Information Resources Management Journal
Volume 37 • Issue 1 • January-December 2024

A Review of Online Information Privacy Theories Advanced in Eight AIS Journals Over the Last Decade

Alanawd Alshehri
https://orcid.org/0000-0002-5969-812X
University of Tabuk, Saudi Arabia

ABSTRACT

Privacy in the information systems (IS) context is becoming increasingly challenging and complicated. This study conducted a systematic review of the information privacy literature in the IS context to identify theories to understand and explain online information privacy. We reviewed eight journals from the Association for Information Systems over the 10-year period from 2013 to 2023. These journals were identified as mainstream in the IS discipline by the authors. We identified and explored 20 theories in depth. Our findings have important implications for academics and practitioners. Scholars can build on our findings to identify and adopt promising theories from other disciplines to be contextualized and applied to examining information privacy. New theories can enrich our understanding of information privacy and provide in-depth insights from different perspectives, thereby enhancing our understanding of information privacy issues.

KEYWORDS

Privacy, Information Privacy, Information Systems, Theory, Information Privacy Concerns, Privacy Calculus, Risk Calculus

INTRODUCTION

Information privacy is a fundamental and universal human right and a serious concern for individuals, organizations, societies, and governments worldwide (Bélanger & Crossler, 2011; Farayola et al., 2024). This privacy is becoming increasingly complicated in the era in which, throughout the globe, personal information has become a commodity that can be bought and sold (Wakefield, 2013(. With the growing use of social media platforms, protecting online information privacy has become a challenging endeavor as ubiquitous technologies can violate basic privacy principles through unregulated access to information and personal data stored and shared in different nodes of the global network (Becker, 2019; Romansky & Noninska, 2020). Security and privacy are at the center of information system (IS) artifacts (Lowry et al., 2017). Various risks have been identified from the breach of information privacy (Romansky & Noninska, 2020). In the digital age, individuals are continuously monitored as they consume products, services, and content (Zarsky, 2019(. The perception of privacy has continuously evolved from the original "right to be left alone" to the "right to be forgotten/to be erased" (Romansky & Noninska, 2020).

Privacy is defined and conceptualized in different ways and is impacted and perceived differently according to individual variances, cultures, and other factors (Miltgen & Peyrat-Guillard, 2014).

DOI: 10.4018/IRMJ.349977

Privacy concepts, definitions, and relationships are inconsistent across studies and disciplines, and privacy has been defined in various ways as "right," "state of access," "control," "emotion," "attitude," "behavior," "process," and "goal" (Dinev et al., 2013; Smith et al., 2011). Individuals may perceive the same information with various degrees of sensitivity and with a lack of absolute agreement on what information is public, personal, or private (S. Lin & Armstrong, 2019). Therefore, the definition of privacy needs to be revisited. In this global age, technologically connected artifacts are embedded and woven into our daily lives; hence, reliance on these ubiquitous artifacts has become inevitable for individuals, companies, societies, and countries. Thus, privacy issues and concerns are critical for maintaining the privacy of individuals and data. The current era can be characterized as data-centric, in reference to the collection, aggregation, and analysis of data to identify individuals and their behaviors. The resulting knowledge can be used for various purposes (e.g., IS design and development, targeting and marketing, personalized e-business services, the tracing of consumer behaviors, and contact tracing).

Protecting information privacy requires that we consider heterogeneous threats, control data flows in ubiquitous technologies, and develop appropriate policies for personal data protection (Romansky & Noninska, 2020). However, challenges have emerged because of cross-border data flow and conflicts in protection laws among countries that organize and prioritize protection differently (De Busser, 2017).

Ozdemir et al. (2017) distinguished between privacy in an institutional context and in a peer context. They investigated the factors influencing individuals' disclosure behaviors in a peer context. Individuals' willingness to share information is affected by external factors such as culture, experience, personal characteristics, and regulatory jurisdictions (Lin et al., 2021). The usability and aesthetic graphics of IT artifacts can influence users' perceptions of privacy risks and trust (Hoehle et al., 2019). Lin et al. (2021) investigated citizens' perceptions of contact-tracing applications during the COVID-19 pandemic and found that relative advantage, compatibility, and trusting beliefs increased the intention to use contact-tracing applications.

Governments and organizations worldwide have enacted and imposed information privacy safeguards to protect data; however, many breaches and misuses still occur. Privacy assurance is defined as a mechanism that directly or indirectly provides customers with an assurance and guarantee that their private information will be protected (Bansal et al., 2015). Posey et al. (2017) developed a taxonomy of personally identifiable PII breach information and identified eight clusters: threats to educational data, financial data, user account data, health data, medical data, and sensitive data; identity theft and fraud on portable computing devices; and threats to sensitive data on portable storage devices. Karwatzki et al. (2017b) identified six categories of actors who could gain access to personal information: the focal organization (service provider), third-party organizations, private contacts, professional contacts, intelligence services, and criminals. Bansal et al. (2015) found that various privacy assurance mechanisms play a role in enhancing individuals' trust and that variations in individuals' perception of privacy result in variations in individual behavior during the formation of trust to disclose private information. Parks et al. (2023) developed the privacy impact assessment (PIA) framework, which focuses on a balance between implementing privacy safeguards and countermeasures and hindering workflow in the healthcare context. In the PIA framework, sixteen means objectives and seven key fundamental objectives have been identified and incorporated to facilitate high-quality decision making vis-à-vis privacy and utility.

Information privacy is a multifaceted concept that has rarely been investigated (Bélanger & Crossler, 2011). Dinev et al. (2013) asserted that "the current understanding of privacy is largely fragmented and discipline-dependent." Privacy in the IS context is challenging and complicated to address, as it extends each link of the systems chain, that is, technologies, policies, processes, people, society, economy, and the legislature (Lowry et al., 2017). Thus, in this study, we contribute to information privacy research by examining the IS literature in depth to identify the established theories used to explain privacy. The findings can help us gauge extant theories to explain privacy and can constitute the basis for future studies on new theories to better explain and understand information

privacy. Therefore, we identify theories used in the information privacy literature and provide a comprehensive view of the theoretical foundation used and adopted to synthesize the findings.

There are fundamental changes in the privacy landscape that necessitate revisiting privacy in the current age, particularly from social and personal psychology perspectives. Stuart et al. (2019) developed a privacy framework to explain the complexity of privacy and encouraged collaborative future research to develop a comprehensive theory of the psychology of privacy. Therefore, in this study, we investigated the concept of privacy from the IS-artifact perceptive that is relevant to IS practices instead of focusing on the technological aspects of systems (Lowry et al., 2017). We revisited and reviewed privacy research in the present age and the prevalence of ubiquitous systems in the context of online platforms, Internet of Things (IoT), and big data (Lowry et al., 2017).

In the following section, we present the research review method we used to identify established privacy theories from the literature to explain and understand information privacy. The concluding section discusses future research directions, implications, and recommendations, as well as this research's limitations.

RESEARCH METHOD

We synthesized the findings of prior research to identify established theories that have shaped our understanding of information privacy in the global age of IS by adopting the PRISMA framework to conduct a systematic review (Moher et al., 2010; Page et al., 2021). Our process of systematic review consisted of four steps: (1) select literature sources, (2) identify the keywords for searching, (3) identify the inclusion criteria, and (4) select studies to be included in the review. Figure 1 presents the PRISMA flow diagram and summarizes the steps followed for extracting, filtering, and screening for each journal.

For the selection of literature sources, we identified and reviewed eight journals from the Association for Information Systems (AIS) covering the 10-year period from 2013 to 2023. These journals, listed in Table 1, were identified as mainstream in the IS discipline by the authors. Studies were extracted from various databases including Taylor & Francis Online, Wiley Online Library, JSTOR, Sage Journals, ScienceDirect, and AIS eLibrary. We identified two keywords, "information privacy" and "data privacy," to capture relevant articles that focus on information privacy. We searched the databases using only keywords present in titles, keywords, and abstracts. The inclusion criteria were empirical and conceptual research without preferences for quantitative or qualitative research methodologies. To select the studies for inclusion in the review, the screening process focused on information privacy theories relevant to the context of "information technology" and "information systems." The titles, abstracts, keywords, and full texts of the identified articles were read, and only those that met our inclusion criteria were included in the final dataset. We identified studies that examine information privacy, its conceptualization, and its factors and dimensions. Thus we obtained a final set of 25 papers (see Table 2), which summarize the total numbers of extracted theories by journal. We noticed that the Journal of Information Technology has no identified theories, and we attribute this to their different research focus, nature, and approach. A detailed summary with citations for the theories identified in the journals is presented in Table 3.

REVIEW OF THEORIES

On the basis of our systematic review, our final dataset included 25 papers. We identified 20 theories used to understand and investigate information privacy. We now introduce each theory and the ways it has been used.

