

Context-Contingent Privacy Concerns and Exploration of the Privacy Paradox in the Age of AI, AR, Big Data, and the IoT: Systematic Review

Christian Herriger, Omar Merlo, Andreas Eisingerich, Annisa Arigayota

Submitted to: Journal of Medical Internet Research
on: January 30, 2025

Disclaimer: © The authors. All rights reserved. This is a privileged document currently under peer-review/community review. Authors have provided JMIR Publications with an exclusive license to publish this preprint on its website for review purposes only. While the final peer-reviewed paper may be licensed under a CC BY license on publication, at this stage authors and publisher expressly prohibit redistribution of this draft paper other than for review purposes.

Table of Contents

Original Manuscript..... 5

Supplementary Files..... 45

0..... 45

Multimedia Appendixes 46

Multimedia Appendix 0..... 46

Context-Contingent Privacy Concerns and Exploration of the Privacy Paradox in the Age of AI, AR, Big Data, and the IoT: Systematic Review

Christian Herriger¹; Omar Merlo¹; Andreas Eisingerich¹; Annisa Arigayota¹

¹ Imperial College London London GB

Corresponding Author:

Omar Merlo

Imperial College London
Imperial College Business School
London
GB

Abstract

Background: Despite extensive research into technology users' privacy concerns, a critical gap remains in understanding why individuals adopt varying standards for data protection across different contexts. The emergence of advanced technologies such as the Internet of Things (IoT), artificial intelligence (AI), augmented reality (AR), and Big Data has created rapidly evolving and complex privacy landscapes. However, privacy is frequently treated as a static construct, failing to capture the fluid and context-dependent nature of user concerns. This oversimplification has led to fragmented research, inconsistent findings, and a limited ability to address the nuanced challenges posed by these technologies. Understanding these dynamics is particularly crucial in fields such as digital health and informatics, where sensitive data and user trust are central to technology adoption and ethical innovation.

Objective: This study synthesizes existing research on privacy behaviors in emerging technologies, focusing on IoT, AI, AR, and Big Data. The primary objectives are to (1) identify the psychological antecedents, outcomes, and theoretical frameworks that explain privacy behavior, (2) assess whether traditional online privacy literature—such as studies on e-commerce and social networking—applies to these advanced technologies, and (3) advocate for a context-dependent approach to understanding privacy concerns.

Methods: A systematic literature review was conducted following PRISMA 2020 guidelines. Searches were performed across three electronic databases (ScienceDirect, SAGE, and EBSCO) to identify empirical studies related to privacy behaviors in emerging technologies. A total of 521 studies were initially retrieved, of which 179 met the inclusion criteria after screening and eligibility assessment. Studies were included if they (1) examined privacy behaviors within IoT, AI, AR, or Big Data contexts, (2) were empirical, peer-reviewed research, and (3) were published in English. Non-empirical papers, review articles, and studies focusing solely on privacy-enhancing technologies were excluded. Data extraction focused on psychological antecedents, privacy outcomes, and theoretical frameworks. Risk of bias was minimized through predefined inclusion criteria and independent screening by two reviewers. Data synthesis was performed using a narrative approach.

Results: Findings indicate that contextual dimensions—including data sensitivity, recipient transparency, and transmission principles—are often overlooked despite their significant influence on privacy concerns. Of the 179 included studies, 54.2% explicitly analyzed information sensitivity, yet only 28.4% considered transmission principles. Furthermore, traditional privacy theories, developed for earlier technologies such as e-commerce and social media, frequently fail to address the complexities of modern, context-contingent privacy concerns. Results suggest that privacy behaviors in AI, IoT, AR, and Big Data settings deviate from established models, necessitating updated frameworks that better capture context-dependent dynamics.

Conclusions: This study advances the understanding of user privacy by emphasizing the critical role of contextual factors in data-sharing scenarios. Findings challenge static interpretations of privacy and highlight the necessity of frameworks that address dynamic, context-dependent behaviors. Limitations include potential selection bias and the heterogeneous methodologies of included studies. Practical implications include guiding healthcare providers, policymakers, and technology developers toward privacy strategies that build trust, enhance data protection, and support the ethical development of digital health practices.

