 1 showed that for people who used Facebook less intensively, those with high levels of trust were less concerned about their information being collected by advertisers on Facebook (*M* = 2.467, *SD* = .169) than those with low levels of trust (*M* = 3.275, *SD* = .097), *t* (150) = 1.782, *p* < .05. A relationship between trust and privacy concerns did not exist for people who used Facebook more intensively.

Predicting Adoption of Privacy Protection Behavior and Privacy Setting

For privacy protection behavior, older adults (β = .146, *p* < .05) and people with more negative online experiences (β = .118, *p* < .05) took more privacy protection measures on Facebook, supporting hypothesis 2b. Knowledge about technology ubiquity ($\beta = .293$, $p < .001$) and companies' business strategies ($\beta = .193$, $p < .001$) was positively related to privacy protection behavior, supporting hypotheses 3b and 6b. Concerns about technology ubiquity ($\beta = .095$, $p < .05$) and data breaches in the era of big data ($\beta = .135$, $p < .05$) compelled people to protect their privacy on Facebook, supporting hypotheses 4b and 7b. People who used Facebook more intensively ($\beta = -.120$, $p < .05$) and had higher levels of trust ($\beta = -.111$, $p < .01$) adopted fewer privacy protection measures. Privacy concerns had no relationship to privacy protection behavior, rejecting hypothesis 5a.

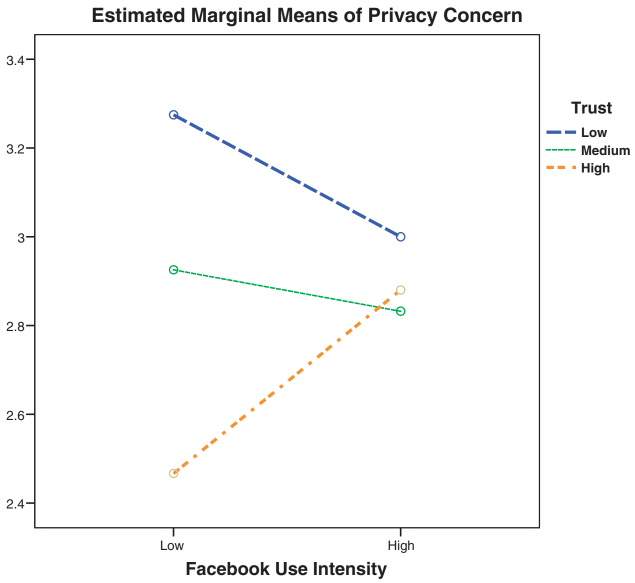


Figure 1. Interaction between trust and Facebook use intensity in predicting consumer privacy concern.

Table 3 showed that, for privacy settings for different types of personal information, males tended to share social identity information ($\beta = -.239$, $p < .001$), contact information ($\beta = -.193$, $p < .01$), and daily life and entertainment information ($\beta = -.151$, $p < .01$) more publicly on Facebook. Frequent mobile shoppers also set all three types of personal information ($\beta_{\text{social identity information}} = -.164$, $p < .05$; $\beta_{\text{contact information}} = -.188$, $p < .01$; $\beta_{\text{daily life information}} = -.213$, $p < .001$) as more open on Facebook, supporting hypothesis 2a. However, people with more negative online experiences were more likely to protect their social identity information ($\beta = .116$, $p < .05$) and daily life and entertainment information ($\beta = .130$, $p < .01$), supporting hypothesis 2b. Those who were more concerned about personal data breaches set all three types of personal information ($\beta_{\text{social identity information}} = .128$, $p < .05$; $\beta_{\text{contact information}} = .181$, $p < .01$; $\beta_{\text{daily life information}} = .143$, $p < .05$) to private, providing support for hypothesis 4b. Concerns about technology ubiquity increased the possibility of setting contact information to private ($\beta = .162$, $p < .01$), supporting hypothesis 7b. Intensive Facebook users shared their social identity information ($\beta = -.280$, $p < .001$) and daily life and entertainment information ($\beta = -.256$, $p < .001$) more openly on Facebook. Privacy concerns had no correlation with privacy settings of the three types of personal information, rejecting hypothesis 5b.

Table 3. Hierarchical regression models predicting consumers' privacy settings on Facebook.