Table 1. Eight journals from the Association for Information Systems (AIS)

Eight IS Journals
European Journal of Information Systems (EJIS)
Information Systems Journal (ISJ)
Information Systems Research (ISR)
Journal of the Association for Information Systems (JAIS)
Journal of Information Technology (JIT)
Journal of Management Information Systems (JMIS)
Journal of Strategic Information Systems (JSIS)
MIS Quarterly (MISQ)

Table 2. Summary of identified theories by journal in ascending order

Journal	Initial Extracted Papers	Filtered Papers
Journal of the Association for Information Systems (JAIS)	19	10
MIS Quarterly (MISQ)	137	4
European Journal of Information Systems (EJIS)	13	3
Information Systems Journal (ISJ)	6	3
Journal of Management Information Systems (JMIS)	24	3
Information Systems Research (ISR)	118	1
Journal of Strategic Information Systems (JSIS)	37	1
Journal of Information Technology (JIT)	5	0

Communication Privacy Management Theory

The communication privacy management (CPM) theory was developed to explain how individuals reveal or conceal private information. Petronio (2002) defined CPM as "a map that presumes private disclosures are dialectical, that people make choices about revealing or concealing based on criteria and conditions they perceive as salient, and that individuals fundamentally believe they have a right to own and regulate access to their private information." In CPM theory, the metaphor of a boundary is used to explain an individual's privacy management behavior. Boundary synchronicity/harmony occurs when individuals and co-owners understand and comply with mutually agreed-upon privacy rules. Boundary turbulence occurs when the information owner and co-owners fail in the coordination process to abide by and agree on mutual rules for boundary regulation, thus disrupting synchronized coordination (Petronio, 2002). According to CPM theory, individuals own their own private information and set rules to control it; when they disclose private information to others, they become co-owners of the information and negotiate mutually agreeable privacy rules for the shared information. Petronio (2002) identified five decision criteria used to develop privacy rules to manage boundaries: culture, gender, motivation, context, and risk-benefit ratio. Metzger (2007) adopted CPM theory in the e-commerce context to investigate information disclosure, finding that information seeking and information falsification were used as a privacy protection strategies. Xu et al. (2011) adopted CPM theory to develop a theoretical model that explains the link between individuals' privacy perceptions and institutional privacy assurances. In particular, they examined how institutional privacy policies and industry self-regulation can reduce individual privacy concerns. S. Lin and Armstrong (2019) adopted CPM theory to investigate individual privacy management behaviors on social network sites (SNS) in terms of information privacy (private information disclosure) and territory privacy

Table 3. Summary of theories adopted in information privacy research in the IS context

Theory		Reference	Journal
1	Communication privacy management theory	Yaraghi et al. (2019)	Journal of the Association for Information Systems
		Lin and Armstrong (2019)	Journal of the Association for Information Systems
2	Multidimensional developmental theory of privacy	Hoehle et al. (2019)	European Journal of Information Systems
		Hong and Thong (2013)	MIS Quarterly
3	Elaboration likelihood model	Bansal et al. (2015)	European Journal of Information Systems
4	Privacy calculus theory	Cheng et al. (2022)	European Journal of Information Systems
		Kehr et al. (2015)	Information Systems Journal
		Keith et al. (2015)	Information Systems Journal
		Teubner and Flath (2019)	Journal of the Association for Information Systems
		Choi et al. (2018)	Journal of the Association for Information Systems
		Yaraghi et al. (2019)	Journal of the Association for Information Systems
		Kordzadeh and Warren (2017)	Journal of the Association for Information Systems
5	Deterrence theory	Wall et al. (2016)	Journal of the Association for Information Systems
		Willison et al. (2018)	Journal of the Association for Information Systems
6	Social cognitive theory	Keith et al. (2015)	Information Systems Journal
7	Strain theory (Merton, 1938)	Wallet al. (2016)	Journal of the Association for Information Systems
8	Impression formation theory	Choi et al. (2018)	Journal of the Association for Information Systems
9	Structural holes theory	Osch et al. (2023)	Journal of the Association for Information Systems
10	Social capital theory	Osch et al. (2023)	Journal of the Association for Information Systems
11	Prevention motivation theory	Lee et al. (2018)	Journal of the Association for Information Systems
12	Activity theory	Valecha et al. (2021)	Journal of the Association for Information Systems
13	Theory of justice	Choi et al. (2016)	Journal of Management Information Systems
		Greenaway et al. (2015)	Information Systems Journal
14	Social norms theory	Choi et al. (2022)	Journal of Management Information Systems
15	Information boundary theory	Karwatzki et al. (2017a)	Journal of Management Information Systems
		Sutanto et al. (2013)	MIS Quarterly
16	Cognitive consistency theory: balance theory and congruity theory	Wakefield (2013)	Journal of Strategic Information Systems
17	Protection motivation theory	Boss et al. (2015)	MIS Quarterly
18	Uses and gratification theory	Sutanto et al. (2013)	MIS Quarterly
19	Prospect theory	Adjerid et al. (2018)	MIS Quarterly
20	Social exchange theory	Choi et al. (2015)	Information Systems Research

(managing the level of access to and interaction with individuals). Yaraghi et al. (2019) adopted CPM theory to examine privacy decision making between medical providers and patients to obtain patient consent for information disclosure when medical records are shared on health information exchange (HIE) platforms. Petronio and Child (2020) reviewed CPM conceptualization and operationalization in term of privacy boundaries, privacy rules, collectives, and privacy turbulence.

Multidimensional Developmental Theory of Privacy

Multidimensional developmental theory (MDT) is a framework for understanding individuals' perceptions of privacy. MDT defines individuals' privacy as a multidimensional and contextual concept that is affected by ego, environmental, and interpersonal dimensions (Laufer & Wolfe, 1977). The *ego dimension* refers to the influence of individuals' developmental processes on their perceptions of privacy. The ego can be interpreted as the impact of individual characteristics in terms of age, education, experience, computer literacy, and so on. The *environmental dimension* refers to external factors that influence individuals' abilities to perceive, have, and use available privacy options, such as variations in governmental privacy legislation and policies that provide various levels of privacy protection. Environmental factors that can affect an individual's perception of privacy may be environmental surroundings in physical, social, and cultural settings. The interpersonal dimension comprises information and interaction management. *Information management* refers to decision making regarding personal information disclosure, while *interaction management* refers to decision making regarding interactions with others. Thus, for MDT, privacy concerns are a result of personal and environmental and interpersonal impacts (Peras & Mekovec, 2022). MDT enables us to better understand emerging privacy-related issues in ubiquitous technological practices such as personalization marketing and cloud-based services. Peras and Mekovec (2022) adopted MDT to develop a conceptual model of cloud privacy concerns, including the three dimensions of interaction management, information management, and legislation. C. Wu and Li (2019) adopted MDT with a focus on the impact of environmental factors on privacy behavior and developed a theoretical model of the intention to boycott personalization marketing. Hoehle et al. (2019) adopted MDT to investigate the impact of mobile device application usability on customer privacy concerns and shopping efficiency. They found that customers' privacy concerns can be alleviated by adhering to usability principles and that artifact design and usability have an impact on individual privacy-related constructs, including trust and risk. Hong and Thong (2013) adopted MDT to investigate the concept of Internet privacy concerns and developed a theoretical framework to address them.

Elaboration Likelihood Model

The elaboration likelihood model (ELM) is a dual-process theory of information processing and persuasion that posits that processing information within a message involves two possible routes: central and peripheral (Bansal et al., 2015; Petty & Cacioppo, 1986). Thus, an individual attitude changes through both a central route and a peripheral route. These two routes represent the likelihood that individuals will expend the cognitive effort to process information and depend on an individual's motivation and ability (Kitchen et al., 2014). Individuals in a state of high elaboration likelihood with high motivation to process information choose the central route, which entails effort and time spent on scrutinizing information. Individuals in a state of low elaboration likelihood lack the motivation to process the information and choose the peripheral route, which relies on peripheral cues to evaluate the information. Peripheral cues are the factors affecting attitude through the peripheral route, while central cues are the factors affecting attitude through the central route. Zhou (2017) adopted the ELM to investigate privacy concern in location-based services and found that privacy concern affected by dual-influence of both central cues and peripheral cues. The central cues in terms of privacy policy and information quality and peripheral cues in term of reputation and privacy seals. Furthermore, Zhou (2017) found that privacy policy had the largest effect on privacy concern. Wang et al. (2020) found that self-disclosure intention on mobile social platforms develops along a dual route that is both

central and peripheral. Furthermore, they found that peripheral cues play the role of moderator between the central cues and self-disclosure intention. Bansal et al. (2015) adopted the ELM to investigate the role of privacy assurance mechanisms in enhancing individuals' trust. They found differences between individuals with high and low privacy concerns in forming trust when disclosing private information. Y. Li et al. (2019) provided a summary of central and peripheral routes in the IS context.

