Journal of the Association for Information Systems

Volume 24 | Issue 1 Article 1

2023

Reconciling the Personalization-Privacy Paradox: Exploring Privacy Boundaries in Online Personalized Advertising

Yu-Qian Zhu
National Taiwan University of Science and Technology, yzhu@mail.ntust.edu.tw

Kritsapas Kanjanamekanant
National Taiwan University of Science and Technology, d10509805@mail.ntust.edu.tw

Yi-Te Chiu
Victoria University of Wellington, yi-te.chiu@vuw.ac.nz

Recommended Citation
Zhu, Yu-Qian; Kanjanamekanant, Kritsapas; and Chiu, Yi-Te (2023) "Reconciling the Personalization-Privacy Paradox: Exploring Privacy Boundaries in Online Personalized Advertising," *Journal of the Association for Information Systems*, 24(1), 294-316.
DOI: 10.17705/1jais.00775
Available at: https://aisel.aisnet.org/jais/vol24/iss1/1

Journal of the Association for Information Systems (2023) **24**(1), 294-316
doi: 10.17705/1jais.00775

RESEARCH ARTICLE

ISSN 1536-9323

Reconciling the Personalization-Privacy Paradox: Exploring Privacy Boundaries in Online Personalized Advertising

Yu-Qian Zhu,[1] Kritsapas Kanjanamekanant,[2] Yi-Te Chiu[3]

[1], National Taiwan University of Science and Technology, Taiwan, yzhu@mail.ntust.edu.tw
[2]National Taiwan University of Science and Technology, Taiwan, d10509805@mail.ntust.edu.tw
[3]Victoria University of Wellington, New Zealand, yi-te.chiu@vuw.ac.nz

Abstract

To reconcile the personalization-privacy paradox, we adopt the *privacy as a state* view and define privacy as a state of information boundary rule-following. We further identify five types of boundaries underlying some of the important implicit rules of maintaining privacy: communication channel, platform, device, temporal, and purpose boundaries. Using an online vignette survey, we investigated how each of these boundary types affected users' privacy perceptions when they were subjected to personalized advertisements. Using fixed- and random-effects models, we investigated how violating different boundary rules leads to changes in perceived privacy. Our results show that all five boundary types are significant predictors of perceived privacy within individuals. The communication channel, device, and business versus private purpose are significant predictors of perceived privacy across the whole sample. Temporal boundaries and platform boundaries failed to achieve statistical significance when evaluated simultaneously with the other factors across the whole sample. This means that for each individual, observing the rules of these five boundary types leads to higher perceived privacy than not observing these conditions. Taken as a whole, observing communication channel, device, and business versus private purpose boundaries also leads to higher averages of perceived privacy across the whole sample. Theoretical and practical implications are discussed based on the results.

Keywords: Information Privacy, Privacy as a State, Privacy Boundary Maintenance, Personalization-Privacy Paradox

Mikko Siponen was the accepting senior editor. This research article was submitted on July 13, 2019 and underwent three revisions. Yu-Qian Zhu is the corresponding author.

1 Introduction

The use of information technologies generates a multitude of digital footprints that can be used to predict people's identities, personalities, and intended behaviors (Hinds & Joinson, 2019). By analyzing customer data, organizations can proactively provide personalized services and push relevant advertising, targeting customers in certain demographic or interest groups and thus enhancing customer stickiness and revenue (Benlian, 2015; Choi et al., 2020). Personalized advertising, in particular, has demonstrated impressive effectiveness and become a sizable industry, attracting increasing attention in academia and industry (Chen & Stallaert, 2014). Nonetheless, challenges can arise when the use of personalization goes against customers' privacy expectations. The improper use of user data may lead to consumer backlash and potential lawsuits (Martin & Murphy, 2017; Shilton & Greene, 2017). This tension between how companies and marketers exploit users' information for personalization and users' growing

concerns over privacy, termed the personalization-privacy paradox (PPP), has become a pertinent and ongoing issue confronting the information technology industry (Awad & Krishnan, 2006; Sutanto et al., 2013).

Various perspectives have been applied to address the personalization-privacy paradox. Studies based on privacy calculus theory view *privacy as a commodity* that can be exchanged for perceived net benefits. If the perceived benefits outweigh the risks, privacy concerns are mitigated (e.g., Hui et al., 2007; Dinev et al., 2013; Li & Ungler, 2012). In contrast to the commodity view of privacy, scholars from the *privacy as control* research stream argue that the more people feel in control of their information and the situation, the less they are concerned with privacy (e.g., Awad & Krishnan, 2006; Sutanto et al., 2013).

While PPP has been mainly explored from the *privacy as a commodity* and *privacy as control* perspectives, a growing body of scholars have been enriching the PPP literature from the *privacy as a state* perspective by investigating how contextual factors impact people's privacy perceptions (e.g., Kobsa et al., 2016; Sheng et al., 2008; Xu et al., 2012; Zhu & Kanjanamekanant, 2021). The privacy as a state view regards privacy as a state of being that is bound up with context. According to this view, privacy expectations vary as a function of contextual factors (Laufer & Wolfe, 1977; Smith et al., 2011). Accordingly, privacy is fluid, flexible, and malleable, and privacy boundaries are drawn with regard to contextual factors such as information, the environment, and the interaction (Smith et al., 2011).

Our research adopts the *privacy as a state* perspective. We define privacy as a state of information boundary rule-following: privacy is achieved when all parties involved abide by the information boundary rules (Petronio, 1991, 2002; Sutanto et al., 2013). Besides rules that are explicitly agreed upon, such as terms and conditions spelled out in the user agreement, individuals also rely on implicit and unstated rules to manage their private information (Petronio, 1991, 2002). Achieving a clear understanding of these implicit rules, however, has been a challenge. In personalized advertising, scholars have acknowledged that our current knowledge of the information boundaries in data usage is still very limited: digital service providers and marketers struggle to understand where to draw the line for how the wealth of personal data that has been collected should be used for personalization, leading to consumers' increasing concerns about privacy (John et al., 2018; Martin & Shilton, 2016; Zhu & Kanjanamekanant, 2021). Facebook, for example, has been under close scrutiny and has been the subject of lawsuits for actions such as collecting users' data from third-party websites and allowing users' private information to be made public.[1]

To address such issues, we propose and confirm a set of privacy boundary rules in personalized advertising with a framework encompassing contextual factors that people can use to regulate personal information. Based on the communication privacy management theory (CPM) (Petronio, 1991, 2002a) and Marx's (2001) conceptualization of personal boundaries, we identify five types of boundaries that underlie some of the important implicit rules of maintaining privacy: communication channel, platform, device, temporal, and purpose boundaries. In the following sections, we first introduce our theoretical foundations and hypotheses, then describe the research methodology, analysis, and results, and conclude by discussing theoretical and managerial implications.

2 Theoretical Foundations and Hypotheses

2.1 Three Perspectives of the Personalization-Privacy Paradox

The personalization-privacy paradox presents a dilemma in which people need to decide whether to trade private information for personalization benefits (Awad & Krishnan, 2006; Karwatzki et al., 2017). A large body of information systems (IS) research has contributed to reconciling the paradox from the *privacy as control* and *privacy as a commodity* views (e.g., Awad & Krishnan, 2006; Koh et al., 2020; Summers et al., 2016). We argue that the *privacy as a state* perspective deserves more attention and can shed light on the sophisticated normative privacy decision process. In the following sections, we elaborate on these three views and how they address the personalization-privacy paradox.

2.1.1 The Privacy as Control View

The control view argues that privacy is "the selective control of access to the self" (Altman, 1975, p. 24) and relates to people's ability to "control the terms under which their personal information is acquired and used" (Culnan, 1999, p. 20). Privacy is preserved when users are given authority and autonomy over decisions concerning their personal information, such as what information is being collected, who can access it, and how it can be used. In the personalization research, the extant literature has identified the essential role of

[1] More details can be found on NBC's website at https://www.nbcnews.com/tech/social-media/timeline-facebook-s-privacy-issues-its-responses-n859651

maintaining and enhancing information transparency for perceived control (Awad & Krishnan, 2006; Dinev et al., 2013). When users learn more about the types and the amount of information collected, stored, and used (Summers et al., 2016) and how information is processed for personalization (Sutanto et al., 2013), they are more willing to use the service. In addition, a sense of control can be achieved by offering users flexibility and choices in interacting with personalized services (Awad & Krishnan, 2006). Proactive self-protection (e.g., the use of privacy-preserving features provided by vendors) and proxy control (e.g., industry self-regulation and government legislation) also contribute to a sense of control (Xu et al., 2012).

2.1.2 The Privacy as a Commodity View

The commodity view suggests that value judgments about privacy are subject to personal evaluation based on cost-benefit calculations (Smith et al., 2011). When the benefits outweigh the costs associated with the loss of privacy, individuals are likely to be more willing to give away private information. Maximizing benefits and minimizing risk are the two main strategies used to address the paradox (Culnan & Armstrong, 1999).

Typically, organizations seek to maximize perceived benefits to encourage the use of personalization products and services. Financial rewards are a common benefit (Hui et al., 2007; Xu, Luo, et al., 2011). Intangible benefits, such as efficiency gains from personalization (Koh et al., 2020), augmented service quality (Yaraghi et al., 2019), and the fulfillment of social needs (Proudfoot et al., 2018), also encourage the disclosure of information. On the other hand, privacy risks involve an uncertain event or condition that has the potential to cause the loss of privacy (Dinev & Hart, 2006). Privacy-enhancing technologies, such as anonymous browsing, privacy preferences and cookies management, can be utilized to reduce the likelihood of privacy risks (Kaaniche et al., 2020).

2.1.3 The Privacy as a State View

The concept of privacy as a state of being is well-established in everyday and academic languages. According to this view, it is necessary to first define what the state of privacy is and what factors lead to the specific state of privacy. Westin (1968) described privacy as states of anonymity, solitude, reserve, and intimacy. Schoeman (1984, p. 3) referred to privacy as "a state of limited access to a person," which reflects the mainstream view of privacy as a state (Smith et al., 2011). McCreary (2008) argued that technological advances have made the idea of privacy as keeping personal information secret obsolete. Instead, privacy today concerns social contracts and boundaries. Just like in a small town, despite knowing everything about each other, people tacitly avoid talking about certain things (McCreary, 2008). In other words, privacy is a state of dignity, civility, and cohesion that results from abiding by social contracts and maintaining boundaries.