	Social Identity Information		Contact Information		Daily Life and Entertainment Information	
Predictors[a]	β	*t*	β	*t*	β	*t*
Step 1: Demographics						
Male	−.239	−4.257***	−.193	−3.856**	−.151	−2.788**
Age	.083	1.290	.132	2.114*	.204	3.276***
Education	−.003	−.039	−.089	−1.119	.019	.306
Household income	.068	1.201	.116	2.132	−.035	−.635
ΔR^2	.074***		.091***		.066***	
Step 2: Experiences						
Mobile shopping experience	−.164	−2.368*	−.188	−3.125**	−.213	−3.395***
Negative personal experience	.116	2.012*	−.038	−.682	.130	1.975**
ΔR^2	.026*		.043***		.053***	
Step 3: Knowledge						
Knowledge of business strategies	.063	.962	.193	3.064***	.064	.999
ΔR^2	.004		.037***		.004	
Step 4; Sources of concern						
Concern of data breaches	.128	1.919*	.181	3.108**	.143	2.058*
Concern of technology ubiquity	.052	.793	.162	1.975**	−.019	−.291
ΔR^2	.019		.030**		.015	
Step 5						
Facebook intensity	−.280	−5.028***	−.077	−1.423	−.256	−4.770***
ΔR^2	.078***		.006		.066***	
Total R^2	.197		.215		.199	

[a] Trust, knowledge of technology ubiquity, privacy concern, and the interaction term between trust and Facebook intensity were not significant in predicting consumers' privacy settings on Facebook. Thus, they were removed from the final model.

*$p < .05$; **$p < .01$; ***$p < .001$.

Discussion

This study extended CPM theory, PKM, and TAM to the context of social media advertising and examined how young U.S. consumers managed their privacy on Facebook. It also provided insights into the conditions on which their decision to reveal or retain personal information on Facebook was contingent. Such factors included previous experiences, knowledge, and concerns about technology ubiquity, knowledge and concern of business strategies, trust, and Facebook intensity.

Echoing CPM theory, this study showed that consumers set up different privacy boundaries for different types of personal information on Facebook to avoid advertisers. They used the most secure method to protect their contact information, such as cell phone number and e-mail address, on Facebook. Nonetheless, social identity information and daily life or entertainment information was left more accessible to the public (hypothesis 1). These results suggested that people set up different privacy boundary rules and regulate access to personal information by allowing different levels of permeability of information through the boundaries (Jin 2013; Metzger 2007). Such boundaries set them up as potential targets for commercial information, which ranges from general to specific. They establish a more private or a "thicker" boundary and allow less boundary permeability for sensitive information. On the other hand, they establish a more collective or a "thinner" boundary for daily life and entertainment information, such as birthday, relationship status, favorite music, books, or movies—which is exactly the data that marketers need for relationship management and building brand loyalty. This study was in line with past studies on the dynamics between privacy protection and self-disclosure in e-commerce situations and extended CPM theory into the domain of social media advertising.

This study also found that frequent mobile shoppers were more likely to set their contact information and daily life and entertainment information to public on Facebook. The reason may be that they wish to be contacted for more benefits and the perceived benefits outweighed the potential risks. This result was consistent with previous findings that online shoppers would trade sensitive information for ease of purchase or immediate gratifications (Youn 2009). Now with advancements in big data analytics, it is even easier for advertisers to target specific groups of consumers and deliver customized ads. Big data are increasingly available due to customers' mobile purchasing activities on mobile apps, scanners at checkouts, and interactions on mobile devices, where all actions can be easily recorded (Martin and Murphy 2017). In the interest of both consumers and advertisers, it is critical for young mobile shoppers to understand the mobile marketing and social media marketing environments and the potential risks of publicizing sensitive information such as cell phone numbers and e-mail addresses on Facebook.

Previous negative online experiences increased consumers' adoption of privacy protection strategies and private settings on Facebook. Metzger (2007) suggested that future research should examine the impacts of privacy boundary turbulence on information disclosure in the e-commerce context. This study extended Metzger's (2007) work to the Facebook advertising domain and found that when consumers experienced boundary turbulence, such as online spam, they would readjust privacy boundary permeability and take more privacy protection measures. Such results were consistent with reactance theory, which reveals consumers' propensity to protect privacy or engage in negative consumer response behavior when encountering marketing messages that violate privacy (Tucker 2014). They are more likely to react negatively to privacy intrusion to restore freedom and autonomy (Martin and Murphy 2017).