Privacy Calculus Theory

According to privacy calculus theory (PCT), individuals calculate the tradeoff between perceived risks and benefits along with the outcomes of this tradeoff (Cheng et al., 2022; Xu et al., 2009). *Perceived benefits* refers to individuals' perception of the value derived from information disclosure, whereas *perceived risks* refers to individuals' perception of the potential harm from information disclosure. Risks from information disclosure can lead to physical, financial, and moral damage (Cheng et al., 2022(. The privacy calculus is a complex psychological process affected by privacy controls and various risk and benefit factors (Cheng et al., 2022; Y. Li, 2012). Meier and Krämer (2024) investigated the psychological process of the privacy calculus and distinguished between the between- and within-person levels that exist when individuals make information disclosure decisions. They also distinguished between rational and intuitive privacy decision making styles. Decision making aids can be used to support individuals in privacy calculus decisions using privacy tools that show privacy levels and privacy information to individuals (Meier & Krämer, 2024). PCT explains how individuals deal with the tradeoff between perceived benefits and risks before disclosing personal information (Xu et al., 2009).

Cheng et al. (2022) adopted PCT in the context of ridesharing platforms. Kehr et al. (2015) extended PCT to consider the situation-specific assessment of risks and benefits that are influenced by dispositional factors such as privacy concerns and institutional trust. Kordzadeh and Warren (2017) adopted a privacy calculus to investigate the disclosure of personal health information in virtual health communities. They found that affective commitment did not affect information disclosure. Moreover, they found that privacy concerns decrease individuals' willingness to participate on virtual community platforms. Yaraghi et al. (2019) investigated the influence of physicians' recommendations on patients' decisions to disclose information on HIE platforms, which can enable healthcare providers to access patients' electronic health records (EHR). They found that patients do not simply follow their physician's recommendations for information disclosure; rather, they consider the benefits and risks of giving consent for information disclosure. The success of HIE depends on patient consent to share and disclose information that can be exchanged by healthcare providers. B. Choi et al. (2018) adopted privacy calculus to investigate the acceptance of friend requests on SNS. They found that privacy calculus is evaluated in terms of perceived risks, namely network mutuality and profile diagnostics, and previewed benefits in terms of expected social capital gains. They found that individuals' perceptions of risks and benefits influenced their connectivity on SNS. Teubner and Flath (2019) adopted privacy calculus in the sharing economy context, which is characterized by consumer-to-consumer information disclosure and the exchange of personal information that raises privacy concerns.

Deterrence Theory

Deterrence theory (DT) was originally developed in criminology research but has been used in IS security research to explain information security intention and behavior (Siponen et al., 2022) and to investigate information security policy compliance (Wall et al., 2016). This theory posits that the perception of sanctions designed to punish violators deters individuals from deviant behavior (Wall et al., 2016). Thus, deterrence aims to inhibit misconduct and precedes prevention measures that are used to deter intruders and prevent crime. Hu et al. (2011) investigated IS policy violations by employees in an organizational setting. They suggested that one possible solution is to establish and implement sanctions to deter and reduce future employee violations and misconduct. They identified and measured perceived deterrence according to the severity, certainty, and celerity of sanctions.

The *severity of sanctions* refers to "the perceived degree of punishment for the intended act" The *certainty of sanctions* refers to "the perceived probability of being punished for the intended act" The *celerity of sanctions* refers to "the perceived swiftness of being punished for the intended act" (Hu et al., 2011). Many studies have adopted DT in an organizational context to improve privacy and security compliance (Wall et al., 2016; Willison et al., 2018). Lembcke et al. (2019) found that perceived sanction severity had a positive impact on information security compliance. Herath and Rao (2009) adopted DT and found that resource availability is an important factor enhancing self-efficacy, which in turn is a significant predictor for policy compliance. Willison et al. (2018) reviewed and criticized the applicability of DT in information security literature and the way it has been adopted and contextualized to deter internal computer abuse in organizational settings. They argued that it was important to theoretically recontextualize DT and proposed future research areas.

Social Cognitive Theory

Social cognitive theory (SCT) focuses on the role of social influence in motivation and learning (Bandura, 1986, 1991). SCT posits that human behavior is extensively motivated and regulated by the ongoing exercise of self-influence (Bandura, 1991). According to SCT, individual behavior operates within the framework of reciprocal interactions among personal, behavioral, and social/environmental factors. The identified constructs of SCT include goals, self-evaluation of progress, outcome expectations, values, social comparisons, and self-efficiency (Schunk & Usher, 2012). *Self-efficacy* is a key construct in SCT. It refers to "an individual's cognition" of their "ability to act in the process of achieving a specific goal and a degree of self-confidence" in their ability (L. Ma et al., 2020). According to SCT, self-efficacy is an important determent for an individual's performance and affects the individual's behavior and the tasks they choose to perform. SCT is widely used to understand and predict individual behavior and in IS adopting behavior (D. Wu et al., 2021), as it helps understand and identify the influential factors between individual behavior and environmental outcomes. SCT has been used to understand the adoption of e-government systems (Rana & Dwivedi, 2015) and telemedicine services (D. Wu et al., 2021). Keith et al. (2015) adopted SCT to explain perceived mobile app risk and provider trust. They found that high individual self-efficacy positively affected trust in app providers and reduced perceived risks.

Strain Theory

Strain theory (ST) states that "certain strains or stressors lead to negative emotions, which create pressure for corrective action" which in turn result in crime as one possible response (Jang & Agnew, 2015). This classical theory of strain was developed originally in criminology by Merton (1938). Classic ST focuses on one type of strain, the inability to achieve conventional success goals (Jang & Agnew, 2015). Agnew (1992, 2006) extended the classical view of ST and developed general ST, which takes into account a broad range of strains including 1) the inability to achieve valuable goals, 2) losing valuable possessions, and 3) negative/unwanted behavior by others (Agnew & Scheuerman, 2010). Broidy and Agnew (1997) extended general ST and developed gendered general ST, which distinguishes between the types of strains and responses to strains in males and females.

Organizations under strain, such as the strain due to slack performance, are more vulnerable to violations of privacy regulations (Wall et al., 2016). According to ST (Merton, 1938), entities may seek to achieve their goals through deviant or non-routine behaviors when they are unable to do so through legitimate means (Wall et al., 2016). Adopting ST is a promising avenue to enrich understanding of privacy and cybercrime issues and can help improve compliance with privacy and security rules. Wall et al. (2016) developed a theoretical model of the selective organizational information privacy and security violations model to explain how organizational structures, processes, and characteristics of regulatory rules influence perceptions of risk in organizations under strain and thereby affect the likelihood of rule violations.

Impression Formation Theory

B. Choi et al. (2018) defined impression formation theory (IFT) as the process of interpersonal evaluation that begins when an interactant presents themself in a social interaction. Another individual typically attempts to process social information to develop an impression of the interactant. Depending on the individual's evaluation, positive impressions are typically met with positive responses, whereas negative impressions are often detrimental to relationship development. There are two types of information that influence the formation of impressions: category-based information, such as occupation type and gender, and attribute-based information, such as behavior and body language (Fiske & Neuberg, 1990). IFT helps us understand the key impression information that an individual considers when making decisions, forming relationships, and forming connections, thus revealing privacy-related information. In social media platforms, impressions are formed on the basis of self-disclosure information on social media profiles. Thus, self-disclosure is a central factor influencing the formation of social relationships online. The information disclosed can be positive, neutral, or negative, a description termed *self-disclosure valence* (B. Choi et al., 2018). Qin et al. (2021) investigated the effect of social media self-disclosure profiles on first-impression formation. They found that positive self-disclosure has a positive impact on impression formation and perceived trustworthiness and leads to the highest likability. B. Choi et al. (2018) investigated individual responses to online friend requests on SNS and their potential privacy implications. They adopted IFT to understand individuals' assessments and responses to online social network connections by identifying the key impression-related information considered in the process of forming impressions and the resulting outcomes that influence the development of social relationships.

Structural Holes Theory

The structural holes theory (SHT) focuses on weak connection between clusters/groups referred to as "holes" in social networks that create competitive advantage for an individual whose network spans the holes (Burt, 1992, 2002). SHT posits that the benefits of social capital result from the diversity and non-redundancy of information and perspectives that stem from occupying a brokerage position between loosely connected clusters (Osch et al., 2023). In SHT, a lack of connection among clusters/groups is referred to as a structural hole (SH). Thus, individuals occupying bridge positions among various clusters play an important role in providing social capital, as they control key information dissemination pathways (Burt, 2004). These bridge positions, which fill the holes, are known as SH spanners and are advantageous in controlling information diffusion to heterogeneous clusters and obtaining rich information from those clusters (Z. Lin et al., 2022). Osch et al. (2023) adopted SHT to investigate creative dialogue among groups and the roles of transparency and privacy in workplace technology-enterprise social networks (ESNs). ESNs enable the creators of groups to select transparency/privacy settings in which transparent group activities and exchanges are open to observation by any members of the ESN across the organization while private group activities and exchanges are open to group members only. They found that creative dialogues aligned with expansion emerged in the transparent groups, while creative dialogues aligned with reframing emerged in the private groups.