Since the state of privacy is associated with individual cognition and the interaction between individuals in a particular context, contextual factors play a key role in predicting privacy as a state (Smith et al., 2011). The extant research has tapped into the privacy as a state perspective by investigating how contextual factors affect privacy perceptions in the personalization-privacy paradox. For example, cloud-based or client-based personalization may affect perceived privacy. People tend to express greater privacy concerns when personalization occurs in the cloud instead of on users' local devices (Kobsa et al., 2016). In location-based advertising, ads that are personalized and disseminated based on covert data collection (push-based) would be expected to lead to greater privacy concerns than ads that are disseminated based on user requests (pull-based) (Xu et al., 2011). The purpose of personalization, e.g., whether it is for the purpose of preparing for an emergency, also matters. Statistically speaking, people are more concerned about privacy with personalized services in nonemergency contexts than in emergency contexts, such as alerts for natural disasters (Sheng et al., 2008). Lastly, the source and nature of the information used for personalization are also linked to perceived privacy. Users tend to have greater privacy concerns when the data used for personalization comes from third parties external to the website they are currently visiting (John et al., 2018; Zhu & Kanjanamekanant, 2021). Additionally, if the nature of the data may cause people to feel embarrassed or uncomfortable—for example, data about health, financial, or sexual orientation—people often perceive less privacy with personalization (Zhu & Kanjanamekanant, 2021). Table 1 summarizes key practices used to influence privacy decision-making from these three perspectives.

2.1.4 Comparisons among the Three Perspectives

The *privacy as a commodity* and *privacy as control* literatures offer valuable insights into how the personalization-privacy paradox can be reconciled. The *privacy as a state* view differs from these two views in two ways. First, in both the privacy as a commodity and privacy as control views, the definition focuses on managing privacy, while privacy as a state describes the state of having privacy (Tavani, 2007). Some researchers argue that privacy as control captures "actual privacy," or privacy practices, and privacy as a state is a reflection of "perceived privacy" (Bhave et al., 2020).

Table 1. Key Practices that Influence Personalization-Privacy Decision-Making

View	Rationale	Practices to address the paradox
Control	Privacy concerns for personalized benefits are reduced when control or perceived ability to control increases. **Question to consider:** How can control (actual and perceived) be enhanced?	1. Increasing information transparency about the types and the amount of information collected, stored, and used (Summers et al., 2016; Tsai et al., 2011) and how information is processed (Sutanto et al., 2013) 2. Increasing flexibility and choices in how users interact with the service (Awad & Krishnan, 2006; Tsai et al., 2011) 3. Increasing proactive self-protection (e.g., use of privacy-preserving features provided by vendors) and proxy control (e.g., industry self-regulation and government legislation) (Xu et al., 2011; Xu et al., 2012)
Commodity	A tradeoff between privacy and personalization is made based on calculations of privacy risk and benefits/rewards. **Question to consider:** How can benefits be maximized while minimizing risks?	1. Increasing tangible benefits: monetary incentives (Hann et al., 2007; Hui et al., 2007), coupons (Koh et al., 2020; Sutanto et al., 2013; Xu, Luo, et al., 2011), personalized prices (Preibusch et al., 2013) 2. Increasing intangible benefits/perceived value: Efficiency gains via personalized search and recommendation (Karwatzki et al., 2017; Koh et al., 2020), perceived personalization quality (Li & Unger, 2012; Xu, Luo, et al., 2011; Yaraghi et al., 2019), fulfillment of social needs (Proudfoot et al., 2018), perceived accuracy and reliability (Balapour et al., 2020; Xu, Dinev, et al., 2011), perceived usefulness (Chang et al., 2018) 3. Risk reduction via data protection technologies: user-side techniques (anti-tracking techniques and privacy preservation techniques), service-side techniques (self-destructing data systems, statistical disclosure control), and channel-side techniques (secure communication and trusted third party) (see a review by Kaaniche et al., 2020)
State	A state of being (from limited access to boundary rule-following). The definition may vary from one context to another. **Question to consider:** How is the state of privacy defined? What are important contextual factors leading to privacy?	1. Local personalization: Localized personalization is perceived as less invasive (Kobsa et al., 2016) 2. Reactive personalization: Covert/proactive personalization leads to higher concerns compared with overt/reactive personalization (Xu et al., 2011) 3. Justify the cause of personalization: A justified purpose for personalization, e.g., emergency preparation lowers privacy concerns (Sheng et al., 2008) 4. Using data from internal sources and avoiding using embarrassing information for personalization (Zhu & Kanjanamekanant, 2021)

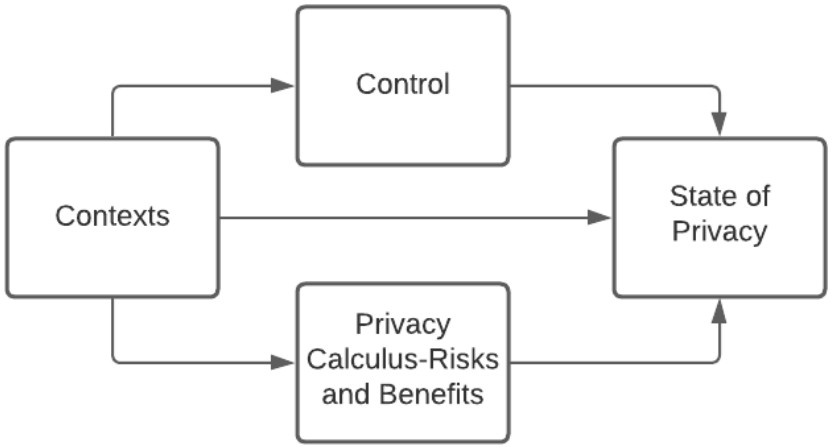

Figure 1. A Unified View of the Three Perspectives on Privacy

Second, for the *privacy as control* and *privacy as a commodity* perspectives, the main actor is the individual actively making decisions about their information disclosure and management. Privacy is preserved through control over these decisions or cost-benefit analysis. When contextual factors are discussed, they are typically mediated through perceived control, benefits, or risks (Xu et al., 2011; Xu et al., 2012). In contrast, for the *privacy as a state* perspective, environmental and interactional factors take a more salient and direct role in privacy (Smith et al., 2011) because the complexity of today's technologies makes it increasingly difficult for users to understand, control, and make decisions about every detail of their privacy (Gerber et al., 2018). Most people find it burdensome to manage privacy by selecting preferences, opting out of behavioral targeting, indicating consent, and turning off geotracking on the many websites, apps, and online platforms they use (Schreiber, 2020). Instead of engaging in rational and deliberate information processing concerning privacy, scholars argue that many people currently engage in privacy-related behavior spontaneously, with little deliberation (Dinev et al., 2015). Contextual factors may exert direct influences on privacy through heuristic thinking or mental shortcuts because human judgment is subject to cognitive limitations (Dinev et al., 2015).

Despite their differences, there is a way to unify these three views on privacy. Dinev et al. (2013) observed that the most common theme that emerges from different privacy definitions is that "privacy is a state in which an individual is found in a given situation at a given moment of time" (Dinev et al., 2013, p. 298). Researchers from the different perspectives, at some point, all use the word "state" to describe privacy—e.g., "state of control" (Altman, 1975) and "state of limited access" (Margulis, 2003a, 2003b). Privacy as a state is tied to concrete situations and is shaped by multiple factors (Smith et al., 2011). Contextual factors (and norms underlying them) can influence the state of privacy either directly or indirectly—through the mediation of perceived control, risks, or benefits (See Figure 1 below).

This research takes the view of privacy as a state of boundary rule-following. We seek to explore different contextual factors that help form boundary rules in maintaining privacy. We build our theoretical framework on communication privacy management theory, which we discuss in the next section.

2.2 CPM and Privacy Boundaries

The view of *privacy as a state* is highlighted with the theoretical framework of communication privacy management theory (CPM) (Petronio, 1991, 2002b). CPM uses the boundary metaphor to illustrate the regulatory process of exchanging private information between co-owners of information. It contends that individuals maintain and coordinate privacy boundary rules depending on contextual factors (Petronio, 1991, 2002b). Once information is shared, a collective information boundary is formed and owned by the original information owner and the confidant.

CPM is centered around a rule-based privacy management system for managing privacy boundaries. The rules can be either explicit, via negotiations with involved parties, or implicit, as unstated assumptions (Petronio, 1991, 2002). Implicit rules are used more often than explicit rules (Smith & Brunner, 2017). What constitutes implicit rules becomes an important question to address because these unstated rules can determine whether personalization will raise privacy concerns beyond what has been explicitly expressed and agreed upon. Prior research has suggested that these rules may be based on norms; general ethical, legal, and political principles; and context-specific purposes and values (Nissenbaum, 2004; Smith & Brunner, 2017). Several studies have endeavored to explore these implicit boundary rules (for a summary, see Table 2). Following Smith et al., (2011), we categorize these studies into three dimensions: information, environment, and interaction. The table below shows that information features (e.g., sensitivity, volume, purpose), environmental features (e.g., privacy policy, co-ownership, security), and interaction features (e.g., frequency of interaction) are all possible determinants of boundary rules.

2.3 Theorizing Privacy Boundaries and Hypothesis Development

To further understand boundary rules in personalized advertising and to theorize privacy boundaries, we draw on Marx's (2001) conceptual framework, which consists of four personal boundaries in real-world contexts. Before delving into the development of the hypotheses, we briefly introduce these privacy boundaries in offline and online settings.

First, natural boundaries shield personal information from unintended audiences. These boundaries can be physical objects such as doors, walls, or screens; they can also be virtual, based on the directed nature of the communication. Marx (2001) views phone calls, letters, and other forms of directed communication as having a natural boundary by explicitly specifying who the intended audience is, thereby excluding those not on the receiving list. We propose that online communication channels (public channels that broadcast vs. private channels that are directed toward a limited audience) can serve as a natural boundary.