(JMIR Preprints 30/01/2025:71951)

DOI: <https://doi.org/10.2196/preprints.71951>

Preprint Settings

1) Would you like to publish your submitted manuscript as preprint?

✓ **Please make my preprint PDF available to anyone at any time (recommended).**

Please make my preprint PDF available only to logged-in users; I understand that my title and abstract will remain visible to all users.

Only make the preprint title and abstract visible.

No, I do not wish to publish my submitted manuscript as a preprint.

2) If accepted for publication in a JMIR journal, would you like the PDF to be visible to the public?

✓ **Yes, please make my accepted manuscript PDF available to anyone at any time (Recommended).**

Yes, but please make my accepted manuscript PDF available only to logged-in users; I understand that the title and abstract will remain visible to all users.

Yes, but only make the title and abstract visible (see Important note, above). I understand that if I later pay to participate in a JMIR publication, my title and abstract will remain visible to all users.

No. Please do not make my accepted manuscript PDF available to anyone.

Original Manuscript

Context-Contingent Privacy Concerns and Exploration of the Privacy Paradox in the Age of AI, AR, Big Data, and the IoT: Systematic Review

Abstract

Background: Despite extensive research into technology users' privacy concerns, a critical gap remains in understanding why individuals adopt different standards for data protection across contexts. The rise of advanced technologies such as the Internet of Things (IoT), artificial intelligence (AI), augmented reality (AR), and Big Data has created rapidly evolving and complex privacy landscapes. Yet privacy is often treated as a static construct, failing to reflect the fluid, context-dependent nature of user concerns. This oversimplification has led to fragmented research, inconsistent findings, and limited capacity to address the nuanced challenges posed by these technologies. Understanding these dynamics is especially crucial in fields like digital health and informatics, where sensitive data and user trust are central to adoption and ethical innovation.

Objective: This study synthesizes existing research on privacy behaviors in emerging technologies, focusing on IoT, AI, AR, and Big Data. Its primary objectives are to identify the psychological antecedents, outcomes, and theoretical frameworks explaining privacy behavior, and to assess whether insights from traditional online privacy literature—such as e-commerce and social networking—apply to these advanced technologies. It also advocates a context-dependent approach to understanding privacy.

Methods: A systematic review of 179 studies synthesized psychological antecedents, outcomes, and theoretical frameworks related to privacy behaviors in emerging technologies. Following established guidelines and using leading research databases, studies were screened for relevance to privacy behaviors, focus on emerging technologies, and empirical grounding. Methodological details were analyzed to assess the applicability of traditional privacy findings—e.g., from e-commerce and social networking—to today's advanced technologies.

Results: The systematic review reveals key gaps in the privacy literature on emerging technologies such as IoT, AI, AR, and Big Data. Contextual factors—like data sensitivity, recipient transparency, and transmission principles—are often overlooked, despite their critical role in shaping privacy concerns and behaviors. The findings also show that theories developed for traditional technologies often fall short in addressing the complexities of modern contexts. By synthesizing psychological antecedents, behavioral outcomes, and theoretical frameworks, this study underscores the need for a context-contingent approach to privacy research.

Conclusions: This study advances understanding of user privacy by emphasizing the critical role of

context in data-sharing, particularly amid ubiquitous and emerging health technologies. The findings challenge static views of privacy and highlight the need for tailored frameworks that reflect dynamic, context-dependent behaviors. Practical implications include guiding healthcare providers, policymakers, and technology developers toward context-sensitive strategies that build trust, enhance data protection, and support ethical digital health innovation.

Keywords: privacy paradox; systematic literature review; contextual integrity; artificial intelligence (AI); Internet of things (IoT); privacy concerns.