Social Capital Theory

Social capital theory posits that social relationships are resources that constitute valuable assets and are defined in various ways (Kim & Cannella, 2008). Coleman (1990) defined social capital by its function and indicated that social capital is created "when the relations among persons change in ways that facilitate action." Burt (1992) defined social capital on the basis of relationships such as "friends, colleagues, and more general contacts through whom you receive opportunities to use your financial and human capital." Putnam (1993) defined social capital as the property of groups and as "features of social organization, such as trust, norms, and networks that can improve the efficiency of society by facilitating coordinating actions." The underlying effect of social capital is

that relationships can influence individuals' perceptions, attitudes, behaviors, and relationships. Social capital is composed of complex interrelations between three dimensions: the structural, relational, and cognitive aspects (Claridge, 2018; X. Lin et al., 2013). The structural dimension concerns network structure—that is, the structure of access to people and resources—while the relational and cognitive dimensions concern capability, perception of resources exchanged, and shared perception and feelings (Claridge, 2018). Osch et al. (2023) adopted social capital theory to investigate the social capital effect (transparent groups vs. private groups) on information sharing and the level of sharing in enterprise social media. X. Lin et al. (2013) adopted social capital theory to identify factors that influence an individual's information sharing behaviors on social media sites; they identified social presence, privacy risk, and commitment.

Prevention Motivation Theory

Prevention motivation theory (PMT; Lee et al., 2018) is similar to protection motivation theory (Rogers, 1975), in which individuals are motivated to take protective actions in relation to their fear of a threat and desire to avoid risks (Lee et al., 2018). However, in PMT, additional factors, such as the possibility of self-protection failure, the possibility of preventively eliminating the origin of cyberattacks, and the cost-effectiveness gap between prevention and protection, are considered (Lee et al., 2018). Thus, if individuals fear that the protection approach may fail, they can prevent potential threats. PMT focuses on preventing or reducing prominent sources of risk rather than on threat appraisal and coping appraisal to provide threat protection. Lee et al. (2018) developed PMT and five principles for bright Internet initiatives: origin responsibility, deliverer responsibility, identifiable anonymity, global collaboration, and privacy protection. Lee et al. (2018) defined the bright Internet as "the Internet that can preemptively reduce the origins of cybersecurity threats by having the capability of identifying malicious origins and deliverers on a global scale, while maintaining the freedom of anonymous expression and a legitimate level of privacy protection for innocent netizens."

Activity Theory

Activity theory (AT; Verenikina, 2001) provides a theoretical framework for analyzing and understanding human interaction by using tools and artifacts (Hashim & Jones, 2007). Kaptelinin and Nardi (2012) identified AT as the foundational concept of human activity, which is understood as a purposeful, mediated, and transformative interaction between human beings and the world. Activity is divided into the analytical components of subject, tool, and object to understand the relationship between the subject (actor) and object (entity) using the mediated tools that facilitate action execution (Kaptelinin & Nardi, 2012; Hashim & Jones, 2007). Engeström (2001) extended the original AT to include two more elements: rules and division of labor. Thus, community and interaction among them can be analyzed, and work can be coordinated. The five basic principles of AT are hierarchical structure of activity, object orientedness, internalization/externalization, tool mediation, and development, which are considered integrated systems because they represent various aspects of the whole activity (Kaptelinin & Nardi, 2012). In AT, technology integration is a tool to facilitate social interaction (Hashim & Jones, 2007). Valecha et al. (2021) investigated the violation of privacy laws resulting from the leaking of patient health information and adopted AT to develop an access control model to detect and mitigate information leakage.

Theory of Justice

Justice (also known as fairness) determines how fairly individuals are treated by others, either individuals or organizations. Justice theory identifies three types of justice: distributive, procedural, and interactional. *Distributive justice* refers to the perceived fairness of outcome distribution. Distributive justice is based on the notion of equity in which individuals compare inputs to outputs (B. C. F. Choi et al., 2016). *Procedural justice* refers to the perceived fairness of the procedure used to produce outcomes (B. C. F. Choi et al., 2016). Distributive justice focuses on accomplished ends, whereas

procedural justice focuses on the means to accomplish them. *Interactional justice* refers to the perceived fairness of interpersonal treatment in which procedures are executed or outcomes delivered. Greenaway et al. (2015) adopted procedural justice to investigate differences in organizational approaches to information privacy offered to individual customers, as personal data is being combined and used for personalization. B. C. F. Choi et al. (2016) investigated online customer behavior responses to online firms' post-incident recovery endeavors in the case of privacy breaches. They found that the three types of justice jointly influence individual psychological responses, which in turn influence individuals' decisions regarding post-incident outcomes, such as post-word of mouth and the likelihood of switching (B. C. F. Choi et al., 2016). Introna (2000) discussed workplace surveillance from a justice and fairness perspective and proposed establishing a framework for distributing the rights of privacy and transparency between the individual (employee) and the institution (employer).

Social Norms Theory

Social norms can be defined as behaviors prevalent within a group that influence individuals' behavioral decisions. As individuals are social beings, they are affected by other individuals and prevailing social norms. Social norms are described as rules of conduct that are dynamic, changeable over time, culture and context dependent, and collectively shaped; these rules can influence how one behaves; they are learned through interaction and observation (Rashidi et al., 2020). Social norms in relation to group size, levels, and variances among group members can affect self-disclosure behaviors (H. S. Choi et al., 2022). Social norms govern acceptable and unacceptable behavior and can influence individuals' behaviors and decision-making. H. S. Choi et al. (2022) adopted social norms theory to investigate reviewers' self-disclosure behavior in the context of product review sites. As part of the product review process, individuals may disclose personal information that compromises privacy. H. S. Choi et al. investigated the effects of group size and variance on self-disclosure behavior. Rashidi et al. (2020) investigated sanctions of nonconforming social norms on SNS. They identified social norms on SNS as implicit and informal, playing an important role in defining acceptable behavior. They identified three sanction strategies: on-site and off-site sanctions, individual and collaborative sanctions, and visible and invisible sanctions. Spottswood and Hancock (2017) investigated the effects of social norms on disclosure and privacy decisions on SNS.

Information Boundary Theory

Information boundary theory (IBT) posits that motivation to reveal or withhold valued information via a given medium follows rules for "boundary opening" and "boundary closure" (Petronio, 1991). Boundary opening and closure are dynamic psychological processes of regulation conducted by individuals to assess the type and amount of information disclosure. Boundary opening is the state in which individuals become open to sending and receiving information, whereas boundary closure is the state in which individuals restrict information flow to and from others (Stanton & Stam, 2003). IBT considers the interrelations between the benefits and risks of information disclosure, while privacy calculus assesses benefits and risks independently (Karwatzki, et al., 2017a).

Karwatzki et al. (2017a) adopted IBT to investigate the factors that influence individuals' willingness to disclose information. Sutanto et al. (2013) adopted IBT and proposed a privacy-safe application prototype by retaining users' information locally on their smartphones while still providing them with the process and content gratifications derived from personalization. Xu et al. (2008) adopted IBT and developed an integrative model for privacy concern formation. They found that privacy concern is formed on the basis of an individual's disposition to value privacy or on the basis of situational cues that enable assessment of the consequences of information disclosure.

Cognitive Consistency Theory

The cognitive consistency theory (CCT) posits that individuals strive to maintain elements within a cognitive system that are internally consistent with one another. Balance theory is a CCT that asserts

that individuals prefer to maintain a balance and behave in ways that maximize the internal consistency of their cognitive system (Heider, 1946(. Individuals prefer agreement or consistency among cognitive elements that constitute the "system" so that a balanced state exists (Wakefield, 2013). As defined by Heider (1946), a balanced state exists if all parts of a unit have the same dynamic character (i.e., all are positive or negative) and if entities with different dynamic characters are segregated from each other. If no balanced state exists, either the dynamic characters change or the unit relations change through action or cognitive reorganization. If a change is not possible, a state of imbalance produces tension.

The congruity theory (Osgood & Tannenbaum, 1955) is a CCT that asserts that individuals strive to maintain consistency among their cognitions and tend to change cognitions to avoid incongruity and restore congruity among elements. Thus, congruity theory can predict the attitude change of individuals by the degree of congruity between the assertion of individuals and their frame of reference.

Wakefield (2013) adopted balance and congruity theories to investigate the role of affect (positive and negative) on online disclosure and found that positive affect had a significant influence on users' website trust and privacy beliefs, an influence that in turn facilitated information disclosure.