Table 2. Summary of Literature on Privacy Boundary Rule Determinants Based on CPM

Author	Method and context	Potential boundary rule determinants	Boundary rule dimensions		
			Information	Environment	Interaction
Anderson & Agarwal (2011)	Survey: 1,089 adults	1.Information sensitivity 2. Purpose of information (health-related or marketing) 3.Trustworthiness of others	1,2		3
Balapour et al. (2020)	Survey: 1,046 mobile app users	1. Information sensitivity 2. Privacy policy of the platform	1	2	
Eastin et al. (2016)	Survey: 416 smartphone users	1. Attitude towards the platform		1	
Li et al. (2015)	Dataset analysis: 1,216 social media accounts	1. Number of total interactions with the platform 2. Type of information	2	1	
Lin & Armstrong (2019)	Survey: 168 undergraduate students	1. Information sensitivity 2. Security of information cyberspace	1	2	
Liu & Wang (2018)	Survey: 831 respondents (US and China)	1. Group norm			1
McNealy & Mullis (2019)	Qualitative: around 10,000 gossip forum threads analysis	1. Collective information ownership of users 2. Presence of collective information protection strategies		2	1
Metzger (2007)	Survey: 213 university students	1. Information sensitivity 2. Stringency of platform privacy policies	1	2	
Xu et al. (2011)	Survey: 823 university students	1. Whether or not private information in cyberspace has been violated		1	
Yaraghi et al. (2019)	HIE dataset analysis: 12,444 patient records	1. Number of confidants 2. Volume of information shared to the platform	2		1
Yu et al. (2019)	Meta-analysis of 101 articles	1. emotional platforms (related to affectionate relationships between users) have more privacy disclosure than instrumental platforms (related to disclosure based on specific purposes)		1	
Zhu & Kanjanamekanant (2021)	Survey-349 social media users	1. Source of data (internal or external) 2. Perceived co-ownership with platform 3. Personification of the platform	1	2,3	

Second, social boundaries, or the expectation of confidentiality based on social norms, prescribe the code of conduct accepted by group members. We expect people with certain social roles, such as lawyers, doctors, and secretaries, to protect confidentiality and secrets. Similarly, we contend that people hold normative expectations toward platforms. Different platforms comprise different social group members whose information behaviors should conform to the norm.

Third, spatial boundaries assume that people are entitled to the separation of information based on the locations of their lives. We argue that the different devices on which information is shared (e.g., work laptop vs. personal mobile phone) demarcate spatial boundaries. What is shared on one device should not be used for personalization on another device.

Fourth, temporal boundaries describe the time at which content is shared and focus on the recency of the

information. Marx (2001) explains that interactions, communication, and their remnants, such as discarded letters or notes, are ephemeral and transitory and should not be captured and retained forever. We conceptualize this feature with temporal boundaries relating to the transient nature of information. We maintain that individuals should have a "right to be forgotten" (cf. Article 17 of the EU's GDPR) and that outdated information should not be used by digital service providers.

Inspired by prior literature that stresses the role of the purpose (Sheng et al., 2008), we further propose privacy boundaries based on the purpose of the information behind the shared content. Privacy boundaries should be clearly drawn when the purpose of the information is recognized as personal instead of business. Table 3 summarizes the relationships between our framework and the prior literature below. We detail our rationale for these boundaries in different contexts and according to their impact on privacy in the following hypotheses.

2.3.1 Communication Channel Boundaries

We define a communication channel as the digital channel through which information is sent to the intended receivers on a particular online platform. There are various forms of communication channels online with differing degrees of exclusiveness, ranging from directed communication such as private messages, private chat, and emails to more public messages on public Facebook venues, bulletin boards, and discussion forums. The online environment allows people to maintain different personas, which contributes to our willingness to share certain information (Suler, 2004). Given the increasing number of people online, concerns about privacy are also increasing (Teubner & Flath, 2019). Users thus seek to limit who has access to their information so that they can discriminately share information without fear that the information will be widely broadcast (Martin, 2016). When users want to discuss more personal matters, they therefore usually opt for communication channels that are more "private," such as private messages and emails with a selected audience. Accordingly, the distinction between public and private online communication channels helps people preserve different online identities and maintain public and private information boundaries online.

We thus propose communication channel boundary rules for privacy. This corresponds to Marx's (2001) proposition of directed communication as a natural boundary. We argue that any communication online that is directed to a specific addressee or audience, such as private messages, private chats, and emails, embodies a communication channel boundary. Thus, content and information delivered via private communication channels should be kept private rather than being analyzed and reused by platform providers, even though they technically have ready access to this content. Therefore, in some countries, such as the US, multiple legal cases have been raised against online service providers such as Google and Facebook for scanning private messages stored on their servers for advertising purposes.[2] Hence, we hypothesize:

H1: Personalized ads based on information from private communication channels lead to less perceived privacy than those from public communication channels.

2.3.2 Platform Boundaries

Social boundaries suggest that people should be discreet about what others share with them based on their professional ethics (e.g., lawyers or doctors) or social expectations (Marx, 2001). People tend to treat the digital medium as if it were real life (Reeves & Nass, 1998). In real life, we choose to open up to certain people and expect them to keep our secrets. Similarly, in the online world, we choose to disclose more information on some platforms than on others. People typically set different privacy expectations for different online platforms (Wang et al., 2017). A recent meta-analysis revealed that people are likely to be less concerned about privacy on relationship-building platforms such as Facebook than on service-oriented instrumental platforms such as Google Search or online forums (Yu et al., 2019). People also tend to disclose more private or sensitive information on relationship-building platforms (Osatuyi, 2013).

We expect what we have shared with one platform (e.g., Facebook) should be kept on the platform and not be accessed by other platforms (e.g., Google ads). This is similar to what Smith et al. (1996) termed "unauthorized secondary usage," where information is collected by one organization for one purpose but released to another organization without consent and used for another purpose. The secondary use of data has been a primary privacy concern for users (Gerlach et al., 2015), and external secondary usage exacerbates this concern (Smith et al., 1996).

[2] More coverage can be found at https://archive.nytimes.com/www.nytimes.com/interactive/2013/10/02/technology/google-email-case.html and https://www.bloomberg.com/news/articles/2014-01-02/facebook-sued-over-alleged-scanning-of-private-messages

Table 3. Relationships between This Research and Prior Literature

Marx (2001)	This research	Contextual feature
Social boundaries delineate expected secrecy for certain roles.	***Platform boundaries*** are set according to which platform the content is being shared on. What is shared on one platform should not be used by another platform for personalization.	Source of information
Spatial boundaries delineate where the information sharing happens.	***Device boundaries*** are set according to which device the content is being shared on. What is shared on one device should not be used for personalization on another device.	Location of sharing
Natural boundaries delineate an explicit audience	***Channel boundaries*** determine the audience of the message: private message versus broadcast. Private channels represent strong physical properties that lead people to believe they are in a personal space. People who are not granted access cannot enter this space. Private messages should not be used for personalization.	The intended audience
Temporal boundaries delineate the transient nature of information.	***Temporal boundaries*** of the shared content concern the "right to be forgotten" and content shared in the distant past should not be used for personalization.	Time of sharing
N/A	***Business-personal boundaries*** describe the rationale or purpose behind the shared content. Content created for personal purposes should not be used for personalization	Purpose of information

Technologies that allow businesses to identify a group of consumers for targeting by tracking customers across websites and platforms, such as web bugs, cookies, and clickstream data, are primary sources of privacy concerns (Goldfarb & Tucker, 2011). Research has confirmed that if a user perceives that a personalized ad on Facebook is based on data from external sources such as browsing history from other websites rather than data shared to Facebook, they tend to perceive less privacy (Kim et al., 2019; Zhu & Kanjanamekanant, 2021). Therefore, we propose:

H2: Personalized ads based on information shared on a different platform lead to less perceived privacy than information shared on the same platform.

2.3.3 Device Boundaries

Cross-device identification technology enables marketers to identify and target a person who, for example, is on Facebook using a personal computer and later watches YouTube videos on their mobile phone. Technologies that match the identity of customers across diverse devices and platforms allow organizations to more accurately predict user behavior and these technologies are experiencing exponential growth due to their effectiveness (Neufeld, 2017). However, such technologies have also raised serious privacy concerns (Montgomery et al., 2018). A Federal Trade Commission report revealed that many consumers are surprised and concerned to find that their browsing behavior on one device may inform ads on another device (Federal Trade Commission, 2017).

When people use online services, they tend to spontaneously create virtual boundaries as a means to control their online information (Lin & Armstrong, 2019). For example, people may set different privacy restrictions in chat groups, photo albums, or even their profile pages. One way for individuals to manage boundaries between private and public spheres is by separateness: separating themselves and the information they want to keep secret from others (Acquisti et al., 2018). One way that people develop personal privacy boundaries is by separating the use of work and personal mobile devices or computers (Cecchinato et al., 2015).

Separateness echoes what Marx (2001) proposed as spatial boundaries, which enable the separation of information from various aspects (such as location) of one's life. In the online world, users observe spatial boundaries by using different devices or gadgets for different purposes. Therefore, we hypothesize that if users perceive that personalized ads are based on information shared to a different device instead of the one they are currently using, they would perceive less privacy. This, however, excludes data stored on cloud services that aims to provide ubiquitous access and multiscreen roaming experiences for different devices, such as Dropbox or Google Drive.[3]

H3: Personalized ads based on information shared to a different device lead to less perceived privacy than information shared to the same device.

[3] We thank an anonymous reviewer for making this point.

2.3.4 Temporal Boundaries

To conduct business more effectively, firms rely on both past and current customer data to make inferences about their preferences. However, customers may be concerned that accessing a full range of historical data may come at the expense of their privacy (Holtrop et al., 2017). Lawmakers have enacted regulations regarding the storage of individual customer data for prolonged periods of time (Holtrop et al., 2017). There are several reasons why temporal boundaries should be set to regulate the use of user data. First, customer behaviors may change over time; using historical data may not produce an accurate prediction of the customer's current preferences (Lewis, 2005). Second, people's preferences regarding privacy may also change over time. This is particularly true for teenagers, for example, who may recklessly disseminate their personal information without thinking much about the consequences but later come to regret it (Ayaburi & Treku, 2020; Chou et al., 2019; Hallam & Zanella, 2017). Finally, similar to the rationale of the "right to be forgotten" promulgated by the European Union, over time, data may become "inaccurate, inadequate, irrelevant, or excessive" (Bode & Jones, 2017, p. 77). People should have the right to erase outdated data, especially those seeking to recover from a bankruptcy, negative credit record, or criminal history (Bode & Jones, 2017).

When people share their information online, they do not expect the information to be kept forever—or, as Marx (2001, p. 158) put it, ephemeral information is like a river flowing, and should not be preserved. Consumers' needs, preferences, and behaviors change over time (Lewis, 2005). Information shared may soon become irrelevant. A one-time booking of hotels in a particular city should not generate ads for hotel room sales in that city for a prolonged period. People are also entitled to a clean start. For example, a recovering online game addict may sense an intrusion of privacy when ads from game companies still target them. There should be temporal boundaries so that our digital remnants are relevant only temporarily. People understandably dislike feeling "stalked" for weeks by personalized ads for a particular product after conducting an online search for the item on a search engine or via an online retailer's website; such ads can feel like an unrelenting salesperson that will not leave them alone (Learnmonth, 2010). Therefore, we hypothesize:

H4: Personalized ads based on information shared some time ago lead to lower perceived privacy than information shared recently.