Introduction

The context in which data is collected is crucial to individuals, as they are more likely to feel concerned about their privacy when their conversations are recorded without their knowledge or consent [1]. Moreover, the latest technological advances, such as Big Data, Augmented Reality (AR), Artificial Intelligence (AI), and the Internet of Things (IoT), are changing the privacy context at an increasingly rapid pace [2–6]; i.e., devices like Alexa collect rich data by continuously monitoring, tracking, and analyzing user behavior, which has resulted in increased concerns about their pervasiveness and user privacy [7,8]. In the context of digital health technologies, inadequate privacy policies—such as unclear or inaccessible terms—have hindered user trust and adoption, as users question the transparency and commitment of developers to safeguarding their data [9]. Broader concerns about data privacy and trust, as highlighted by incidents such as Cambridge Analytica's exploitation of personal data and the NHS Royal Free Trust's data-sharing with DeepMind, underscore the critical need for stronger privacy governance frameworks [10].

In this study we focus on the privacy paradox [11,12]. More specifically, although scholars have theorized that users engage in a risk-benefit assessment to weigh the benefits of sharing their data against the potential risks [13,14], numerous questions remain about the privacy paradox. For example, why are users more concerned about privacy in some contexts than others? And in today's environment, where more and more cutting-edge technologies are available to users, are privacy concerns changing compared to before, when they had access to just a few connected technologies, such as e-commerce websites and social media platforms? In addition, research has tended to offer a fragmented view of this phenomenon, analyzing it from several different perspectives, which points to the need to bring together and synthesize a disparate body of literature.

We posit that user privacy should be studied as a context-dependent and fluid concept rooted in Nissenbaum's contextual integrity theory [15], because context is a critical variable in data disclosure scenarios [16–20]. Accordingly, the present study aims to make several important

contributions to the field of privacy research in cutting-edge technologies.

We conduct a systematic literature review that synthesizes the various contexts in which research on privacy behaviors in IoT, AI, AR, and Big Data has been undertaken. The purpose of the systematic literature review is to identify the psychological antecedents, outcomes, and theories that describe privacy behavior in these new scenarios. Critically, we explore whether the findings from this body of research on cutting-edge technologies differ from previous findings in the traditional online privacy literature, such as e-commerce and social networking sites. By doing so, the study makes a valuable contribution by providing insights into how technological advancements are changing the privacy landscape and whether established privacy theories are applicable in these new contexts.

In addition, we offer a more context-contingent lens of privacy that positions context as the key variable in understanding different user behaviors in privacy scenarios. This addresses a significant gap in the literature, as calls for the usage of such lens have so far been neglected [21,22]. The current study aims to bridge the gap towards a more context-contingent privacy discussion by examining 179 research studies and offering several theoretical contributions. The findings confirm that contextual factors have been largely overlooked in privacy research on cutting-edge technologies, with only a small number of studies explicitly defining items aligning with Nissenbaum's [15] five parameters of information flows. Our findings suggest that the perceived dichotomy between privacy concerns and behavioral intentions is not inherently paradoxical but instead reflects a lack of comprehensive understanding in a holistic and context-sensitive framework. Also, we find that past research findings in related domains (e.g., e-commerce) do undergo alterations when study designs are transferred into the context of contemporary cutting-edge technologies.

The study offers significant implications for businesses, regulators, policymakers, and researchers, underscoring the importance of adopting context-sensitive privacy practices and policies. By tailoring privacy measures to the specific contexts in which cutting-edge technologies such as IoT, AI, AR, and Big Data operate, stakeholders can better safeguard users' privacy while fostering trust and responsible technology adoption. These insights are also particularly relevant for healthcare and technology domains, where privacy concerns are critical to user acceptance and the ethical deployment of emerging innovations [23].

Background

The rise of the internet has amplified concerns about privacy in interactions with online services. Paradoxically, however, individuals often display minimal effort or intent to safeguard their

privacy [24]. Over the years, scholars have sought to explain this apparent disconnect between privacy attitudes and behaviors, employing various theoretical frameworks and conceptual approaches [14,22,25]. To date, however, a widely accepted explanation of such user behavior in online disclosure situations, or the privacy paradox, has not been formulated, despite systematic efforts [13].