Protection Motivation Theory

Rogers (1975) originally proposed protection motivation theory. Boss et al. (2015) reviewed the use of protection motivation theory in information security studies. Protection motivation theory is a theoretical framework for understanding individuals' behavior in response to threats. This theory has become the leading theoretical framework adopted in information security research to encourage individuals to comply with security measures and procedures through persuasion (Boss et al., 2015). The *protection motivation* concept involves any threat for which there is an effective recommended response that can be carried out by the individual (Floyd et al., 2000). According to this theory, protection motivation for individuals is based on two concepts: threat appraisal and coping appraisal. Individual motivation toward protection is induced by perceived threats and the desire to avoid negative potential consequences. The central idea here is that a fear appeal triggers the threat appraisal process. During the threat appraisal process, individuals evaluate perceived threats and generate fears that induce protection motivation against the maladaptive rewards earned by not engaging in protection motivation (Boss et al., 2015). The former outweighs the latter. Threat appraisal compromises perceived threat vulnerability and maladaptive rewards. The coping appraisal process includes response efficacy, self-efficacy, and response costs. Individual response efficacy and self-efficacy must outweigh the costs of engaging in protection motivation. After evaluating threat and coping appraisals, individuals choose to behave adaptively or maladaptively. In adaptive behaviors, recommended responses are adopted to tackle threats and provide the required protection, while in maladaptive behaviors, recommended responses are avoided.

Herath and Rao (2009) adopted protection motivation theory and developed the integrated protection motivation and deterrence model of security policy compliance. Orszaghova and Blank (2024) adopted protection motivation theory and found that privacy protection behavior is divided into two types, security actions and preventive actions, each with different motivations. Security actions include basic protection measures, such as string passwords and the installation of security updates requiring no prior technological knowledge. Preventive actions require technological knowledge and a proactive approach to security, such as the installation of ad-blocking software and the proactive rejection of cookies.

Uses and Gratification Theory

Uses and gratification theory (UGT) focuses on studying "the gratifications that attract and hold audiences to the kinds of media and the types of content that satisfy their social and psychological needs" (Ruggiero, 2000). According to UGT, media affects individuals differently depending on how it fulfills the needs that motivate their behavior (Hossain et al., 2019). There is a distinction between gratification sought and gratification obtained: the former is related to an expectation and the latter

to what is actually received from media (Hossain et al., 2019). Additionally, there is a distinction between the gratification process and gratification content: the former is related to performing an activity and the latter to the content consumed (Urista et al., 2009). Sutanto et al. (2013) adopted gratification theory to investigate the trade-off between personalization, which makes individuals experience more gratification, and privacy concerns that result from individuals' sharing personal information to gain personalization. Hossain et al. (2019) found that three types of gratification—namely, hedonic gratification (enjoyment), utilitarian gratification (information seeking), and social gratification (social interaction)—have a significant impact on liking behavior among users of Facebook, which in turn influences continuous usage intentions. UGT has been adopted in various contexts to understand individuals' motivation and behavior, including use of the Internet (Song et al., 2004), online shopping (Lim & Ting, 2012), and continuous content contribution behaviors on microblogging (Liu et al., 2020). S. Ma et al. (2019) adopted UGT and found that perceived content quality, perceived social influence, and perceived entertainment have a significant impact on user satisfaction in a security education context through the use of social media in order to strengthen individuals' information security knowledge.

Prospect Theory

Kahneman and Tversky (1979) developed prospect theory (PT) to understand the process of decision making under risk. PT posits that individuals tend to be risk averse in the domain of gains and relatively risk seeking in the domain of losses (McDermott, 1998). According to Bahamonde and Canales (2022), PT is based on two concepts. First, utility is defined according to changes in outcomes with respect to a reference point; thus, changes relative to that point are perceived as either losses or gains. Second, individuals distort values of outcomes in an asymmetrical, nonlinear, S-shaped way when making risky decisions. Adjerid et al. (2018) adopted PT to investigate the impact of privacy protection on consumers' decisions to report privacy concerns and willingness to disclose personal information. Qu et al. (2019) adopted PT in a cybersecurity context to encourage better decisions regarding security recommendations designed to promote security compliance. They found that showing the disadvantages of security risk could help persuade users about security recommendations. Furthermore, they found that there is a preference to eliminate risk rather than reduce overall risk.

Social Exchange Theory

Social exchange theory (SET) posits that social interaction is a reciprocal process involving a series of sequential transactions between two or more parties and that the resources to be exchanged are either tangible or intangible (Cropanzano et al., 2017). Foa and Foa (1974, 1980) identified six types of resources that may be exchanged: love, status, information, money, goods, and services. The social exchange process is governed by "rules" (Cropanzano & Mitchell, 2005) and involves structures with varying degrees of power and influence (Cook et al., 2013). B. C. Choi et al. (2015) adopted SET to investigate individuals' responses to privacy invasion in the context of embarrassment regarding private information revealed on social media platforms. Individuals are motivated to exchange their personal information in return for perceived benefits. Cloarec et al. (2022) adopted SET to investigate personalization–privacy trade-offs in which individuals disclose and share personal information in exchange for personalized services. They found that Internet happiness is the strongest driver of willingness to disclose information in exchange for personalization. Additionally, they found that trust beliefs are positively related to a willingness to disclose information in exchange for personalization, while risk beliefs are not. K. Li et al. (2016) found that perceived benefit increases willingness to disclose information privacy on SNS.

CONCLUSION AND FUTURE RESEARCH

We identified and reviewed 20 theories in online information privacy research in the IS context to shed light on how and with which theories information privacy has been investigated. Theories are conceptualizations of real-world phenomena that help us understand social reality and enhance our world. As individuals' information becomes a valuable asset and commodity in the present age, an in-depth investigation of "information privacy" research is necessary to shed light on how we can contribute to this area of study. Individual personal privacy is an important issue. Hence, further investigation is essential for learning how we can protect individuals' information privacy along each link of the systems chain: technologies, policies, processes, people, society, economy, and legislature. The concept of privacy has become increasingly complex with the advancement and ubiquity of technology, which exposes individuals and their privacy to compromise. More advanced and interdisciplinary research is required to adopt and develop theories that fulfill privacy needs and requirements.

Y. Li (2012) reviewed 15 established theories to understand online information privacy. On the basis of their review, they developed a dual-calculus model in which individual decisions for information disclosure are the result of two interrelated tradeoffs: privacy calculus and risk calculus. Some theories in their research did not emerge in our systematic study, which reinforces the idea that privacy is a complex concept that is largely fragmented and discipline-dependent. Bélanger and Crossler (2011) reviewed privacy in the IS literature and found that the majority of studies on information privacy have focused on explaining and predicting theoretical contributions, followed by those presenting analytical theories, and few studies have presented design and action theories. On the basis of their review, they developed a multilevel conceptual framework to provide a comprehensive view of privacy at the individual, group, societal, organizational, and government levels. Smith et al. (2011) conducted an interdisciplinary review of privacy, developing the antecedents–privacy concerns–outcomes model, in which the relationships between privacy and other constructs are classified. Lowry et al. (2017) reviewed the literature in the IS context and identified privacy artifacts, including ethics, information, legal, organizational, person, process, protection, social, technology, threats, and vulnerability. Privacy issues that have been investigated in ubiquitous technology include mobile networking (Kommineni & Prasad, 2024), artificial intelligence-driven healthcare systems (Williamson & Prybutok, 2024), and EHR (Tertulino et al., 2024), data from the IoT (Pinto et al., 2024), privacy in the Metaverse (Huang et al., 2023), unpiloted aerial vehicles (Hadi et al., 2023), and deep and machine learning (Boulemtafes et al., 2020). However, further research is required to synthesize fragmented privacy studies and develop a comprehensive information privacy framework that fits the present era of ubiquitous technology and fulfills individual privacy needs. Information privacy is a globally challenging issue that spans various disciplines, and it is defined and conceptualized in the literature in different ways, thus requiring collaboration and an interdisciplinary research approach to consolidate the diversity of perspectives.

Implications and Recommendations

We investigated the extant literature to gauge current research and the identified theories used to understand and explain information privacy. Information privacy is a growing concern in the present age, which is characterized by technologies that are woven into everyday life and are becoming indispensable. Technical revolutions in data collection, storage, and processing include social media, personalization, big data, artificial intelligence, and the IoT. Thus, more research is needed to identify approaches and measures to protect individuals' personal data and enact laws that are compatible with emerging technologies. By identifying the theories adopted in the privacy literature, we contribute to synthesizing the current theories adopted in privacy research. Thus, future research can build on these to develop new theories and enrich our insight and understanding of individual privacy. Moreover, promising theories from other disciplines should be identified and

adopted in future research for contextualization and application to information privacy and to extend our identified list of theories. Other theories can provide deeper insights from different perspectives, thereby enhancing our understanding of information privacy issues.

Limitations

This study is limited to established theories published in the eight journals from the AIS that have been empirically adopted in the literature. Thus, we may have overlooked other valuable references outside the scope of the identified literature. Many established theories have been adopted to investigate information privacy in journals outside the scope of this study (Y. Li, 2012). Thus, the scope of this study excludes relevant theories in IS literature and other disciplines, potentially restricting the diversity of perspectives on online information privacy.