2.3.5 Business-Personal Boundaries

Finally, to reflect the overarching concept of public-private boundaries, we propose business-personal purpose boundaries that capture the nature of the information, i.e., whether the information is for business/public purposes or personal/private purposes. People's disclosure behaviors differ in professional versus nonprofessional contexts. Research has shown that people have a higher tendency to disclose more personal information when the context is nonprofessional versus professional (John et al., 2011). This signifies that information relating to business would have different privacy boundaries than information related to one's personal life. Furthermore, people's thresholds for privacy vary between business and personal information. Privacy has traditionally been viewed as a reasonable claim primarily in private domains (Palm, 2009). Privacy issues related to work are different from general privacy issues (Persson & Hansson, 2003). People are likely to be more tolerant of privacy invasions at work because their right to privacy is frequently "overridden by competing moral principles" that follow from the contract of employment to ensure that employees perform the appropriate tasks and fulfill their role responsibilities (Persson & Hansson, 2003, p. 59). As a result, what would be considered unacceptable in a private setting, such as electronic surveillance, is justified at work if certain criteria are met (Persson & Hansson, 2003).

The idea of business-personal boundaries extends Marx's (2001) discussion of the line between personal information that should be kept private versus social information that is, by nature, public. Nissenbaum (2010) argued that the purpose of using information matters in determining privacy. When the purpose is not related to business purposes, the amount of information and level of privateness/sensitivity tend to be higher than they are in a business context (John et al., 2011), and it is expected that stricter confidentiality will be observed. Therefore, the breach of boundary rules related to personal (vs. business) information typically results in heightened concerns about privacy. Gironda and Korgaonkar (2018) warned against advertisements containing too much personal information about an individual as they may be perceived as disturbing and even "creepy." Therefore, we hypothesize:

H5: Personalized ads based on information pertaining to one's personal life lead to less perceived privacy than those based on information pertaining to business.

3 Research Methodology

3.1 Vignette Survey

The factorial survey approach uses vignettes or scenarios to provide contextual details related to decision-making situations and asks respondents to rate a series of hypothetical vignettes. It enables researchers to obtain reliable and valid measures of

perceptions related to participants' experiences and has been applied widely in IS research (e.g., Dennis et al., 2012; Johnston et al., 2017; Siponen & Vance, 2010; Vance et al., 2014). We created hypothetical vignette scenarios, each containing a piece of personalized advertisement copy that included manipulated contextual stimuli, or vignette factors. Our study consists of five factors, each with two values. This aggregated to 32 unique vignette sets. Table 4 below summarizes the vignette factors, levels, and possible combinations.

We used a Taiwan-based market research firm to distribute our online survey. The firm has over 200,000 active members who voluntarily participate in market surveys for redeemable points as rewards. Invitation emails with links to the survey were sent to members until an adequate number of responses were received during June 2018. We generated ten vignettes for each respondent via a randomized vignette generator. After a pretest with a group of graduate students, we confirmed that a vignette pack comprising 10 vignettes was a suitable number for respondents of our study (Aguinis & Bradley, 2014).

The data from a total of 207 online respondents (2,070 vignettes) were analyzed, with no missing data. For each of the vignettes, an average of 64 ratings was received. Each respondent spent about 5-6 minutes completing the survey. Table 5 provides the demographic characteristics of our respondents.

Each respondent was given the following instructions about the survey:

> *This study uses situational vignettes to explore potential factors that might influence your privacy perceptions. Each of the following ten vignettes describes a scenario that is slightly different from each other—for example, using your* ***mobile phone*** *or* ***computer****, posting on the* ***Facebook timeline*** *or* ***Facebook messenger****,* ***a month*** *later or* ***two days*** *later, browsing* ***Facebook*** *or* ***Gmail****,* ***business trip*** *or* ***family tour package****. Before filling out the survey, please note these differences.*

The respondents were then asked to rate their perceived privacy in each of the situations described. Perceived privacy is an individual's self-assessed state of how their privacy is preserved (Dinev et al., 2013). We measured perceived privacy with items from Dinev et al. (2013). After each vignette, the respondents were asked to rate whether they felt comfortable, whether they felt they had enough privacy, and whether they felt their privacy was preserved in the situation described.

3.2 Control Variables

Following prior privacy research, respondents' gender, education, age, and income level were used as control variables (Park, 2015). We also assessed and controlled for perceived information ownership by Facebook with one item "Do you think online websites such as Facebook have ownership of the information you posted on them?" (Martin & Murphy, 2017).

3.3 Analysis

We modeled our dataset at two levels—the five vignette factors (communication channel, platform, device, time, and purpose) and individual effects (random effects). Procedures to test whether aggregation bias existed (if the behavior of all respondents could be described by one regression) was executed following Jasso (2006). First, we tested whether individual effects, i.e., random effects, matter by comparing the model with fixed factors and the random-intercept-only model using the *stats package*, *lmerTest package* (Kuznetsova et al., 2017), and *lme4 package* (Bates et al., 2015) in R (Team, 2018). The Shapiro-Wilk normality test suggested that the data was not normally distributed ($W = 0.96542$ and $p < 0.001$). Thus, the generalized linear model was used.

The general equation is:

$$Y_{ij} = \beta_{0j} + \beta_1 Device_{j1} + \beta_2 CommuncationChannel_{j2} + \beta_3 Time_{j3} + \beta_4 Purpose_{j4} + \beta_5 Platform_{j5} + e_j$$

where Y_{ij} is the rating of vignette *j* by the i^{th} respondent, β_{1-5} are regression coefficients of the five vignette factors, and e_j is the regression residual error term. Then we compared the null model with the random-intercept-only model: $Y_{ij} = \gamma_{00} + u_{0j} + e_{ij}$, where Y_{ij} is the rating of vignette *j* by the i^{th} respondent, γ_{00} is the random intercept, u_{0j} is the (random) residual error term, and e_{ij} is the respondent error term. Next, we compared the results to other mixed models—random intercept with common slope, common intercept with random slope, and random intercept with random slope. The final mixed model with random intercept and random slope can be expressed as:

$$\begin{aligned} Y_{ij} = \beta_0 + \beta_1 Device_{ij} + \beta_2 CommuncationChannel_{ij} \\ + \beta_3 Time_{ij} + \beta_4 Purpose_{ij} \\ + \beta_5 Platform_{ij} + u_{0j} \\ + u_{1j} Device_{ij} \\ + u_2 CommuncationChannel_{ij} \\ + u_3 Time_{ij} + u_4 Purpose_{ij} \\ + u_5 Platform_{ij} + e_{0ij} \end{aligned}$$

where u_{0j} denotes a departure from the overall intercept β_0 , u_{1-5} represents random effects associated with each β_{1-5} , and e_{0ij} is the individual-level residual or respondent error term.

Table 4. Vignette Factors and an Example

Vignette Factor	Vignette level
Communication Channel	Facebook Timeline (0) / Facebook Messenger (1)
Platform	Facebook (0) / Gmail (1)
Device	mobile phone (0) / computer (1)
Time	two days later (0) / a month later (1)
Purpose	accommodation for your business trip (0) / family tour package (1)
Template	**Narrative example**
One day, you asked for recommendations for [PURPOSE] in Japan via [COMMUNICATION CHANNEL] using your mobile phone. [TIME], while browsing [PLATFORM] on your [DEVICE], you saw relevant, targeted advertisements.	One day, you asked for recommendations for accommodation for your business trip to Japan via Facebook Messenger using your mobile phone. Two days later, while browsing Facebook on your computer, you saw relevant, targeted advertisements.

Table 5. Demographic Characteristics of the Respondents (*n* = 207)

	Items	Frequency	Percent
Gender	Male	107	51.7
	Female	100	48.3
Age	15 - 19	35	16.9
	20 - 29	50	24.2
	30 - 39	51	24.6
	40 - 49	48	23.2
	50 and above	23	11.1
Income (yearly)	NTD 250,000 and below	44	21.3
	250,001 – 500,000	67	32.4
	500,001 – 750,000	56	27.0
	750,001 – 1,000,000	22	10.6
	1,000,000 and above	18	8.7
Education	Middle school	3	1.4
	High school	24	11.6
	College	149	72.0
	Graduate school	31	15.0

4 Results

4.1 Common Method Bias

Common method bias was assessed in two ways. First, as shown in Table 6, none of the correlations between variables was higher than 0.9, suggesting that there was no strong method bias (Pavlou et al., 2007). Second, the variance inflation factor (VIF) and the tolerance of the constructs were examined and reported—communication channel (1.025, 0.976), platform (1.010, 0.990), device (1.032, 0.969), time (1.050, 0.952), purpose (1.044, 0.958), gender (1.129, 0.886), income (1.515, 0.660), age (1.440, 0.694), education (1.382, 0.724), and perceived information ownership (1.045, 0.957). All values were within the recommended ranges (VIF < 5 and tolerance > 0.2), suggesting that our data was not likely affected by common method bias (O'Brien, 2007). Finally, we alleviated potential concerns about common method bias by collecting nonidentifiable, anonymous data, which can help minimize method bias (Podsakoff et al., 2003).

4.2 Model Comparison and Selection

We tested and compared several alternative models to determine the best fit for our data. The GLM model (Model 1) accounted for 7.38% of total variance with an Akaike information criterion (AIC) value of 5480 and a Bayesian information criterion (BIC) value of 5519. The random-effect model (Model 2) showed a drastic model improvement with an *R*-squared of 0.537, and an AIC and BIC of 4560 and 4577, respectively.