Another significant finding of the study was that people who were more knowledgeable about technology ubiquity and companies' business strategies involving big data had higher privacy concerns and were more likely to take privacy protection strategies on Facebook. Knowledge about business strategies involving big data analytics has not received much attention in previous research on Facebook privacy. Nevertheless, the respondents' knowledge about technology ubiquity ($M = 2.26$ out of 5) and companies' business strategies ($M = 2.86$ out of 5) was only around or a little above the average level in this study. Considering that our sample was composed of college students, it is possible that the general public may be less knowledgeable about these technologies or strategies. Previous scholars have warned that consumers are often unaware of data collection (Hofacker, Malthouse, and Sultan 2016). In adopting PKM, this study called for researchers' attention and highlighted the need to increase consumers' business and technology literacy in the era of big data. Nowadays, this issue is becoming even more prominent because consumers' privacy is under surveillance by businesses such as the "Gang of Four": Amazon, Apple, Facebook, and Google (Shozi and Mtsweni 2016). Moreover, the low cost of data storage makes companies less compelled to delete consumer data, and so more data are being collected, processed, and stored (Shozi and Mtsweni 2016). One noteworthy finding was that knowledge accounted for more than 15% of the variances in privacy protection behavior. Thus, it is crucial to increase public knowledge and literacy about the new ubiquitous technologies and companies' business strategies, such as data mining and consumer profiling, so that all consumers can better protect their privacy.

The study adopted the concept of perceived ubiquity from TAM and showed that concern for technology ubiquity increased privacy concerns, privacy protection behavior, and the willingness to set contact information to private on Facebook. Concerns for data breaches also made people more likely to adopt privacy protection behavior on Facebook and set social identity, contact information, and entertainment and daily life information to private. Ubiquitous technologies and big data consumer analytics have changed advertising. Given technology ubiquity, data sources for marketers and advertisers may include consumers' social media participation, location data, data from mobile beacons, and data generated by the IOT (Hofacker, Malthouse, and Sultan 2016). The rapid growth of big data is blurring the lines of data ownership and is posing special risks for consumer data on Facebook (Shozi and Mtsweni 2016).

Privacy concerns were not related to privacy protection behavior, which reflects the online privacy paradox (Barnes 2006; Feng and Xie 2014; Xie, Fowler-Dawson and Tvauri 2019): Although people express concerns about their online privacy, they still do not adopt privacy protection behavior. Further data analysis showed that privacy concerns were positively correlated with privacy protection behavior ($\beta = .165$, $p < .001$) and privacy settings for social identity information ($\beta = .117$, $p < .05$), contact information ($\beta = .108$, $p < .05$), and daily life and entertainment information ($\beta = .160$, $p < .001$) when controlled only for demographics. However, their relationship became insignificant in the final hierarchical regression model after controlling for mobile shopping experience. This result may be explained by privacy calculus theory. Privacy calculus theory has been applied to explain the privacy paradox and argues that people perform a calculus between the potential benefits of disclosure and the expected loss of privacy, and they will give up their privacy if the benefits outweigh the losses (Lee, Park, and Kim 2013). Thus, it may be possible that consumers who frequently shop on mobile phones receive more coupons, discount information, and sales information. Such benefits outweigh their privacy concerns, so they may decide to stop protecting their privacy.

More interestingly, Facebook intensity moderated the relationship between trust and privacy concerns. Specifically, for less intensive Facebook users, their privacy concerns were negatively related to trust. However, the relationship between trust and privacy concerns did not hold true for more intensive Facebook users. It is possible that intensive Facebook users develop an emotional or psychological connection with Facebook; thus, Facebook has been incorporated into their everyday lives so much so that they tend to disclose private information on Facebook regardless of whether they are aware of the information's recipient, thereby allowing marketers to collect and categorize them into the big data that are then formulated to target them.

Theoretical Implications

By incorporating CPM theory, PKM, and TAM, this study contributes to the body of social media advertising research by providing insights into consumers' privacy concerns and privacy protection behavior on Facebook in the era of big data. Unlike social norm theory (Mesch and Beker 2010), which emphasizes the norms governing people's disclosure behavior, or reactance theory (Tucker 2014), which focuses only on consumers' reaction to privacy violation, this study explores consumers' privacy management from three theoretical perspectives to examine the factors of previous experiences, knowledge of business strategies, technology ubiquity, trust, and Facebook use.