DECLARATION OF INTEREST

The author reports that there are no competing interests to declare.

FUNDING STATEMENT

No funding was received for this work.

PROCESS DATES

07, 2024

This manuscript was initially received for consideration for the journal on 05/11/2024, revisions were received for the manuscript following the double-anonymized peer review on 06/24/2024, the manuscript was formally accepted on 06/23/2024, and the manuscript was finalized for publication on 07/08/2024

CORRESPONDING AUTHOR

Correspondence should be addressed to Alanawd Alshehri; a_alshehri@ut.edu.sa

REFERENCES

Adjerid, I., Peer, E., & Acquisti, A. (2018). Beyond the privacy paradox: Objective versus relative risk in privacy decision making. *Management Information Systems Quarterly*, *42*(2), 465–488. 10.25300/MISQ/2018/14316

Agnew, R. (1992). Foundation for a general strain theory of crime and delinquency. *Criminology*, *30*(1), 47–88. 10.1111/j.1745-9125.1992.tb01093.x

Agnew, R. (2006). *Pressured into crime: An overview of general strain theory*. Roxbury Publishing.

Agnew, R., & Scheuerman, H. (2010). Strain theories. In McLaughlin, E., & Newburn, T. (Eds.), *The Sage handbook of criminological theory* (pp. 196–113). Sage. 10.4135/9781446200926.n6

Bahamonde, H., & Canales, A. (2022, December). Electoral risk and vote buying, introducing prospect theory to the experimental study of clientelism. *Electoral Studies*, *80*, 102497. 10.1016/j.electstud.2022.102497

Bandura, A. (1986). *Social foundations of thought and action*. Prentice Hall.

Bandura, A. (1991). Social cognitive theory of self-regulation. *Organizational Behavior and Human Decision Processes*, *50*(2), 248–287. 10.1016/0749-5978(91)90022-L

Bansal, G., Zahedi, F. M., & Gefen, D. (2015, February 17). The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern. *European Journal of Information Systems*, *24*(6), 624–644. 10.1057/ejis.2014.41

Becker, M. (2019). Privacy in the digital age: Comparing and contrasting individual versus social approaches towards privacy. *Ethics and Information Technology*, *21*(4), 307–317. 10.1007/s10676-019-09508-z

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *Management Information Systems Quarterly*, *35*(4), 1017–1041. 10.2307/41409971

Boss, S. R., Galletta, D., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do users have to fear? Using fear appeals to engender threats and fear that motivate protective behaviors in users. *Management Information Systems Quarterly*, *39*(4), 837–864. 10.25300/MISQ/2015/39.4.5

Boulemtafes, A., Derhab, A., & Challal, Y. (2020). A review of privacy-preserving techniques for deep learning. *Neurocomputing*, *384*(7), 21–45. 10.1016/j.neucom.2019.11.041

Broidy, L., & Agnew, R. (1997). Gender and crime: A general strain theory perspective. *Journal of Research in Crime and Delinquency*, *34*(3), 275–306. 10.1177/0022427897034003001

Burt, R. S. (1992). *Structural holes: The social structure of competition*. Harvard University Press. 10.4159/9780674029095

Burt, R. S. (2002). The social capital of structural holes. In M. F. Guillèn, R. Collins, P. England, & M. Meyer (Eds.), *The New Economic Sociology: Developments in an Emerging Field*. Russell Sage Foundation.

Burt, R. S. (2004). Structural holes and good ideas. *American Journal of Sociology*, *110*(2), 349–399. 10.1086/421787

Cheng, X., Su, L., Luo, X., Benitez, J., & Cai, S. (2022). The good, the bad, and the ugly: Impact of analytics and artificial intelligence-enabled personal information collection on privacy and participation in ridesharing. *European Journal of Information Systems*, *31*(3), 339–363. 10.1080/0960085X.2020.1869508

Choi, B., Wu, Y., Yu, J., & Land, L. P. W. (2018). Love at first sight: The interplay between privacy dispositions and privacy calculus in online social connectivity management. *Journal of the Association for Information Systems*, *19*(3), 124–151. 10.17705/1jais.00487

Choi, B. C., Jiang, Z., Xiao, B., & Kim, S. S. (2015). Embarrassing exposures in online social networks: An integrated perspective of privacy invasion and relationship bonding. *Information Systems Research*, *26*(4), 675–694. 10.1287/isre.2015.0602

Choi, B. C. F., Kim, S. S., & Jiang, Z. (2016). Influence of firm's recovery endeavors upon privacy breach on online customer behavior. *Journal of Management Information Systems*, *33*(3), 904–933. 10.1080/07421222.2015.1138375

Choi, H. S., Oh, W., Kwak, C., Lee, J., & Lee, H. (2022). Effects of online crowds on self-disclosure behaviors in online reviews: A multidimensional examination. *Journal of Management Information Systems*, *39*(1), 218–246. 10.1080/07421222.2021.2023412

Claridge, T. (2018). Dimensions of social capital—Structural, cognitive, and relational. *Social Capital Research*, *1*, 1–4.

Cloarec, J., Meyer-Waarden, L., & Munzel, A. (2022). The personalization–privacy paradox at the nexus of social exchange and construal level theories. *Psychology and Marketing*, *39*(3), 647–661. 10.1002/mar.21587

Coleman, J. S. (1990). *Foundations of social theory*. Harvard University Press.

Cook, K. S., Cheshire, C., Rice, E. R., & Nakagawa, S. (2013). Social exchange theory. In DeLamater, J., & Ward, A. (Eds.), *Handbook of Social Psychology* (pp. 61–88). Springer. 10.1007/978-94-007-6772-0_3

Cropanzano, R., Anthony, E. L., Daniels, S. R., & Hall, A. V. (2017). Social exchange theory: A critical review with theoretical remedies. *The Academy of Management Annals*, *11*(1), 479–516. 10.5465/annals.2015.0099

Cropanzano, R., & Mitchell, M. S. (2005). Social exchange theory: An interdisciplinary review. *Journal of Management*, *31*(6), 874–900. 10.1177/0149206305279602

De Busser, E. (2017). Big data: The conflict between protecting privacy and securing nations. In Atlantic Council & Thompson Reuters (Eds.), *Big Data: A twenty-first century arms race*. https://www.atlanticcouncil.org/wp-content/uploads/2017/06/Big_Data_A_Twenty-First_Century_Arms_Race_web_0627_Chapter_1.pdf

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. 10.1057/ejis.2012.23

Engeström, Y. (2001). Expansive learning at work: Toward an activity theoretical reconceptualization. *Journal of Education and Work*, *14*(1), 133–156. 10.1080/13639080020028747

Farayola, O. A., Olorunfemi, O. L., & Shoetan, P. O.Oluwatoyin Ajoke FayayolaOluwabukunmi Latifat OlorunfemiPhilip Olaseni Shoetan. (2024). Data privacy and security in IT: A review of techniques and challenges. *Computer Science & IT Research Journal*, *5*(3), 606–615. 10.51594/csitrj.v5i3.909

Fiske, S. T., & Neuberg, S. L. (1990). A continuum of impression formation, from category-based to individuating processes: Influences of information and motivation on attention and interpretation. In *Vol. 23*, pp. 1–74). Advances in experimental social psychology. Academic Press. 10.1016/S0065-2601(08)60317-2

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology*, *30*(2), 407–429. 10.1111/j.1559-1816.2000.tb02323.x

Foa, U. G., & Foa, E. B. (1974). *Societal structures of the mind*. Charles C Thomas.

Foa, U. G., & Foa, E. B. (1980). Resource theory: Interpersonal behavior as exchange. In Gergen, K. J., Greenberg, M. S., & Willis, R. H. (Eds.), *Social exchange: Advances in theory and research*. Plenum. 10.1007/978-1-4613-3087-5_4

Greenaway, K. E., Chan, Y. E., & Crossler, R. E. (2015). Company information privacy orientation: A conceptual framework. *Information Systems Journal*, *25*(6), 579–606. 10.1111/isj.12080

Hadi, H. J., Cao, Y., Nisa, K. U., Jamil, A. M., & Ni, Q. (2023, April). A comprehensive survey on security, privacy issues and emerging defence technologies for UAVs. *Journal of Network and Computer Applications*, *213*, 103607. 10.1016/j.jnca.2023.103607

Hashim, N. H., & Jones, M. L. (2007). *Activity theory: A framework for qualitative analysis*. University of Wollongong, Research Online. Retrieved July 2, 2024, from https://ro.uow.edu.au/commpapers/408/

Heider, R. (1946). Attitudes and cognitive organization. *The Journal of Psychology*, *21*(1), 107–112. 10.1080/00223980.1946.991727521010780

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106–125. 10.1057/ejis.2009.6

Hoehle, H., Aloysius, J. A., Goodarzi, S., & Venkatesh, V. (2019). A nomological network of customers' privacy perceptions: Linking artifact design to shopping efficiency. *European Journal of Information Systems*, *28*(1), 91–113. 10.1080/0960085X.2018.1496882