Table 6. Correlation Matrix for Estimates of Fixed Effects

	Privacy	Channel	Purpose	Time	Device	Platform	Gender	Income	Age	Edu
Channel	-0.326									
Purpose	-0.292	0.063								
Time	-0.443	0.082	0.181							
Device	-0.285	0.108	-0.056	0.096						
Platform	-0.230	0.054	-0.024	-0.015	-0.070					
Gender	-0.002	0.001	-0.006	0.005	0.000	-0.001				
Income	0.009	0.000	-0.003	-0.002	-0.001	0.003	0.237			
Age	0.002	0.001	0.003	-0.002	-0.002	-0.002	0.023	-0.467		
Education	0.008	0.002	0.001	0.004	-0.005	0.007	-0.087	-0.450	0.446	
Ownership	-0.052	0.006	0.000	-0.004	-0.003	-0.001	0.199	0.026	0.040	0.039

Table 7. Model Summary with Selection Criteria

	Fixed effects	**Random effects**	**Mixed effects**				
Model	**1**	**2**	**3**	**4**	**5**	**6[a]**	**7[b]**
Fixed effects	Yes	-	Yes	Yes	Yes	Yes	Yes
Random effects (respondents)	-	Yes	Yes	Yes	Yes	Yes	Yes
Intercept	-	Random	Random	Common	Random	Random	Random
Slope	-	-	Common	Random	Random	Random	Random
R^2	0.0738	0.5374	0.5887	0.6757	0.8349	0.8369	0.8343
Deviance	n.a.	4554	4299	4350	3738	3736	3728
AIC	5480	4560	4315	4394	3794	3794	3762
BIC	5519	4577	4360	4518	3952	3958	3948
Log-likelihood	n.a.	-2277	-2149	-2175	-1869	-1868	-1848

Note: [a]Model 5 + Random Effects (Vignette). [b]Model 5 + covariates

As Models 3-5 were nested within Model 2, we used the information criterion, the deviance difference test, and chi-square difference test to check whether there was a significant improvement in the model fit (Hox et al., 2018). The three nested models showed lower deviances and better AIC and BIC values. We further conducted chi-square difference tests. The chi-square difference statistics are summarized in Table 7. The results suggest that Model 3 and Model 5 provided a significantly better model fit than Model 2. Model 5 provided a substantial model fit improvement compared with Model 3, as the value of AIC, BIC, and deviance were significantly lower, with a chi-square difference of 560.8 (20) ($p < 0.001$). We concluded that the mixed-effect model should be used to explain how different factors lead to perceived privacy. In Model 6, we added a dummy variable, the vignette sequence number, as a random variable to test whether the vignette sequence had any effect on the judgment of perceived privacy ratings (Beham et al., 2019; Steiner et al., 2017; Su & Steiner, 2018). A parametric bootstrap (n = 1,000) was performed, and the result showed that the added random effect was not significant, in congruence with the likelihood ratio test (p = 0.1916). Therefore, Model 6 was not selected. Finally, we added the covariates and used the results from Model 7 for the parameter estimations. The covariates were selected from prior research related to privacy research and included age, gender, education (Li, 2014), income (Park, 2015), and information ownership (Martin & Murphy, 2017).

4.3 Parameter Estimates

The mixed-effects model informs us how fixed effects (boundary rules) and random effects (individual variations) influence the level of perceived privacy. Fixed effects were examined first. We calculated the significance of the fixed-parameter estimates using the type II Wald chi-square test and *t*-test with Satterthwaite's method. Standard error and confidence intervals were calculated using parametric bootstrapping with n = 1,000. The likelihood ratio test was used to test for the significance of the random variance components. From Figure 2, we can see that *communication channel*, *device*, and *purpose* showed negative and significant effects, whereas *time* and *platform* showed no significant effects on perceived privacy.

For control variables, only perceived information ownership by Facebook showed a significant positive effect on the level of perceived privacy, while age, gender, education, and income were not significantly related to perceived privacy. Therefore, respondents who thought that Facebook rightfully co-owned their personal information once they posted it perceived higher levels of privacy than those who did not think Facebook had ownership rights to their information.

While the fixed effects can help us understand how each type of boundary affects the level of perceived privacy for the population level, the individual-level effects and random effects tell us whether the contextual factors affect each respondent differently. The random intercepts account for individual differences in baselines (perceived privacy), and the random slopes account for possible differences in slopes (of each contextual factor). To examine the random effects, we performed the Brown-Forsythe test to check the homoscedasticity of individual-level effects (Dag et al., 2018). The random effects yielded an F ratio of $F(df1,df2) = 12.678$, $p < 0.001$, suggesting that the variances of each individual are statistically different.

The likelihood ratio test was used to test for the significance of each random variance component, and the 95% CI of variance *SD* estimate for each random component excludes zero, meaning each factor exerts different effects on the perceived privacy of different individuals.

The correlations between the random effects associated with each type of boundary and intercepts are -0.3, -0.26, -0.45, -0.25, -0.19 for communication channel, purpose, time, device, and platform, respectively. These results reveal that when the individual slope decreases, the level of individual intercept increases; in other words, the consequences of a boundary violation would be more severe for those with a higher baseline level of perceived privacy. Further, except for the individual platform random slope (skewness [g_1] = -0.22, p = 0.191), the rest of the individual random slopes for each boundary show significant negative skewness (communication channel = -1.63, $p < 0.001$; device = -1.11, $p < 0.001$; time = -1.30, $p < 0.001$; purpose = -2.30, $p < 0.001$). This provides evidence that some individuals are more adversely affected by the communication channel, device, time, and purpose boundary violations than others.

The predictive power of the mixed model significantly improved compared with the fixed-effect-only model. Figure 3 shows how the prediction of privacy is enhanced by incorporating the random effects into the model (more overlapping areas with raw data).

Following the reporting format of prior literature with mixed models (Bates et al., 2015; Chen et al., 2019; Hox et al., 2018; Ketelhöhn & Quintanilla, 2012; Orquin et al., 2020; Safi & Yu, 2017), we summarize the final model estimates and results in Table 8.

4.4 Summary of Hypothesis Testing

Table 9 below summarizes the hypothesis testing results. Specifically, communication channel boundaries (directed vs. nondirected), device boundaries (same device vs. cross-screen), and business vs. personal purpose boundaries are validated as significant predictors of perceived privacy with personalized ads at both the within-person (random effects, for each individual) and across-person (fixed effects, for the whole sample) level, while platform boundaries (same vs. cross-platform) and temporal boundaries (two days later vs. a month later) failed to affect privacy at the across-person level.

Our results show that for the whole sample, personalized ads based on the combination of private channel, different device, and personal purpose lead to the lowest mean values in perceived privacy, with private channel being the most salient factor in lowering privacy. Other different combinations of contexts lead to varying levels of perceived privacy, with the combination of public channel, same device, and business purpose generating the highest mean values of perceived privacy. For each individual, preserving all five boundaries leads to the highest perceived privacy.

5 Discussion

To reconcile the personalization-privacy paradox, we suggest delving deeper into the *privacy as a state* perspective and exploring where the boundaries are for information usage in personalized advertising. We found that all five proposed contextual conditions are significant predictors of perceived privacy within individuals.

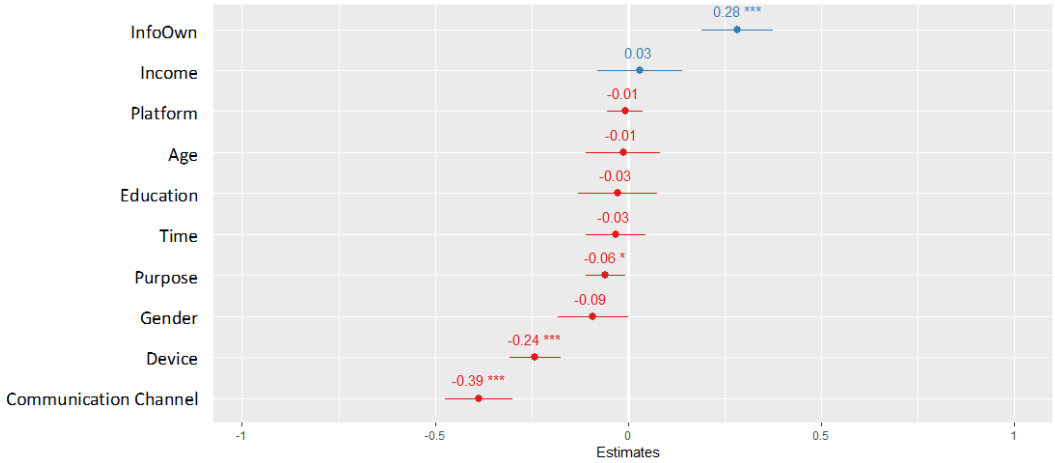

Figure 2. Fixed Effects Estimate of the Final Model

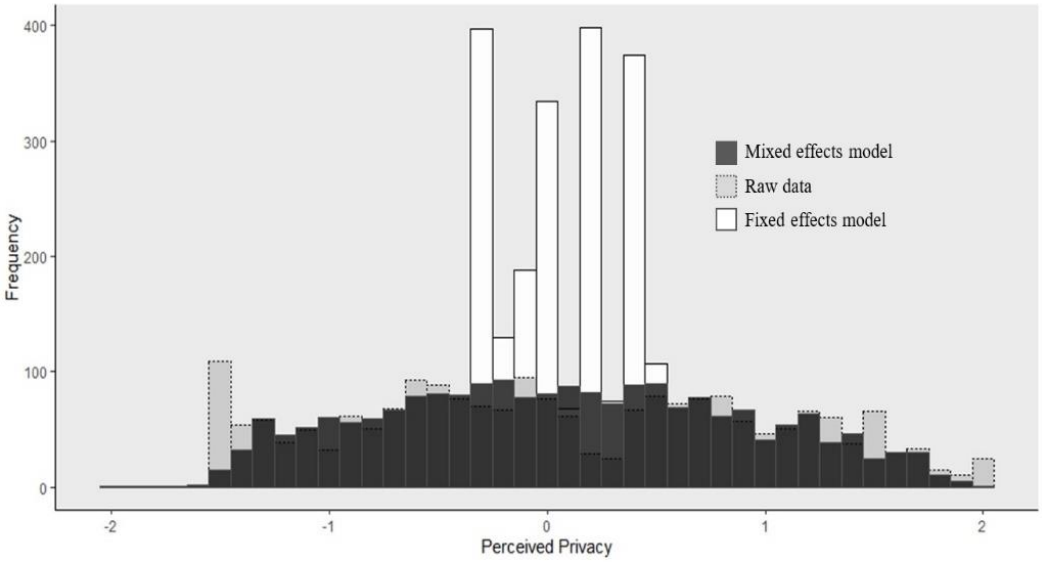

Figure 3. Comparing Model Predictions against Standardized Perceived Privacy Scores