First, it extended CPM theory to the realm of social media advertising. To our knowledge, few studies on social media advertising have applied CPM theory as the main theoretical framework. Though some studies on online advertising have adopted CPM theory, as discussed earlier, social media advertising poses special privacy risks to consumers compared with online advertising. The findings in this study supported CPM theory, suggesting that consumers set up different boundaries for different types of private information on Facebook. When they experience privacy turbulence, they recalibrate privacy boundaries and adopt stricter protection behaviors to prevent advertisers' intrusion. This study contributed to the existing knowledge about consumers' privacy concerns and privacy protection as a response to personalized advertising and data breach. Though earlier research also applied CPM theory to study consumers' response to personalized advertising, such studies focused on either mobile commerce activities (Eastin et al. 2016) or personal data management in health-related activities (Brinson, Eastin, and Bright 2019) instead of the actual privacy protection behavior consumers adopt on Facebook.

Second, this study incorporated new variables, knowledge of business strategies from PKM and technology ubiquity from TAM, into social media advertising privacy research. CPM theory predicts that people decide privacy rules and manage privacy settings based on contextual and individual factors (Petronio 2002). Despite references to the concepts of privacy knowledge and technology ubiquity (Debatin et al. 2009; Liu et al. 2017), to our knowledge CPM is rarely used in conjunction with PKM and TAM in studying privacy management process. Yao and Linz (2008) suggested that future research should apply multiple theories in online privacy research. This study contributed to interactive advertising research through adopting multiple theoretical perspectives and suggesting the possibility of connecting consumers' knowledge about big data and technology ubiquity with CPM theory. The results showed that consumers' knowledge of business strategies using big data analytics increased privacy concerns and translated into privacy protection actions on Facebook. Previous research about PKM mainly focused on traditional advertising or online advertising. To our knowledge, this study is among the pioneering studies to adopt PKM for social media advertising research. Perceived technology ubiquity, a factor in TAM, was used mainly to predict technology adoption behavior. However, this study applied it in privacy research and revealed its positive correlation with privacy concern and adoption of privacy protection measures on Facebook.

Managerial Implications

The findings in this study can help marketers and advertisers better understand consumer needs and improve their campaign outcomes. In a highly competitive environment, the big data collected for profiling consumers is used for greater target reach and predictive behavior analysis. Understanding consumers' privacy concerns and what types of personal data are disclosed on Facebook can help marketers carefully collect information and apply algorithms for strategic decisions. The results reflected that trust reduced consumers' privacy concerns, suggesting that informing consumers of the extent to which their data would be used may heighten trust without sacrificing big data business opportunities.

The results also showed that mobile shopping experiences and coupons and incentives could reduce consumers' privacy concerns and encourage them to share more personal information with advertisers on Facebook. These results suggest that the success of companies is based on how they use big data metrics in their businesses to provide consumers with targeted incentives, mobile alerts, new tactics, coupons, and customer interactions. Markets can redefine their business models to alert and update consumers instantly with new products, incentives, and reviews for quick purchases.

Limitations

The study has several shortcomings. First, the sample in this study was college students between ages 18 and 25. Compared to the general public, college students may use Facebook more intensively and have better knowledge of technologies and business strategies involving big data. Therefore, scholars need to be cautious when generalizing the findings of this study.

Moreover, recent market reports from eMarketer and the Pew Research Center show that the number of Facebook users between ages 18 and 24 has been dropping and older people over age 55 will become the second-biggest demographic of Facebook users (Williamson 2019; Sweney 2018). Previous research has shown that younger and older generations differed in their online privacy concerns and privacy protection (Walrave, Vanwesenbeeck, and Heirman 2012). Thus, a broader mix of ages in a study sample would be more representative and reveal key differences between younger and older generations.

Second, the study has limitations in measurement. When the research was conducted, Facebook privacy settings had only three options: *Open to public*, *Open to friends and friends' friends*, and *Private*. Thus, respondents' privacy settings on Facebook could only be measured on these three levels in this study, which may influence the validity of the measurement. Future research could break down the option of *Open to friends and friends' friends* into *Open to friends* and *Open to friends' friends* to increase the validity of the data. Knowledge of business strategies and ubiquity of technologies were measured through self-report, which may influence the validity and the reliability of measurements, as people may exaggerate their answers due to social desirability bias, may forget details, or may fail to make correct estimates (Rosenman, Tennekoon, and Hill 2011).

Third, this study focused only on Facebook use. However, statistics showed that 18- to 24-year-olds are embracing a variety of social media platforms such as Instagram, Snapchat, and YouTube (Smith and Anderson 2018). Future research can consider how other types of social media use are related to consumers' privacy concerns and privacy protection.