Two key ideas have generated considerable interest in this field. First, prior work has argued that users perform a risk-benefit assessment before disclosing data [13,14]. In this privacy calculus, perceived benefits typically outweigh perceived risks, elucidating why individuals continue to disclose information despite concerns [26]. However, research has shown that the rationality of this calculus is frequently clouded or wholly abandoned. This is due to individuals limited mental processing ability, which is heavily influenced by cognitive biases, heuristics [27–30], habits [31,32], knowledge deficiency [30,33], or personality traits [34,35]. These factors may even contradict the rationalism of the privacy calculus theory as a whole [13,26,35,36].

In recent years, privacy researchers have attempted to clarify the relationship between privacy attitudes and behavior. However, the literature has produced ambiguous findings, prompting some scholars to shift their focus towards contextual explanations. One such approach suggests that privacy concerns should be contextualized by examining users' privacy concerns, corresponding antecedents, and disclosure behavior in specific information-sharing environments [37,38]. According to Nissenbaum's theory of contextual integrity [15], privacy should be evaluated based on whether the flow of information is appropriate in a given context [39]. When informational norms are breached, privacy is violated [40]. These norms are defined by five parameters, namely the type of information being shared (attribute), with which recipient (actor), regarding whose information (subject), using which device (sender) and under which specific condition (transmission principles) [39,40]. Incomplete or ambiguous observations are expected if any of these parameters are missing [40]. It could be argued that the contextualization of privacy also defines how risks and benefits are perceived in the privacy calculus and what heuristics and cognitive processes are evoked.

Since privacy behavior is a highly context-dependent phenomenon, ambiguous results in the privacy literature may be explained by the context in which users experience information-sharing situations [22,41–43]. Solove [21] takes this argument further, suggesting that the privacy paradox may not be a paradox after all because discrepancies between human behavior and attitudes do not necessarily contradict each other. Solove [21] argues that "behavior involves choices about risk in specific contexts" and "attitudes involve people's broader valuation of privacy, often across many contexts" (p. 50). Consequently, findings attempting to predict context-dependent behavior from

generalized privacy attitudes will often be ambiguous, since they fundamentally measure different things (i.e., general attitudes versus specific risks and benefits in a given situation).

Numerous studies have highlighted the significance of context in relation to privacy in information sharing [16–20,44]. Prior work has shown the importance of user engagement [45–47] and also noted the role of transparency and open sharing of information with users [48–55]. However, despite calls within the literature to investigate the role of context in privacy in a comprehensive and theory-grounded manner [37,42,56,57], such research has largely been ignored (see Yun et al. [24] for a notable exception). Developing an understanding of the phenomenon that incorporates context as a critical driver of privacy concerns is essential for researchers, policymakers, and practitioners. This approach not only helps achieve more broadly applicable and less ambiguous results in privacy research but also ensures that future research, policymaking, and product design decisions are more user-centric and ethically grounded [37]. For fields like healthcare and digital health technologies, where privacy is a cornerstone of trust and adoption, a context-sensitive perspective is particularly crucial. By addressing privacy concerns within specific contexts, stakeholders can better design interventions, policies, and technologies that promote secure and responsible use while enhancing user engagement and compliance.

To improve our understanding of context-contingent privacy concerns it is useful to synthesize existing research to identify overarching patterns [37]. While there have been several review studies and one meta-study on the topic [11,13,14,22,24,58–60], to our knowledge, no research has yet attempted to synthesize recent findings through a contextual lens. This study aims to fill this gap by drawing on Nissenbaum's theory of contextual integrity [15]. Additionally, context and associated challenges are constantly evolving due to technological advancements such as IoT, AI, and big data. For instance, machine learning and data aggregation techniques can now infer and predict sensitive behavior or classifications from data types that were not previously considered sensitive [61,62]. These predictions can be made even if the individual being observed has not opted-in to use a particular service or product [63]. An example of this is how AI can predict sexual orientation with up to 91% accuracy from just five images of a person's face [64], which Nissenbaum [40] refers to as the "data food chain" (i.e., data of higher order is inferred from lower-order data).