Table 8. Final Model Estimates and Results

Fixed effects	Coefficient estimate	Standard error	Lower CI [2.50%]	Upper CI [97.50%]	Wald test *p*-value	*t*-test *p*-value
(Intercept)	0.432	0.059	0.315	0.546		$p < 0.001$ ***
Communication channel	-0.387	0.044	-0.477	-0.303	$p < 0.001$ ***	$p < 0.001$ ***
Platform	-0.008	0.024	-0.056	0.037	0.746	0.742
Device	-0.241	0.034	-0.311	-0.176	$p < 0.001$ ***	$p < 0.001$ ***
Time	-0.033	0.039	-0.108	0.043	0.422	0.407
Purpose	-0.059	0.026	-0.112	-0.007	0.022 *	0.024 *
Gender	-0.091	0.047	-0.185	0.001	0.003 **	0.053
Education	-0.027	0.052	-0.126	0.072	0.517	0.608
Age	-0.013	0.050	-0.103	0.089	0.636	0.792
Income	0.031	0.056	-0.086	0.138	0.736	0.584
Ownership	0.283	0.048	0.190	0.381	$p < 0.001$ ***	$p < 0.001$ ***

Random effects	Variance estimate	Standard deviation	Lower CI of *SD* [2.50%]	Upper CI of *SD* [97.50%]	Likelihood ratio test *p*-value
Residuals	0.149	0.386	0.369	0.403	
(Intercept)	0.583	0.764	0.668	0.849	
Comm. Channel	0.325	0.570	0.497	0.637	$p < 0.001$ ***
Platform	0.037	0.192	0.116	0.247	$p < 0.009$ **
Device	0.160	0.401	0.335	0.455	$p < 0.001$ ***
Time	0.240	0.490	0.425	0.551	$p < 0.001$ ***
Purpose	0.054	0.232	0.169	0.286	$p < 0.001$ ***
$^{*}p < 0.05$, $^{**}p < 0.01$, $^{***}p < 0.001$ Marginal R^2 (fixed effects only) = 0.164; Conditional R^2 (both fixed and random effects) = 0.834					

Table 9. Summary of Results

Hypotheses	**Coefficients** (fixed) **Variance** (random)	**Result**
H1: Personalized ads based on information from private communication channels lead to less perceived privacy than those from public communication channels.	Fixed: -0.387*** Random: 0.570***	supported
H2: Personalized ads based on information shared to a different platform lead to less perceived privacy than information shared on the same platform.	Fixed: -0.008 Random: 0.192**	partially supported
H3: Personalized ads based on information shared to a different device lead to less perceived privacy than information shared to the same device.	Fixed: -0.241*** Random: 0.401***	supported
H4: Personalized ads based on information shared some time ago lead to less perceived privacy than information shared recently.	Fixed: -0.033 Random: 0.490***	partially supported
H5: Personalized ads based on information pertaining to personal life lead to less perceived privacy than information pertaining to business.	Fixed: -0.059* Random: 0.232***	supported
Control variables	**Coefficients**	**p-value**
Gender	-0.091	0.053
Education	-0.027	0.608
Age	-0.013	0.792
Income	0.031	0.584
Information ownership	0.283***	$p < 0.001$
Note: $*p < 0.05$, $**p < 0.01$ $***p < 0.001$, (n.s.) = nonsignificant		

For each individual, we found that observing these five boundary rules was more likely to lead to higher perceived privacy than when these boundary rules were violated. Our results indicate that communication channel, device, and purpose are significant predictors of perceived privacy across the whole sample. Temporal boundaries and platform boundaries failed to achieve statistical significance when evaluated simultaneously with the other factors across the entire sample. Thus, observing the communication channel, device, and purpose boundaries led to higher averages of perceived privacy across the entire sample, while the effects of temporal and platform boundary rules did not lead to significantly higher averages of perceived privacy across the entire sample.

The relative strength of contextual stimuli may account for the result. Communication channel, device, and purpose boundary rules present strong stimuli that impact people's privacy evaluations in the face of personalization benefits. We conclude that since these three types of boundary rules are stable and salient, the respondents in our sample demonstrated consensus. In other words, we suspect that these rules are more likely to be activated. In contrast, temporal and platform boundaries are fluid. Individuals differ in their construal of psychological time (Zimbardo & Boyd, 1999), and differences in individuals' focus on the past (i.e., thinking more about the past), present, and future can trigger different decision and behavioral outcomes (Shipp & Aeon, 2019). Thus, temporal stimuli may not be activated for people who are more focused on the

present or the future versus the past. Similarly, individuals differ in their social expectations about digital platforms. Some people treat social networking sites such as Facebook as a part of their work life (Koch et al., 2012) and, as such, may not differentiate it from a more task-oriented platform such as Gmail.

5.1 Theoretical Implications

This research contributes to the extant literature in four ways. First, we contribute to the personalization-privacy paradox literature by enriching it from the *privacy as a state* perspective. Instead of viewing privacy as a result of a rational calculation or perceived control, we argue that privacy is a state of "maintaining boundaries" for all parties involved. The violation of boundary rules directly lowers privacy, echoing Dinev et al.'s (2015) observation of the frequency of spontaneous privacy decisions involving little rational deliberation. This approach complements the commodity and control perspectives (Smith et al., 2011) by addressing the complexity of privacy management and the limitations of our cognitive capabilities, and enhances our understanding of the privacy decision-making process by focusing on the role of context.

Second, we enrich the *privacy as a state* literature by exploring and empirically testing boundary-maintaining practices beyond information access. Prior *privacy as a state* literature has mostly viewed privacy as limiting who can and cannot have access to what information (Alpert, 2003; Di Pietro & Mancini, 2003; Smith et al., 2011) and has suggested that the decision to share information implies giving up any expectation of privacy regarding the shared information (Alfino & Mayes, 2003; Martin, 2015). We explored and tested a set of privacy boundaries considering when the data is shared (temporal boundary rule), why the data is shared (business/personal boundary), where the data is shared (device boundary rule), and how the data is shared after it is shared with a particular social group (platform boundary rule). We maintain that privacy does not stop at access to information, but also relates to further dissemination of the information *after* the information is shared. This shifts the focus of privacy from restricting access to information to delineating the proper use of information after it is shared, guided by a set of boundary rules, which could be mutually beneficial and sustainable for both consumers and platforms.

Third, we supplement the CPM literature by theorizing and testing a novel set of implicit privacy boundary rules. These virtual boundaries contribute to CPM by shedding light on where to draw the boundary in personal data, and how to avoid boundary turbulence. It enhances our understanding of people's expectations for online data privacy. Moreover, our results enrich and expand Marx's (2001) conceptualization of privacy boundaries to the online realm. We improve the applicability of privacy boundaries (Marx, 2001) and obtain one of the first sets of empirical results regarding such boundaries in the online personalized advertising context. By testing different contextual factors in the same model with both fixed and random effects, we are able to identify strong stimuli versus weak stimuli at different levels. Contextual factors exert different levels of strength on people's privacy perceptions. Stronger contextual factors, such as communication channel, device, and purpose boundary rules, are more likely to affect the state of privacy than weaker contextual factors. This framework could serve as a starting point toward building a comprehensive and nuanced understanding of how discrete, situational contexts shape implicit boundary rules regarding privacy.

Finally, from a methodological point of view, we contribute by considering the fixed effects and random effects on privacy simultaneously, compared with the fixed-effects-only approach in prior research. The differences between fixed and random effects signify the interpersonal variations of privacy perceptions: what one person deems as highly unacceptable may be found to be more acceptable by another person. For example, although, in general, the temporal boundary rule was not found to be statistically significant as a fixed effect, it is significant as a random effect, meaning that, individually, the time boundary matters in terms of privacy: the longer the data is retained and used, the less the perceived privacy. However, at the sample level, due to significant variations in individuals' perceived privacy, the effect may not be statistically significant. This finding reflects the heterogeneity of privacy preferences and responds to the call for more privacy research adopting the within-person approach (Hann et al., 2007).

5.2 Managerial Implications

For digital service providers, this research offers several suggestions on how to resolve the personalization-privacy paradox by considering specific, discrete contexts that users care about.

First, users value the boundary between public and private communication channels. This context-specific privacy boundary rule indicates that anything that is directed to a specific audience, for instance, a person or a group of friends, is intended for that audience only. The content in that communication should thus not be used for personalized ads as it invades the sharer's personal sphere. This includes private messages, emails, voice calls, chats, etc. Tapping into this kind of communication and reusing the content will evoke perceptions of privacy invasion and should be avoided. On the other hand, for content that is shared via a public channel, for example, public Facebook Timeline content, it is acceptable to reuse this information for personalized ad purposes.

Second, the device boundary rule advises that what happens on one device should stay on that device and not be propagated to other devices linked by the same person or account. For example, searches on a home computer should not be used for personalized ad content on one's work computer. This boundary rule fulfills people's desire to separate parts of their lives into different compartments and should be respected.

Third, temporal boundary rules demand that service providers treat information as ephemeral: At the exact moment that information arises it is relevant, but it should not be retained forever. Hence, it is acceptable to extract some content from users' recent interactions with others (public posts, discussion) or a system (e.g., a Google search), and users may appreciate this as relevant. However, when information is retained and repeatedly used to create personalized ads in the future, for example, it may raise concerns among users.

Fourth, the platform boundary rule suggests that selling or sharing users' information with other service platforms without prior consent is objectionable. What one shares with one platform should stay on that platform. Cross-platform sharing will lead to feelings of privacy invasion and may do more harm than good. The recent decision by Google to phase out the use of third-party cookies to preserve users' privacy[4] reflects the essence of observing the platform boundary: what happens on one platform should not be shared with other platforms.

Finally, considering the purpose behind shared content (business-related versus personal), people seem to have a lower threshold for privacy requirements in the context of business-related context and are less likely to be offended if information from this context is shared. Information pertaining to personal and private purposes, however, should be treated with extra care, as sharing such information would infringe on one's personal sphere and may lead to greater privacy concerns when inappropriately shared.

5.3 Limitation and Future Research

The findings of this research should be interpreted in light of certain limitations. The factorial vignette methodology uses hypothetical scenarios. Although the design captures the complexities of real decision-making and controls for confounding factors, researcher bias could influence the inclusion of factors, and factors that were not included could have changed the final results (Martin, 2018). We alleviate these concerns by drawing on Marx's (2001) conceptualization of privacy. The systematic development of privacy contexts helps incorporate essential contextual factors in the study. However, as we have discussed, contexts are, by nature, multifaceted. For instance, digital platforms can be broadly categorized into text-based context (e.g., Reddit), audio-based context (e.g., Clubhouse), and video-based context (e.g., Twitch). We do not know if the latency of sharing personal information (a temporal stimulus) (McFarland & Ployhart, 2015) influences the maintenance of boundaries and personalization-privacy decisions. Further, although our results show that the fixed effects of temporal and platform boundaries are not significant and that there are considerable variations between individuals, we did not identify where the variations came from and what they were. Future research could further explore what contributes to the considerable variations between individuals. Individual differences, such as contextual sensitivity (Adair et al., 2016) and temporal orientation (Shipp & Aeon, 2019) should also be considered.