Fourth, the regression analyses in this study could provide only correlations among the variables. To test the causal relationships of the model, future research should use longitudinal or experimental design.

Conclusions

In conclusion, this study applied the communication privacy management theory, persuasion knowledge model, and technology acceptance model to provide an understanding of consumers' perceptions of security and privacy on Facebook. The results suggested that consumers used different strategies to protect different types of personal data on Facebook to avoid advertisers' intrusion. Increasing consumers' knowledge of companies' big data marketing strategies and technology ubiquity could increase their privacy concerns and help them protect privacy. Marketers should act responsibly while mining and using consumer data and avoid data breaches to build consumer trust and long-term relationships.

Notes

1. A four-point Likert scale was adopted (instead of a five- or seven-point Likert scale) because previous marketing research has shown that, when measuring respondents' attitudes, eliminating the midpoint may minimize social desirability bias, which arises from respondents' desire to please researchers or to avoid giving what they perceive to be a socially unacceptable answer (Garland 1991). Nunnally, Bernstein, and Berge (1967) favor eliminating the neutral category in psychometric questions because more answering options may confuse or irritate respondents. Researchers have also observed that when large numbers of respondents choose the midpoint, the results are less likely to reach statistical significance (Clason and Dormody 1994). Therefore, some researchers use four-point Likert scales, deleting the midpoint (Clason and Dormody 1994; Linacre 2002).

2. Varimax rotation method was chosen because it is the most common rotation method of principal component analysis. Varimax rotation maximizes the sum of the variances of the squared loadings of a factor on all variables and keeps the factor loading matrix a simple structure (Dunteman 1989).

3. The Bonferroni correction method was adopted to control Type I error due to multiple comparisons. The acceptance familywise error (.05) was divided by the number of tests ($n = 3$) for each test ($p = .017$).

ORCID

Wenjing Xie http://orcid.org/0000-0003-0575-7072

References

Ardiansyah, Yusfi, Paul Harrigan, Geoffrey Soutar, and Timothy Daly (2018), "Antecedents to Consumer Peer Communication through Social Advertising: A Self-Disclosure Theory Perspective," *Journal of Interactive Advertising*, 18 (1), 55–71.

Attaran, Sharmin, Elaine M. Notarantonio, and Charles J. Quigley, Jr. (2015), "Consumer Perceptions of Credibility and Selling Intent among Advertisements, Advertorials, and Editorials: A Persuasion Knowledge Model Approach," *Journal of Promotion Management*, 21 (6), 703–20.

Barnes, Susan B. (2006), "A Privacy Paradox: Social Networking in the United States," *First Monday*, 11 (9), https://firstmonday.org/ojs/index.php/fm/article/view/1394/1312%2523.

Beam, Michael, Jeffrey Child, Myiah Hutchens, and Jay Hmielowski (2018), "Context Collapse and Privacy Management: Diversity in Facebook Friends Increases Online News Reading and Sharing," *New Media and Society*, 20 (7), 2296–2314.

Bleier, Alexander, and Maik Eisenbeiss (2015), "The Importance of Trust for Personalized Online Advertising," *Journal of Retailing*, 91 (3), 390–409.

Brinson, Nancy H., and Matthew S. Eastin (2016), "Juxtaposing the Persuasion Knowledge Model and Privacy Paradox: An Experimental Look at Advertising Personalization, Public Policy, and Public Understanding," *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 10 (1), article 7.

———, ———, and Laura F. Bright (2019), "Advertising in a Quantified World: A Proposed Model of Consumer Trust, Attitude toward Personalized Advertising, and Outcome Expectancies," *Journal of Current Issues and Research in Advertising*, 40 (1), 54–72.

Chang, Chen-Wei, and Jun Heo (2014), "Visiting Theories that Predict College Students' Self-Disclosure on Facebook," *Computers in Human Behavior*, 30 (January), 79–86.

Child, Jeffrey, Paul Haridakis, and Sandra Petronio (2012), "Blogging Privacy Rule Orientations, Privacy Management, and Content Deletion Practices: The Variability of Online Privacy Management Activity at Different Stages of Social Media Use," *Computers in Human Behavior*, 28 (5), 1859–72.

Choi, Sujeong (2018), "What Promotes Smartphone-Based Mobile Commerce? Mobile-Specific and Self-Service Characteristics," *Internet Research*, 28 (1), 105–22.

Clason, Dennis, and Thomas Dormody (1994), "Analyzing Data Measured by Individual Likert-Type Items," *Journal of Agricultural Education*, 35 (4), 31–35.