Hong, W., & Thong, J. Y. L. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. *Management Information Systems Quarterly*, *37*(1), 275–298. 10.25300/MISQ/2013/37.1.12

Hossain, M., Kim, M., & Jahan, N. (2019). Can "liking" behavior lead to usage intention on Facebook? Uses and gratification theory perspective. *Sustainability (Basel)*, *11*(4), 1166. 10.3390/su11041166

Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM*, *54*(6), 54–60. 10.1145/1953122.1953142

Huang, Y., Li, Y. J., & Cai, Z. (2023). Security and privacy in metaverse: A comprehensive survey. *Big Data Mining and Analytics*, *6*(2), 234–247. 10.26599/BDMA.2022.9020047

Introna, L. D. (2000). Workplace surveillance, privacy and distributive justice. *Computers & Society*, *30*(4), 33–39. 10.1145/572260.572267

Jang, S. J., & Agnew, R. (2015). Strain theories and crime. In Wright, J. D. (Ed.), *International Encyclopedia of the Social & Behavioral Sciences* (2nd ed., *Vol. 23*, pp. 495–500). Elsevier. 10.1016/B978-0-08-097086-8.45088-9

Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica*, *47*(2), 263–291. 10.2307/1914185

Kaptelinin, V., & Nardi, B. (2012). *Activity theory in HCI: Fundamentals and reflections*. Morgan & Claypool Publishers. 10.1007/978-3-031-02196-1

Karwatzki, S., Dytynko, O., Trenz, M., & Veit, D. (2017a). Beyond the personalization–privacy paradox: Privacy valuation, transparency features, and service personalization. *Journal of Management Information Systems*, *34*(2), 369–400. 10.1080/07421222.2017.1334467

Karwatzki, S., Trenz, M., Tuunainen, V. K., & Veit, D. (2017b). Adverse consequences of access to individuals' information: An analysis of perceptions and the scope of organisational influence. *European Journal of Information Systems*, *32*(2), 688–715. 10.1057/s41303-017-0064-z

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal*, *25*(6), 607–635. 10.1111/isj.12062

Keith, M. J., Babb, J. S., Lowry, P. B., Furner, C. P., & Abdullat, A. (2015). The role of mobile-computing self-efficacy in consumer information disclosure. *Information Systems Journal*, *25*(6), 637–667. 10.1111/isj.12082

Kim, Y., & Cannella, A. A.Jr. (2008). Toward a social capital theory of director selection. *Corporate Governance*, *16*(4), 282–293. 10.1111/j.1467-8683.2008.00693.x

Kitchen, P. J., Kerr, G., Schultz, D. E., McColl, R., & Pals, H. (2014). The elaboration likelihood model: Review, critique and research agenda. *European Journal of Marketing*, *48*(11/12), 2033–2050. 10.1108/EJM-12-2011-0776

Kommineni, K. K., & Prasad, A. (2024). A review on privacy and security improvement mechanisms in MANETs. *International Journal of Intelligent Systems and Applications in Engineering*, *12*(2), 90–99.

Kordzadeh, N., & Warren, J. (2017). Communicating personal health information in virtual health communities: An integration of privacy calculus model and affective commitment. *Journal of the Association for Information Systems*, *18*(1), 45–81. 10.17705/1jais.00446

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *The Journal of Social Issues*, *33*(3), 22–42. 10.1111/j.1540-4560.1977.tb01880.x

Lee, J. K., Cho, D., & Lim, G. G. (2018). Design and validation of the bright internet. *Journal of the Association for Information Systems*, *19*(2), 63–85. 10.17705/jais1.00484

Lembcke, T. B., Masuch, K., Trang, S. T. N., Hengstler, S., Plics, P., & Pamuk, M. (2019, August). *Fostering information security compliance: Comparing the predictive power of social learning theory and deterrence theory* [conference presentation]. Americas Conference on Information Systems (AMCIS), Cancun, Mexico.

Ki, Wang, X., Li, K., & Che, J. (2016). Information privacy disclosure on social network sites: An empirical investigation from social exchange perspective. *Nankai Business Review International*, *7*(3), 282–300. 10.1108/NBRI-02-2015-0005

Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems*, *54*(1), 471–481. 10.1016/j.dss.2012.06.010

Li, Y., Yang, K., Chen, J., Gupta, S., & Ning, F. (2019). Can an apology change after-crisis user attitude? The role of social media in online crisis management. *Information Technology & People*, *32*(4), 802–827. 10.1108/ITP-03-2017-0103

Lim, W. M., & Ting, D. H. (2012). E-shopping: An analysis of the uses and gratifications theory. *Modern Applied Science*, *6*(5), 48. 10.5539/mas.v6n5p48

Lin, J., Carter, L., & Liu, D. (2021). Privacy concerns and digital government: Exploring citizen willingness to adopt the COVIDSafe app. *European Journal of Information Systems*, *30*(4), 389–402. 10.1080/0960085X.2021.1920857

Lin, S., & Armstrong, D. (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. 10.17705/1jais.00540

Lin, X., Featherman, M., & Sarker, S. (2013). *Information sharing in the context of social media: An application of the theory of reasoned action and social capital theory*. Special Interest Group on Human-Computer Interaction SIGHCI 2013 Proceedings, 17. AIS Electronic Library. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1009&context=sighci2013

Lin, Z., Zhang, Y., Gong, Q., Chen, Y., Oksanen, A., & Ding, A. Y. (2022). Structural hole theory in social network analysis: A review. *IEEE Transactions on Computational Social Systems*, *9*(3), 724–739. 10.1109/TCSS.2021.3070321

Liu, X., Min, Q., & Han, S. (2020). Understanding users' continuous content contribution behaviours on microblogs: An integrated perspective of uses and gratification theory and social influence theory. *Behaviour & Information Technology*, *39*(5), 525–543. 10.1080/0144929X.2019.1603326

Lowry, P. B., Dinev, T., & Willison, R. (2017). Why security and privacy research lies at the centre of the information systems (IS) artefact: Proposing a bold research agenda. *European Journal of Information Systems*, *26*(6), 546–563. 10.1057/s41303-017-0066-x

Ma, L., Ding, X., Zhang, X., & Zhang, G. (2020). Mobile users' self-disclosure behaviour on WeChat: Application of social cognitive theory. *Mobile Information Systems*, *2020*, 1–13. Advance online publication. 10.1155/2020/8903247

Ma, S., Zhang, S., Li, G., & Wu, Y. (2019). Exploring information security education on social media use: Perspective of uses and gratifications theory. *Aslib Journal of Information Management*, *71*(5), 618–636. 10.1108/AJIM-09-2018-0213

McDermott, R. (1998). *Risk-taking in international politics: Prospect theory in American foreign policy*. University of Michigan Press. 10.3998/mpub.15779

Meier, Y., & Krämer, N. C. (2024). The privacy calculus revisited: An empirical investigation of online privacy decisions on between-and within-person levels. *Communication Research*, *51*(2), 178–202. 10.1177/00936502221102101

Merton, R. K. (1938). Social structure and anomie. *American Sociological Review*, *3*(5), 672–682. 10.2307/2084686

Metzger, M. J. (2007). Communication privacy management in electronic commerce. *Journal of Computer-Mediated Communication*, *12*(2), 335–361. 10.1111/j.1083-6101.2007.00328.x

Miltgen, C. L., & Peyrat-Guillard, D. (2014). Cultural and generational influences on privacy concerns: A qualitative study in seven European countries. *European Journal of Information Systems*, *23*(2), 103–125. 10.1057/ejis.2013.17

Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. G.PRISMA Group. (2010). Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *International Journal of Surgery*, *8*(5), 336–341. 10.1016/j.ijsu.2010.02.00720171303

Orszaghova, E., & Blank, G. (2024, April 17). Does the type of privacy-protective behaviour matter? An analysis of online privacy protective action and motivation. *Information Communication and Society*, 1–18. Advance online publication. 10.1080/1369118X.2024.2334906

Osch, W. V., Bulgurcu, B., & Liang, Y. (2023). Living in a fishbowl or not: The role of transparency and privacy in creative dialogues on enterprise social media. *Journal of the Association for Information Systems*, *24*(3), 846–881. 10.17705/1jais.00802

Osgood, C., & Tannenbaum, P. (1955). The principle of congruity in the prediction of attitude change. *Psychological Review*, *62*(1), 42–55. 10.1037/h004815314357526

Ozdemir, Z. D., Smith, H. J., & Benamati, J. H. (2017). Antecedents and outcomes of information privacy concerns in a peer context: An exploratory study. *European Journal of Information Systems*, *26*(6), 642–660. 10.1057/s41303-017-0056-z

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., & Moher, D. (2021, March 29). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ (Clinical Research Ed.)*, *372*(71), n71. Advance online publication. 10.1136/bmj.n7133782057