Recent review studies, such as Gerber et al. [14] and Yun et al. [24], have not focused on IoT or AI technologies. In contrast, the current study aims to shed light on potential novel privacy concerns in the context of cutting-edge technologies. Yun et al. [24] demonstrated that the literature on privacy has undergone significant changes in the past two decades, including increased focus on contextual factors. However, with the rise of IoT, AI, AR, and Big Data technologies, which have

gained greater attention in academia due to higher adoption rates, there is a need for an up-to-date analysis. The current study is also driven by recent calls for more systematic reviews to better understand the complex and ever-changing concept of "user privacy" [14,22,65].

To address this gap in the existing literature, we conduct a systematic literature review focusing on three key research questions: first, in what specific contexts related to information flows have privacy concerns been studied in the age of AI, IoT, Big Data, and AR? Second, what psychological antecedents, outcomes, and theories explain privacy behavior in these technologies? Finally, how does privacy-related behavior in cutting-edge technologies differ from prior findings in contexts such as websites, mobile applications, social networking sites (SNS), or e-commerce? By addressing these questions, this study provides a synthesized overview and a crucial first step toward a context-contingent understanding of privacy, offering actionable insights for future research.

This understanding is particularly relevant for the fields of digital health and medical informatics, where privacy concerns are often heightened due to the sensitive nature of personal data. It equips policymakers and practitioners with tools to better address privacy violations, empower users with greater control over their data (e.g., privacy self-management), and promote safer technological ecosystems through design principles such as privacy by design [11,12,58,66–68]. In doing so, the current study can help advance our understanding and application of technology to improve user trust and system efficacy in healthcare and beyond.

Methodology

We conduct a systematic literature review to offer a transparent and comprehensive analysis of the existing literature and to develop a more context-contingent understanding of privacy concerns [69–71]. Compared to traditional reviews, systematic literature reviews are less biased, more accessible, and provide higher validity because they employ rigorous, scientific, and transparent methods in line with strict guidelines, which allow for replicability of results [72–75]. Systematic literature reviews are particularly helpful to achieve knowledge synthesis and can enable a broader scope than traditional narrative reviews, which is essential when addressing the interdisciplinary research questions posed in this paper [74]. Our systematic literature review adheres to the guidelines suggested by Booth et al. [75] and Fisch and Block [70]. To ensure replicability, we provide a detailed and transparent account of our process, which we outline in the subsequent section.

Motivation, scope, and systematic literature review

A systematic literature search was conducted using electronic databases to minimize biases and selection errors associated with manual search queries [76]. The chosen databases—ScienceDirect (Elsevier), SAGE, and EBSCO—served as the primary sources for the search, given their advanced

search capabilities and extensive collections of scientific articles in pertinent fields, such as business, psychology, and information technology (IT), spanning several decades.

To further enrich the search results, Google Scholar and the reference lists of relevant articles were also utilized to identify potentially overlooked sources [77]. Various keyword combinations, including "AI," "IoT," "Big Data," "Augmented Reality," and "Machine Learning," were employed in the search process, as these terms often encompass overlapping concepts and applications. For instance, IoT devices can operate on artificial intelligence (AI) algorithms, generating augmented realities while collecting vast amounts of data classified as big data [78–81].

Search queries were designed to include the selected keywords in the articles' titles, abstracts, and listed keywords. The following is a representative and simplified Boolean search sentence used for this purpose:

(TI privacy OR "privacy paradox" OR "privacy concern") AND ("privacy concerns" OR "privacy paradox" OR personalization paradox OR perceived vulnerability OR disclosure OR perceived control OR risk OR willingness to disclose OR user OR user OR adoption) AND (internet of things OR iot OR "smart devices" OR "connected device" OR "artificial intelligence" OR ai OR big data OR machine learning OR augmented reality OR ar OR virtual reality)