6 Conclusion

With the advancement of technologies, while organizations can leverage the power of AI, machine learning, and data analytics to better understand their customers and capitalize on the benefits, they must be cautious about their usage of customer data. Customers have become sophisticated, knowledgeable, and sensitive about how their data has been used. Instead of focusing on customers' rational privacy decision-making, this study suggests that more attention should be paid to implicit boundary rules that help users make swift decisions in complex personalization-privacy situations. We propose five context-specific boundary rules on the premises of a contextual framework. The findings demonstrate the profound implications of different types of contextual factors. We encourage future research and practices to consider specific and distinct contexts regarding the evolvement of technologies that will continue adding richness to digital contexts.

Acknowledgments

The authors would like to thank our senior editor, Dr. Mikko Siponen and the anonymous reviewers for their constructive comments and guidance that helped us enormously in developing the paper. The paper received valuable suggestions and feedback from Dr. Jocelyn Cranefield. This research has been funded by the Ministry of Science and Technology of the Republic of China (Taiwan). The grant number is 107-2628-H-011-001-MY2.

[4] More details about Google's decision can be found at https://www.wsj.com/articles/five-things-we-know-about-googles-ad-changes-after-cookies-11615919502

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2018). Privacy and human behavior in the information age. In *The Cambridge Handbook of Consumer Privacy* (pp. 184-197). Cambridge University Press

Adair, W. L., Buchan, N. R., Chen, X.-P., & Liu, D. (2016). A model of communication context and measure of context dependence. *Academy of Management Discoveries*, *2*(2), 198-217.

Aguinis, H., & Bradley, K. J. (2014). Best practice recommendations for designing and implementing experimental vignette methodology studies. *Organizational Research Methods*, *17*(4), 351-371.

Alfino, M., & Mayes, G. R. (2003). Reconstructing the right to privacy. *Social Theory and Practice*, *29*(1), 1-18.

Alpert, S. A. (2003). Protecting medical privacy: challenges in the age of genetic information. *Journal of Social Issues*, *59*(2), 301-322.

Altman, I. (1975). *The environment and social behavior: privacy, personal space, territory, crowding*. Brooks/Cole Publishing Company.

Anderson, C. L., & Agarwal, R. (2011). The digitization of healthcare: boundary risks, emotion, and consumer willingness to disclose personal health information. *Information Systems Research*, *22*(3), 469-490.

Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly*, *30*(1),13-28.

Ayaburi, E. W., & Treku, D. N. (2020). Effect of penitence on social media trust and privacy concerns: The case of Facebook. *International Journal of Information Management*, *50*, 171-181.

Balapour, A., Nikkhah, H. R., & Sabherwal, R. (2020). Mobile application security: Role of perceived privacy as the predictor of security perceptions. *International Journal of Information Management*, *52*, Article 102063.

Bates, D., Mächler, M., Bolker, B., & Walker, S. (2015). Fitting linear mixed-effects models using lme4. *Journal of Statistical Software*, *67*(1), 1-48

Beham, B., Baierl, A., & Eckner, J. (2019). When does part-time employment allow managers with family responsibilities to stay on the career track? A vignette study among German managers. *European Management Journal*. *38*(4), 580-590.

Benlian, A. (2015). IT feature use over time and its impact on individual task performance. *Journal of the Association for Information Systems*, *16*(3), 144-173.

Bhave, D. P., Teo, L. H., & Dalal, R. S. (2020). Privacy at work: A review and a research agenda for a contested terrain. *Journal of Management*, *46*(1), 127-164.

Bode, L., & Jones, M. L. (2017). Ready to forget: American attitudes toward the right to be forgotten. *The Information Society*, *33*(2), 76-85.

Cecchinato, M. E., Cox, A. L., & Bird, J. (2015). Smartwatches. *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems*.

Chang, Y., Wong, S. F., Libaque-Saenz, C. F., & Lee, H. (2018). The role of privacy policy on consumers' perceived privacy. *Government Information Quarterly*, *35*(3), 445-459.

Chen, J., & Stallaert, J. (2014). An economic analysis of online advertising using behavioral targeting. *MIS Quarterly*, *38*(2).

Chen, Y. S., Rungtusanatham, M. J., & Goldstein, S. M. (2019). Historical supplier performance and strategic relationship dissolution: Unintentional but serious supplier error as a moderator. *Decision Sciences*, *50*(6), 1224-1258.

Choi, Y. K., Seo, Y., Wagner, U., & Yoon, S. (2020). Matching luxury brand appeals with attitude functions on social media across cultures. *Journal of Business Research*, *117*, 520-528.

Chou, H.-L., Liu, Y.-L., & Chou, C. (2019). Privacy behavior profiles of underage Facebook users. *Computers & Education*, *128*, 473-485.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, *10*(1), 104-115.

Dag, O., Dolgun, A., & Konar, N. M. (2018). onewaytests: An R Package for One-Way Tests in Independent Groups Designs. *The R Journal*, *10*(1), 175-199.

Dennis, A. R., Robert, L. P., Curtis, A. M., Kowalczyk, S. T., & Hasty, B. K. (2012). Research note—Trust is in the eye of the beholder: A vignette study of postevent behavioral controls' effects on individual trust in virtual teams. *Information Systems Research*, *23*(2), 546-558.

Di Pietro, R., & Mancini, L. V. (2003). Security and privacy issues of handheld and wearable wireless devices. *Communications of the ACM*, *46*(9), 74-79.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61-80.

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*(4), 639-655.

Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems*, *22*(3), 295-316.

Eastin, M. S., Brinson, N. H., Doorey, A., & Wilcox, G. (2016). Living in a big data world: Predicting mobile commerce activity through privacy concerns. *Computers in Human Behavior*, *58*, 214-220.

Federal Trade Commission (2017). *Cross-device tracking: An FTC staff report.* https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, *77*, 226-261.

Gerlach, J., Widjaja, T., & Buxmann, P. (2015). Handle with care: How online social network providers' privacy policies impact users' information sharing behavior. *The Journal of Strategic Information Systems*, *24*(1), 33-43.

Gironda, J. T., & Korgaonkar, P. K. (2018). iSpy? Tailored versus invasive ads and consumers' perceptions of personalized advertising. *Electronic Commerce Research and Applications*, *29*, 64-77.

Goldfarb, A., & Tucker, C. E. (2011). Privacy regulation and online advertising. *Management Science*, *57*(1), 57-71.

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*(2), 13-42.

Hinds, J., & Joinson, A. (2019). Human and computer personality prediction from digital footprints. *Current Directions in Psychological Science*, *28*(2), 204-211.

Holtrop, N., Wieringa, J. E., Gijsenberg, M. J., & Verhoef, P. C. (2017). No future without the past? Predicting churn in the face of customer privacy. *International Journal of Research in Marketing*, *34*(1), 154-172.

Hox, J. J., Moerbeek, M., & Van de Schoot, R. (2018). *Multilevel analysis: Techniques and applications* (3rd ed.). Routledge.

Hui, K.-L., Teo, H. H., & Lee, S.-Y. T. (2007). The value of privacy assurance: An exploratory field experiment. *MIS Quarterly*, *31*(1), 19-33.

Jasso, G. (2006). Factorial survey methods for studying beliefs and judgments. *Sociological Methods & Research*, *34*(3), 334-423.

John, L. K., Acquisti, A., & Loewenstein, G. (2011). Strangers on a plane: Context-dependent willingness to divulge sensitive information. *Journal of Consumer Research*, *37*(5), 858-873.

John, L. K., Kim, T., & Barasz, K. (2018). Ads that don't overstep. *Harvard Business Review*, *96*(1), 62-69.

Johnston, A. C., Warkentin, M., McBride, M., & Carter, L. (2017). Dispositional and situational factors: Influences on information security policy violations. *European Journal of Information Systems*, *25*(3), 231-251.

Kaaniche, N., Laurent, M., & Belguith, S. (2020). Privacy enhancing technologies for solving the privacy-personalization paradox: Taxonomy and survey. *Journal of Network and Computer Applications*, *171*, Article 102807 1-84

Karwatzki, S., Dytynko, O., Trenz, M., & Veit, D. (2017). Beyond the personalization–privacy paradox: Privacy valuation, transparency features, and service personalization. *Journal of Management Information Systems*, *34*(2), 369-400.

Ketelhöhn, N. W., & Quintanilla, C. (2012). Country effects on profitability: A multilevel approach using a sample of Central American firms. *Journal of Business Research*, *65*(12), 1767-1772.

Kim, T., Barasz, K., & John, L. K. (2019). Why am I seeing this ad? The effect of ad transparency on ad effectiveness. *Journal of Consumer Research*, *45*(5), 906-932.

Kobsa, A., Cho, H., & Knijnenburg, B. P. (2016). The effect of personalization provider characteristics on privacy attitudes and behaviors: An elaboration likelihood model approach. *Journal of the Association for Information Science and Technology*, *67*(11), 2587-2606.

Koch, H., Gonzalez, E., & Leidner, D. (2012). Bridging the work/social divide: The emotional response to organizational social networking sites. *European Journal of Information Systems*, *21*(6), 699-717.

Koh, B., Raghunathan, S., & Nault, B. R. (2020). An empirical examination of voluntary profiling: Privacy and quid pro quo. *Decision Support Systems*, *132*, Article 113285.

Kuznetsova, A., Brockhoff, P. B., & Christensen, R. H. B. (2017). lmerTest package: Tests in linear mixed effects models. *Journal of Statistical Software*, *82*(13). https://doi.org/10.18637/jss.v082.i13

Learnmonth, M. (2010). *The pants that stalked me on the web*. Advertising Age. https://adage.com/article/digitalnext/pants-stalked-web/145204

Lewis, M. (2005). Incorporating strategic consumer behavior into customer valuation. *Journal of Marketing*, *69*(4), 230-238.

Li, K., Lin, Z., & Wang, X. (2015). An empirical analysis of users' privacy disclosure behaviors on social network sites. *Information & Management*, *52*(7), 882-891.

Li, T., & Unger, T. (2012). Willing to pay for quality personalization? Trade-off between quality and privacy. *European Journal of Information Systems*, *21*(6), 621-642.