Davis, Fred D., Richard Bagozzi, and Paul Warshaw (1989), "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models," *Management Science*, 35 (8), 982–1003.

Debatin, Bernhard, Jennette P. Lovejoy, Ann-Kathrin Horn, and Brittany N. Hughes (2009), "Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences," *Journal of Computer-Mediated Communication*, 15 (1), 83–108.

Dunteman, George (1989), *Principal Components Analysis*, London: Sage.

Eastin, Matthew S., Nancy H. Brinson, Alexandra Doorey, and Gary Wilcox (2016), "Living in a Big Data World: Predicting Mobile Commerce Activity through Privacy Concerns," *Computers in Human Behavior*, 58 (May), 214–20.

Ellison, Nicole B., Charles Steinfield, and Cliff Lampe (2007), "The Benefits of Facebook 'Friends:' Social Capital and College Students' Use of Online Social Network Sites," *Journal of Computer-Mediated Communication*, 12 (4), 1143–68.

Feng, Yang, and Wenjing Xie (2014), "Teens' Concern for Privacy when Using Social Networking Sites: An Analysis of Socialization Agents and Relationships with Privacy-Protecting Behaviors," *Computers in Human Behavior*, 33 (April), 153–62.

Friestad, Marian, and Peter Wright (1994), "The Persuasion Knowledge Model: How People Cope with Persuasion Attempts," *Journal of Consumer Research*, 21 (1), 1–31.

Garland, Ron (1991), "The Mid-Point on a Rating Scale: Is It Desirable?," *Marketing Bulletin*, 2 (1), 66–70.

Greenwood, Shannon, Andrew Perrin, and Maeve Duggan (2016), "Social Media Update 2016," *Pew Research Center*, November 11, http://www.pewinternet.org/2016/11/11/social-media-update-2016/.

Gupta, Babita, and Anitha Chennamaneni (2018), "Understanding Online Privacy Protection Behavior of the Older Adults: An Empirical Investigation," *Journal of Information Technology Management*, 29 (3), 1–13.

Hallnäs, Lars, and Johan Redström (2002), "From Use to Presence: On the Expressions and Aesthetics of Everyday Computational Things," *ACM Transactions on Computer-Human Interaction (TOCHI)*, 9 (2), 106–24.

Heyman, Rob, Ralf De Wolf, and Jo Pierson (2014), "Evaluating Social Media Privacy Settings for Personal and Advertising Purposes," *Info*, 16 (4), 18–32.

Hofacker, Charles, Edward Malthouse, and Fareena Sultan (2016), "Big Data and Consumer Behavior: Imminent Opportunities," *Journal of Consumer Marketing*, 33 (2), 89–97.

Jagerson, John (2019), "Wall Street Likes Facebook's Earnings," *Investopedia*, February 1, https://www.investopedia.com/wall-street-likes-facebook-s-earnings-4586348.

Jin, Seung-A. Annie (2013), "Peeling Back the Multiple Layers of Twitter's Private Disclosure Onion: The Roles of Virtual Identity Discrepancy and Personality Traits in Communication Privacy Management on Twitter," *New Media and Society*, 15 (6), 813–33.

Jung, A-Reum, and Jun Heo (2019), "Ad Disclosure vs. Ad Recognition: How Persuasion Knowledge Influences Native Advertising Evaluation," *Journal of Interactive Advertising*, 19 (1), 1–14.

Kang, Ruogu (2015), "Incognito Online: Why and How People Hide Their Information," unpublished doctoral dissertation, Carnegie Mellon University.

———, Stephanie Brown, and Sara Kiesler (2013), "Why Do People Seek Anonymity on the Internet? Informing Policy and Design," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, New York: ACM, 2657–66.

Karanja, Alice W., Daniel W. Engels, Ghizlane Zerouali, and Ariel Francisco (2018), "Unintended Consequences of Location Information: Privacy Implications of Location Information Used in Advertising and Social Media," *SMU Data Science* Review, 1 (3), article 13.

Kessinger, Kristen, and Aaron Berger (2014), "2014 ISACA IT Risk/Reward Barometer—US Consumer Results," *ISACA*, October, http://www.isaca.org/SiteCollectionDocuments/2014-Risk-Reward-Survey/2014-US-Consumer-Data-Summary_res_Eng_1114.pdf.