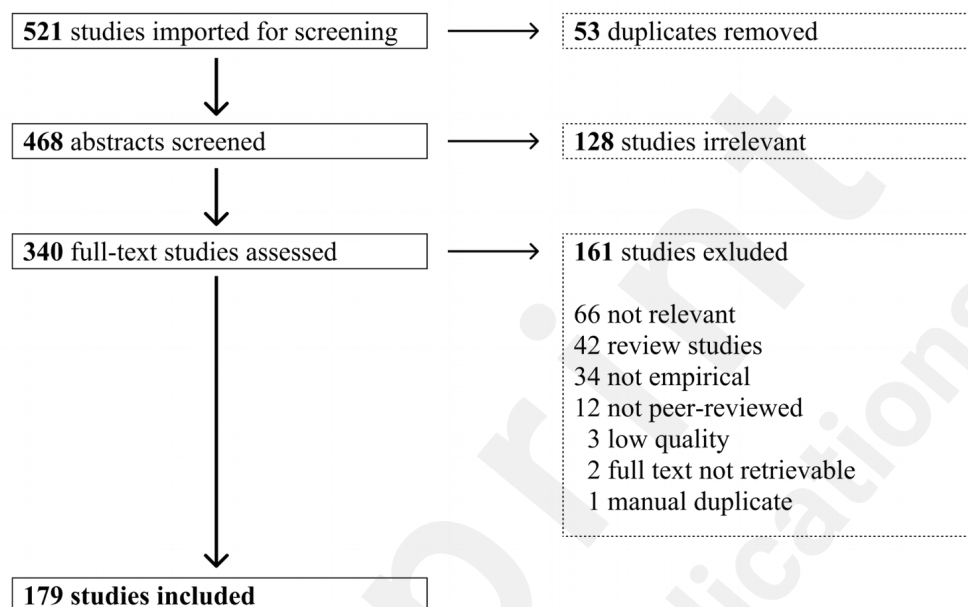
Furthermore, advanced search functions, such as filtering for peer-reviewed articles only, were employed to streamline the search process and enhance the quality of the results. Consequently, a total of 521 articles and conference papers were identified and retrieved from the initial search conducted on the three primary databases, in addition to the supplementary searches on Google Scholar and relevant reference lists.

Assessing the existing body of literature

The body of literature retrieved was subsequently assessed using the Covidence tool, with explicit exclusion and inclusion criteria established to systematically evaluate the existing evidence [70]. The primary objective of this initial assessment was to refine the dataset to include only the most pertinent articles that would address the research questions. To this end, duplicates (53) and non-relevant papers (128) were removed from the total pool of 521 abstracts. Articles were deemed non-relevant if they were not written in English or focused on different aspects of privacy research, such as technical privacy-enhancing software or ethics, rather than examining the psychological or behavioral interrelationships. Following this initial screening, 340 studies remained and underwent a full-text review for eligibility. An additional 161 articles were excluded at this stage for various reasons: they were not peer-reviewed, not empirical (including review studies), unrelated to the

research objectives, of low quality (i.e., lacking clarity or transparency), previously overlooked duplicates, or their full texts were unattainable [75]. As a result, the final dataset for analysis comprised 179 studies. The literature screening and selection process is depicted in Figure 1.

Figure 1. Inclusion and exclusion flow chart.



Analyzing and synthesizing findings

In the final stage of analysis, the 179 selected studies were systematically synthesized and categorized. Following the guidelines proposed by Booth et al. [75], key characteristics of each study, such as authors, title, abstract, year of publication, and the type and name of the publication, were organized in a table. Methodological factors, including study design, sample size, employed theories, data collection procedures, and measures, were also documented. To address the first research question (i.e., in what contexts related to information flows have privacy concerns been studied?), the analysis of the final dataset involved coding the studies according to the domains and contexts in which they were conducted. Nissenbaum's [15] theory of contextual integrity was employed, with studies coded based on the five parameters of information flows: data subject, sender, recipient, information type, and transmission principle. Additionally, Yun et al.'s [24] five-party personal information privacy model, building on Conger et al. [82], was adopted to gain a more nuanced understanding of the recipients of personal information (see Figure 2). The model facilitated the identification of numerous, often concealed parties potentially engaged in data sharing scenarios, highlighting the complexity of privacy in advanced technologies that extend beyond a traditional

sender-recipient model. Lastly, the findings of each study, including graphical conceptualizations of research models if given, were incorporated into the analysis. This comprehensive approach facilitated a deeper examination of antecedents, mediators, moderators, control variables, and outcomes related to privacy attitudes and behaviors, which in turn allowed for the exploration of the second and third research objectives (i.e., identifying key psychological antecedents, outcomes and theories, and comparing privacy-related behavior in cutting-edge technologies vs older technologies).