Li, Y. (2014). The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns. *Decision Support Systems*, *57*, 343-354.

Lin, S., & Armstrong, D. J. (2019). Beyond information: the role of territory in privacy management behavior on social networking sites. *Journal of the Association for Information Systems*, *20*(4), 434-475.

Liu, Z., & Wang, X. (2018). How to regulate individuals' privacy boundaries on social network sites: A cross-cultural comparison. *Information & Management*, *55*(8), 1005-1023.

Margulis, S. T. (2003a). On the status and contribution of Westin's and Altman's theories of privacy. *Journal of Social Issues*, *59*(2), 411-429.

Margulis, S. T. (2003b). Privacy as a social issue and behavioral concept. *Journal of Social Issues*, *59*(2), 243-261.

Martin, K. (2015). Privacy notices as tabula rasa: An Empirical investigation into how complying with a privacy notice is related to meeting privacy expectations online. *Journal of Public Policy & Marketing*, *34*(2), 210-227.

Martin, K. (2016). Understanding privacy online: Development of a social contract approach to privacy. *Journal of Business Ethics*, *137*(3), 551-569.

Martin, K. (2018). The penalty for privacy violations: How privacy violations impact trust online. *Journal of Business Research*, *82*, 103-116.

Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, *45*(2), 135-155.

Marx, G. T. (2001). Murky conceptual waters: The public and the private. *Ethics and Information Technology*, *3*, 157-169.

McCreary, L. (2008). What was privacy? *Harvard Business Review*, *86*(10), 123-130, 142.

McFarland, L. A., & Ployhart, R. E. (2015). Social media: A contextual framework to guide research and practice. *Journal of Applied Psychology*, *100*(6), 1653.

McNealy, J., & Mullis, M. D. (2019). Tea and turbulence: Communication privacy management theory and online celebrity gossip forums. *Computers in Human Behavior*, *92*, 110-118.

Metzger, M. J. (2007). Making sense of credibility on the Web: Models for evaluating online information and recommendations for future research. *Journal of the American Society for Information Science and Technology*, *58*(13), 2078-2091.

Montgomery, Chester, & Kopp. (2018). Health wearables: Ensuring fairness, preventing discrimination, and promoting equity in an emerging internet-of-things environment. *Journal of Information Policy*, *8*(1), 34-77.

Neufeld, E. (2017). Cross-device and cross-channel identity measurement issues and guidelines: How advertisers can maximize the impact of an identity-based brand campaign. *Journal of Advertising Research*, *57*(1), 109-117.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, *1*(79), 119.

Nissenbaum, H. (2010). *Privacy in context: technology, policy, and the integrity of social life*. Stanford Law Books.

O'Brien, R. M. (2007). A caution regarding rules of thumb for variance inflation factors. *Quality & Quantity*, *41*(5), 673-690.

Orquin, J. L., Bagger, M. P., Lahm, E. S., Grunert, K. G., & Scholderer, J. (2020). The visual ecology of product packaging and its effects on consumer attention. *Journal of Business Research*, *111*, 187-195.

Osatuyi, B. (2013). Information sharing on social media sites. *Computers in Human Behavior*, *29*(6), 2622-2631.

Palm, E. (2009). Securing privacy at work: the importance of contextualized consent. *Ethics and Information Technology*, *11*(4), 233-241.

Park, Y. J. (2015). Do men and women differ in privacy? Gendered privacy and (in)equality in the Internet. *Computers in Human Behavior*, *50*, 252-258.

Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS Quarterly*, *31*(1), 105-136.

Persson, A. J., & Hansson, S. O. (2003). Privacy at work: Ethical criteria. *Journal of Business Ethics*, *42*(1), 59-70.

Petronio, S. (1991). Communication boundary management: A theoretical model of managing disclosure of private information between marital couples. *Communication theory*, *1*(4), 311-335.

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

Petronio, S. (2002b). *Boundaries of privacy: Dialectics of disclosure*. Suny Press.

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

Preibusch, S., Kübler, D., & Beresford, A. R. (2013). Price versus privacy: An experiment into the competitive advantage of collecting less personal information. *Electronic Commerce Research*, *13*(4), 423-455.

Proudfoot, J. G., Wilson, D., Valacich, J. S., & Byrd, M. D. (2018). Saving face on Facebook: Privacy concerns, social benefits, and impression management. *Behaviour & Information Technology*, *37*(1), 16-37.

Reeves, B., & Nass, C. I. (1998). *The media equation: How people treat computers, television, and new media like real people and places*. CSLI Publications.

Safi, R., & Yu, Y. (2017). Online product review as an indicator of users' degree of innovativeness and product adoption time: A longitudinal analysis of text reviews. *European Journal of Information Systems*, *26*(4), 414-431.

Schoeman, F. D. (1984). *Philosophical dimensions of privacy: An anthology*. Cambridge University Press.

Schreiber, A. (2020). [Review of *Privacy's blueprint: The battle to control the design of new technologies*, by Woodrow Hartzog.] *The Cambridge Law Journal*, *79*(2), 377-380.

Sheng, H., Nah, F. F.-H., & Siau, K. (2008). An experimental study on ubiquitous commerce adoption: Impact of personalization and privacy concerns. *Journal of the Association for Information Systems*, *9*(6), 345-376

Shilton, K., & Greene, D. (2017). Linking Platforms, Practices, and Developer Ethics: Levers for Privacy Discourse in Mobile Application Development. *Journal of Business Ethics*, *155*(1), 131-146.

Shipp, A. J., & Aeon, B. (2019). Temporal focus: Thinking about the past, present, and future. *Current Opinion in Psychology*, *26*, 37-43.

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, *34*(3). 487-502

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, *35*(4). 989-1015

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, *20*(2), 167-196.

Smith, S. A., & Brunner, S. R. (2017). To reveal or conceal: Using communication privacy management theory to understand disclosures in the workplace. *Management Communication Quarterly*, *31*(3), 429-446.

Steiner, P. M., Atzmüller, C., & Su, D. (2017). Designing valid and reliable vignette

experiments for survey research: A case study on the fair gender income gap. *Journal of Methods and Measurement in the Social Sciences*, *7*(2), 52-94

Su, D., & Steiner, P. M. (2018). An evaluation of experimental designs for constructing vignette sets in factorial surveys. *Sociological Methods & Research*. *49*(2), 455-497.

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

Summers, C. A., Smith, R. W., & Reczek, R. W. (2016). An audience of one: Behaviorally targeted ads as implied social labels. *Journal of Consumer Research*, *43*(1), 156-178.

Sutanto, J., Palme, E., Tan, C.-H., & Phang, C. W. (2013). Addressing the personalization-privacy paradox: An empirical assessment from a field experiment on smartphone users. *MIS Quarterly*, *37*(4), 1141-1164.

Tavani, H. T. (2007). Philosophical theories of privacy: Implications for an adequate online privacy policy. *Metaphilosophy*, *38*(1), 1-22.

Team, R. C. (2018). *R: A language and environment for statistical computing*. R Foundation for Statistical Computing. https://www.R-project.org/

Teubner, T., & Flath, C. M. (2019). Privacy in the sharing economy. *Journal of the Association for Information Systems*, *20*(3), 213-242.

Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research*, *22*(2), 254-268.

Vance, A., Lowry, P. B., & Eggett, D. (2014). Using accountability to reduce access policy violations in information systems. *Journal of Management Information Systems*, *29*(4), 263-290.

Wang, L., Yan, J., Lin, J., & Cui, W. (2017). Let the users tell the truth: Self-disclosure intention and self-disclosure honesty in mobile social networking. *International Journal of Information Management*, *37*(1), 1428-1440.

Westin, A. F. (1968). Privacy and freedom. *Washington and Lee Law Review*, *25*(1), 166.

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems*, *12*(12), 798-824.. https://doi.org/10.17705/1jais.00281

Xu, H., Luo, X. R., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems*, *51*(1), 42-52.

Xu, H., Teo, H.-H., Tan, B. C. Y., & Agarwal, R. (2012). Research note—Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: A Study of Location-Based Services. *Information Systems Research*, *23*(4), 1342-1363.

Yaraghi, N., Gopal, R. D., & Ramesh, R. (2019). Doctors' orders or patients' preferences? Examining the role of physicians in patients' privacy decisions on health information exchange platforms. *Journal of the Association for Information Systems*, *20*(7), 928-952.

Yu, L., Li, H., He, W., Wang, F.-K., & Jiao, S. (2019). A meta-analysis to explore privacy cognition and information disclosure of internet users. *International Journal of Information Management*. *51*, Article 102015.

Zhu, Y.-Q., & Kanjanamekanant, K. (2021). No trespassing: exploring privacy boundaries in personalized advertisement and its effects on ad attitude and purchase intentions on social media. *Information & Management*, *58*(2), Article 103314.

Zimbardo, P. G., & Boyd, J. N. (1999). Putting time in perspective: A valid, reliable individual-differences metric. *Journal of Personality and Social Psychology*, *77*(6), 1271-1288.

About the Authors

Yu-Qian Zhu is a professor in the Department of Information Management, National Taiwan University of Science and Technology. She holds a PhD in Technology Management from National Taiwan University. Prior to her academic career, she served as R&D engineer and R&D manager in Fortune 100 and InfoTech 100 firms. Her research interests include information privacy and AI in organizations. She has published in journals such as *Journal of Management, Information & Management, International Journal of Information Management*, and *Government Information Quarterly*.

Kritsapas Kanjanamekanant is a PhD candidate in the Department of Information Management, National Taiwan University of Science and Technology. He holds a master's degree in management from the College of Management, Mahidol University. His current research interests include privacy, operations management, Robotic Process Automation, and foresight. He has vast industrial experience working with multinational companies in the food and garment sectors in Asia and the United States. He also practices lean manufacturing concepts, RPA, foresight, and data analytics using R and Power BI.

Yi-Te Chiu is a senior lecturer in the School of Information Management, Victoria University of Wellington, New Zealand. He holds a PhD in management from the Smith School of Business, Queen's University, Canada. Prior to his academic career, he worked in the software industry and helped organizations to improve the value that IS/T (information systems and technology) can bring to the overall organization. His research revolves around socio-technical aspects of emerging and disruptive technologies in digital work environments, with a particular interest in (a) sociotechnical analysis and design, (b) development methodologies, (c) adoption and implementation, and (d) personnel development and team/organizational capabilities. His recent research focuses on designing and evaluating AI-human collaborations for well-being and productivity. He is also enthusiastic about applying IS/T to foster teaching, learning, and research environments.