Khang, Hyoungkoo, Eyun-Jung Ki, and Lan Ye (2012), "Social Media Research in Advertising, Communication, Marketing, and Public Relations, 1997–2010," *Journalism & Mass Communication Quarterly*, 89 (2), 279–98.

Kumar, Senthil, Saravanakumar Kandasamy, and K. Deepa (2016), "On Privacy and Security in Social Media: A Comprehensive Study," *Procedia Computer Science*, 78 (December), 114–19.

Lee, Haein, Hyejin Park, and Jinwoo Kim (2013), "Why Do People Share Their Context Information on Social Network Services? A Qualitative Study and an Experimental Study on Users' Behavior of Balancing Perceived Benefit and Risk," *International Journal of Human-Computer Studies*, 71 (9), 862–77.

Lewis, Kevin, Jason Kaufman, and Nicholas Christakis (2008), "The Taste for Privacy: An Analysis of College Student Privacy Settings in An Online Social Network," *Journal of Computer-Mediated Communication*, 14 (1), 79–100.

Limpf, Nina, and Hilde Voorveld (2015), "Mobile Location-Based Advertising: How Information Privacy Concerns Influence Consumers' Attitude and Acceptance," *Journal of Interactive Advertising*, 15 (2), 111–23.

Linacre, John (2002), "Optimizing Rating Scale Category Effectiveness," *Journal of Applied Measurement*, 3 (1), 85–106.

Liu, Qian, Mike Yao, Ming Yang, and Caixie Tu (2017), "Predicting Users' Privacy Boundary Management Strategies on Facebook," *Chinese Journal of Communication*, 10 (3), 295–311.

Madden, Mary (2014), "Public Perceptions of Privacy and Security in the Post-Snowden Era," *Pew Research Center*, November 12, http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/.

Martin, Kelly, and Patrick Murphy (2017), "The Role of Data Privacy in Marketing," *Journal of the Academy of Marketing Science*, 45 (2), 135–55.

Mesch, Gustavo, and Guy Beker (2010), "Are Norms of Disclosure of Online and Offline Personal Information Associated with the Disclosure of Personal Information Online?," *Human Communication Research*, 36 (4), 570–92.

Metzger, Miriam (2007), "Communication Privacy Management in Electronic Commerce," *Journal of Computer-Mediated Communication*, 12 (2), 335–61.

Nelson, Michelle, Heejo Keum, and Ronald Yaros (2004), "Advertainment or Adcreep: Game Players' Attitudes toward Advertising and Product Placements in Computer Games," *Journal of Interactive Advertising*, 5 (1), 3–21.

Nisbett, Richard, and Lee Ross (1980), *Human Inference: Strategies and Shortcomings of Social Judgment*, Pearson, NJ: Prentice-Hall.

Nunnally, Jum, Ira Bernstein, and Jos Berge (1967), *Psychometric Theory*, New York: McGraw-Hill.

Okazaki, Shintaro, and Morikazu Hirose (2009), "Effects of Displacement–Reinforcement between Traditional Media, PC Internet, and Mobile Internet: A Quasi-Experiment in Japan," *International Journal of Advertising*, 28 (1), 77–104.

———, Hairong Li, and Morikazu Hirose (2009), "Consumer Privacy Concerns and Preference for Degree of Regulatory Control," *Journal of Advertising*, 38 (4), 63–77.

Pavlou, Paul (2003), "Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model," *International Journal of Electronic Commerce*, 7 (3), 101–34.

Petronio, Sandra (2002), *Boundaries of Privacy: Dialectics of Disclosure*, Albany: State University of New York Press.

———, and Wesley Durham (2015), "Communication Privacy Management Theory: Significance for Interpersonal Communication," in *Engaging Theories in Interpersonal Communication: Multiple Perspectives*, Braithwaite and Paul Schrodt, eds., Thousand Oaks, CA: Sage, 335–348.

Prince, Christine (2018), "Do Consumers Want to Control Their Personal Data? Empirical Evidence," *International Journal of Human–Computer Studies*, 110 (Spring), 21–32.

Ramzan, Zulfikar (2010), "Phishing Attacks and Countermeasures," in *Handbook of Information and Communication Security*, P. Stavroulakis and M. Stamp, eds., Berlin: Springer, 433–448.

Rosenman, Robert, Vidhura Tennekoon, and Laura Hill (2011), "Measuring Bias in Self-Reported Data," *International Journal of Behavioural and Healthcare Research*, 2 (4), 320–32.