Parks, R. F., Wigand, R. T., & Lowry, B. P. (2023). Balancing information privacy and operational utility in healthcare: Proposing a privacy impact assessment (PIA) framework. *European Journal of Information Systems*, *32*(6), 1052–1069. 10.1080/0960085X.2022.2103044

Peras, D., & Mekovec, R. (2022). A conceptualization of the privacy concerns of cloud users. *Information and Computer Security*, *30*(5), 653–671. 10.1108/ICS-11-2021-0182

Petronio, S. (1991). Communication boundary management: A theoretical model of managing disclosure of private information between marital couples. *Communication Theory*, *1*(4), 311–335. 10.1111/j.1468-2885.1991.tb00023.x

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. State University of New York Press. 10.1353/book4588

Petronio, S., & Child, J. T. (2020, February). Conceptualization and operationalization: Utility of communication privacy management theory. *Current Opinion in Psychology*, *31*, 76–82. 10.1016/j.copsyc.2019.08.00931526974

Petty, R. E., & Cacioppo, J. T. (1986). *Communication and persuasion: Central and peripheral routes to attitude change*. Springer-Verlag. 10.1007/978-1-4612-4964-1

Pinto, G. P., Donta, P. K., Dustdar, S., & Prazeres, C. (2024). A systematic review on privacy-aware IoT personal data stores. *Sensors (Basel)*, *24*(7), 2197. 10.3390/s2407219738610408

Posey, C., Raja, U., Crossler, R. E., & Burns, A. J. (2017). Taking stock of organisations' protection of privacy: Categorising and assessing threats to personally identifiable information in the USA. *European Journal of Information Systems*, *26*(6), 585–604. 10.1057/s41303-017-0065-y

Putnam, R. (1993, April 1). The prosperous community: Social capital and public life. *The American Prospect*, *13*, 35–42.

Qin, Y., Cho, H., Li, P., & Zhang, L. (2021, June 17). First impression formation based on valenced self-disclosure in social media profiles. *Frontiers in Psychology*, *12*, 656365. 10.3389/fpsyg.2021.65636534220626

Qu, L., Wang, C., Xiao, R., Hou, J., Shi, W., & Liang, B. (2019, May). Towards better security decisions: Applying prospect theory to cybersecurity. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems* (pp. 1–6). Association for Computing Machinery.

Rana, N. P., & Dwivedi, Y. K. (2015). Citizen's adoption of an e-government system: Validating extended social cognitive theory (SCT). *Government Information Quarterly*, *32*(2), 172–181. 10.1016/j.giq.2015.02.002

Rashidi, Y., Kapadia, A., Nippert-Eng, C., & Su, N. M. (2020). "It's easier than causing confrontation": Sanctioning strategies to maintain social norms and privacy on social media. *Proceedings of the ACM on Human-Computer Interaction, 4*(CSCW1), 1–25.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, *91*(1), 93–114. 10.1080/00223980.1975.991580328136248

Romansky, R. P., & Noninska, I. S. (2020). Challenges of the digital age for privacy and personal data protection. *Mathematical Biosciences and Engineering*, *17*(5), 5288–5303. 10.3934/mbe.202028633120553

Ruggiero, T. E. (2000). Uses and gratifications theory in the 21st century. *Mass Communication & Society*, *3*(1), 3–37. 10.1207/S15327825MCS0301_02

Schunk, D. H., & Usher, E. L. (2012). Social cognitive theory and motivation. In Ryan, R. M. (Ed.), *The Oxford Handbook of Human Motivation* (pp. 10–26). Academic. 10.1093/oxfordhb/9780195399820.013.0002

Siponen, M., Soliman, W., & Vance, A. (2022). Common misunderstandings of deterrence theory in information systems research and future research directions. *The Data Base for Advances in Information Systems*, *53*(1), 25–60. 10.1145/3514097.3514101

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *Management Information Systems Quarterly*, *35*(4), 989–1015. 10.2307/41409970

Song, I., Larose, R., Eastin, M. S., & Lin, C. A. (2004). Internet gratifications and Internet addiction: On the uses and abuses of new media. *Cyberpsychology & Behavior*, *7*(4), 384–394. 10.1089/cpb.2004.7.38415331025

Spottswood, E. L., & Hancock, J. T. (2017). Should I share that? Prompting social norms that influence privacy behaviors on a social networking site. *Journal of Computer-Mediated Communication*, *22*(2), 55–70. 10.1111/jcc4.12182

Stanton, J. M., & Stam, K. R. (2003). Information technology, privacy, and power within organizations: A view from boundary theory and social exchange perspectives. *Surveillance & Society*, *1*(2), 152–190. 10.24908/ss.v1i2.3351

Stuart, A., Bandara, A. K., & Levine, M. (2019). The psychology of privacy in the digital age. *Social and Personality Psychology Compass*, *13*(11), e12507. 10.1111/spc3.12507

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. *Management Information Systems Quarterly*, *37*(4), 1141–1164. 10.25300/MISQ/2013/37.4.07

Tertulino, R., Antunes, N., & Morais, H. (2024). Privacy in electronic health records: A systematic mapping study. *Journal of Public Health (Berlin)*, *32*(3), 435–454. 10.1007/s10389-022-01795-z

Teubner, T., & Flath, C. M. (2019). Privacy in the sharing economy. *Journal of the Association for Information Systems*, *20*(3), 213–242. 10.17705/1jais.00534

Urista, M. A., Dong, Q., & Day, K. D. (2009). Explaining why young adults use MySpace and Facebook through uses and gratifications theory. *Human Communication*, *12*(2), 215–229.

Valecha, R., Upadhyaya, S., & Rao, H. R. (2021). An activity theory approach to leak detection and mitigation in patient health information (PHI). *Journal of the Association for Information Systems*, *22*(4), 1007–1036. 10.17705/1jais.00687

Verenikina, I. (2001). Cultural-historical psychology and activity theory in everyday practice. In H. Hasan, E. Gould, P. Larkin, & L. Vrazalic (Eds.), *Information systems and activity theory: Volume 2, Theory and practice* (pp. 23–38). University of Wollongong Press.

Wakefield, R. (2013). The influence of user affect in online information disclosure. *The Journal of Strategic Information Systems*, *22*(2), 157–174. 10.1016/j.jsis.2013.01.003

Wall, J. D., Lowry, P. B., & Barlow, J. B. (2016). Organizational violations of externally governed privacy and security rules: Explaining and predicting selective violations under conditions of strain and excess. *Journal of the Association for Information Systems*, *17*(1), 39–76. 10.17705/1jais.00420

Wang, L., Hu, H.-H., Yan, J., & Mei, M. Q. (2020). Privacy calculus or heuristic cues? The dual process of privacy decision making on Chinese social media. *Journal of Enterprise Information Management*, *33*(2), 353–380. 10.1108/JEIM-05-2019-0121

Williamson, S. M., & Prybutok, V. (2024). Balancing privacy and progress: A review of privacy challenges, systemic oversight, and patient perceptions in AI-driven healthcare. *Applied Sciences (Basel, Switzerland)*, *14*(2), 675. 10.3390/app14020675

Willison, R., Lowry, P. B., & Paternoster, R. (2018). A tale of two deterrents: Considering the role of absolute and restrictive deterrence to inspire new directions in behavioral and organizational security research. *Journal of the Association for Information Systems*, *19*(12), 1187–1216. 10.17705/1jais.00524

Wu, C., & Li, W. (2019). Why do consumers boycott personalization marketing? A perspective from multidimensional development theory and psychological contract violation. In D. Xu, J. Jiang, & H.-W. Kim (Eds.), *Pacific Asia Conference on Information Systems PACIS 2019 Proceedings* (200). AIS eLibrary. https://aisel.aisnet.org/pacis2019/200

Wu, D., Gu, H., Gu, S., & You, H. (2021). Individual motivation and social influence: A study of telemedicine adoption in China based on social cognitive theory. *Health Policy and Technology*, *10*(3), 100525. 10.1016/j.hlpt.2021.100525

Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). Examining the formation of individual's privacy concerns: Toward an integrative view. In *International Conference on Information Systems (ICIS) 2008 Proceedings.* https://aisel.aisnet.org/icis2008/6/

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. 10.17705/1jais.00281

Xu, H., Teo, H. H., Tan, B. C. Y., & Agarwal, R. (2009). The role of push-pull technology in privacy calculus: The case of location-based services. *Journal of Management Information Systems*, *26*(3), 135–174. 10.2753/MIS0742-1222260305

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. 10.17705/1jais.00557

Zarsky, T. Z. (2019). Privacy and manipulation in the digital age. *Theoretical Inquiries in Law*, *20*(1), 157–188. 10.1515/til-2019-0006

Zhou, T. (2017). Understanding location-based services users' privacy concern: An elaboration likelihood model perspective. *Internet Research*, *27*(3), 506–519. 10.1108/IntR-04-2016-0088