Shozi, Nobubele, and Jabu Mtsweni (2016), "Big Data Privacy and Security: A Systematic Analysis of Current and Future Challenges," in *Proceedings of the 11th International Conference on Cyber Warfare and Security*, Sonning Common, United Kingdom: ACPIL, 296–303.

Smith, Aaron, and Monica Anderson (2018), "Social Media Use in 2018," *Pew Research Center*, March 1, http://www.pewinternet.org/2018/03/01/social-media-use-in-2018/.

Smit, Edith G, Guda Van Noort, and Hilde AM Voorveld (2014), "Understanding Online Behavioural Advertising: User Knowledge, Privacy Concerns and Online Coping Behaviour in Europe," *Computers in Human Behavior*, 32 (March), 15–22.

Stelzner, Michael (2018), "2018 Social Media Marketing Industry Report," *Social Media Examiner*, May 7, https://www.socialmediaexaminer.com/social-media-marketing-industry-report-2018/.

Sweney, Mark (2018), "Is Facebook for Old People? Over -5s Flock In as the Young Leave," *The Guardian*, February 12, https://www.theguardian.com/technology/2018/feb/12/is-facebook-for-old-people-over-55s-flock-in-as-the-young-leave.

Thielst, Christina (2011), "Social Media: Ubiquitous Community and Patient Engagement," *Frontiers Health Service Management*, 28 (2), 3–14.

Tucker, Catherine (2014), "Social Networks, Personalized Advertising, and Privacy Control," *Journal of Marketing Research*, 51 (5), 546–62.

Tufekci, Zeynep (2008), "Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites," *Bulletin of Science, Technology, and Society*, 28 (1), 20–36.

Tversky, Amos, and Daniel Kahneman (1974), "Judgement under Uncertainty: Heuristics and Biases," *Science*, 185 (4157), 1124–31.

Uzialko, Adam (2018), "20 Small Business Trends and Predictions for 2019," November 26, https://www.businessnewsdaily.com/7605-business-trend-predictions.html

Venkatesh, Viswanath, and Fred D. Davis (2000), "A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies," *Management Science*, 46 (2), 186–204.

———, and Hillol Bala (2008), "Technology Acceptance Model 3 and a Research Agenda on Interventions," *Decision Sciences*, 39 (2), 273–315.

Vishwanath, Arun, Brynne Harrison, and Yu Jie Ng (2018), "Suspicion, Cognition, and Automaticity Model of Phishing Susceptibility," *Communication Research*, 45 (8), 1146–66.

Walrave, Michel, Ini Vanwesenbeeck, and Wannes Heirman (2012), "Connecting and Protecting? Comparing Predictors of Self-Disclosure and Privacy Settings Use between Adolescents and Adults," *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 6 (1), article 3.

Weiser, Mark (1991), "The Computer for the 21st Century," *Scientific American*, 265 (3), 94–104.

Westin, Alan (2003), "Social and Political Dimensions of Privacy," *Journal of Social Issues*, 59 (2), 431–53.

Williamson, Debra (2019), "US Social Trends in 2019," *eMarketer*, January 10, https://www.emarketer.com/content/us-social-trends-for-2019.

Wisniewski, Pamela J., Bart P. Knijnenburg, and Heather Richter Lipford (2017), "Making Privacy Personal: Profiling Social Network Users to Inform Privacy Education and Nudging," *International Journal of Human-Computer Studies*, 98 (February), 95–108.

Xie, Wenjing, Amy Fowler-Dawson, and Anita Tvauri (2019), "Revealing the Relationship between Rational Fatalism and the Online Privacy Paradox," *Behaviour & Information Technology*, 38 (7), 742–59.

Yang, Hongwei, and Hui Liu (2014), "Prior Negative Experience of Online Disclosure, Privacy Concerns, and Regulatory Support in Chinese Social Media," *Chinese Journal of Communication*, 7 (1), 40–59.

Yao, Mike, and Daniel Linz (2008), "Predicting Self-Protections of Online Privacy," *CyberPsychology and Behavior*, 11 (5), 615–17.

Youn, Seounmi (2009), "Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors among Young Adolescents," *Journal of Consumer Affairs*, 43 (2), 389–418.

Zureik, Elia, and Lynda Stalker (2010), "The Cross-Cultural Study of Privacy: Problems and Prospects," in *Surveillance, Privacy, and the Globalization of Personal Information: International Comparisons*, E. Zureik, L. Stalker, E. Smith, D. Lyon, and Y.E. Chan, eds., Montreal, CA: McGill -Queen's University Press, 8–30.