It is important to note that the codes used during this process were not predetermined; rather, they emerged inductively from the analysis of the articles [73]. Whenever a context, domain, or psychological factor (i.e., antecedents, outcomes) was mentioned, a code was annotated in the full text and subsequently transferred to the table.

Results

Overview of dataset

The analysis of the final dataset comprising 179 studies aimed to provide an overview of common characteristics among the selected research. The volume of relevant studies has experienced a considerable increase in recent years. The earliest article in this dataset was published in 1999, and since the early 2010s, academic interest in privacy-related topics has gained significant momentum. Notably, the number of publications doubled between 2020 and 2021, and 2022 (when the literature review was carried out) witnessed a new peak in output, as at the time of the analysis, publications were only eight short of 2021 levels. This trend aligns with expectations, as the focus of this study is on privacy within the context of emerging technologies (i.e., AI, Big Data, IoT). These technologies have seen a rise in relevance and adoption rates during the same period (e.g., Transforma Insights, [5]). Moreover, the growing prominence of privacy research can be attributed to the unfolding of the Information Age, which has placed privacy at the forefront of academic discourse. Many scholars consider privacy to be "the issue of our times" [83], further highlighting its importance in contemporary research.

The thematic composition of journals publishing articles on privacy merits particular attention. To evaluate the quality and core focus of these journals, we employed the journal quality list devised by Harzing [84], as well as the methodology outlined by Mustak et al. [73]. Our analysis included 157 journal articles, 19 conference papers, and three book chapters. In the infrequent instances where a journal was absent from Harzing's list [84], the authors determined the appropriate categorization by aligning the journal's website description with a suitable classification. As there was no uniform and reliable method for categorizing conference papers and book chapters, these

were grouped under "others" in accordance with the classifications proposed by Harzing [84]. Upon closer examination, it became evident that a multitude of journals from diverse knowledge areas had explored privacy as a research subject, thereby highlighting the interdisciplinary nature and relevance of the topic. However, as illustrated in Table 1, journals within the information systems and knowledge management domains accounted for the largest portion of the literature, comprising over 40% of the total body (179 articles). Additionally, marketing journals made a substantial contribution, with nearly a quarter of the articles appearing in publications from this field.

Table 1. Number of publications in knowledge areas of journals.

Knowledge area (based on Harzing)	Number of publications	Percentage
Management Information Systems, Knowledge Management	80	44.7%
Marketing	40	22.4%
Communication	16	8.9%
Psychology	5	2.8%
Public Sector Management	4	2.2%
Operations Research, Management Science, Production & Operations Management	3	1.7%
Tourism	3	1.7%
Organization Behavior/Studies, Human Resource Management, Industrial Relations	1	0.6%
Innovation	1	0.6%
Economics	1	0.6%
Others (Conference paper, Book chapter, not matching Harzing's category)	25	14%
Total	179	100%

During the analysis, each paper was assigned a code corresponding to a primary theme. This theme was predominantly determined by the device employed in study designs (i.e., the sender parameter) of an article. For instance, if a study examined privacy concerns among mobile app users,

the 'mobile' code was assigned. In cases where chatbot recommendations elicited privacy concerns, the 'AI' code was utilized. When a specific sender was not identified, the thematic topic was recorded, and the 'other' code was applied. This coding system aimed to offer a concise overview of the research focus in contemporary literature, facilitating our analysis in subsequent stages. However, it is important to acknowledge that these codes can be considered subjective and potentially ambiguous due to the often closely related or synonymous terminologies in the field. For example, a voice assistant (i.e., IoT) could also be classified as artificial intelligence. Despite this, the results presented in Table 2 reveal that the primary research focus areas thus far have been IoT, social networking sites (SNS), mobile and artificial intelligence. Lastly, upon excluding non-empirical findings, it was observed that the majority of studies (81.6%) exhibited a quantitative methodological orientation, with only a small number of studies adopting purely qualitative methods (9.5%) or implementing a mixed-method approach (8.9%).

Table 2. Number of predominant themes of analyzed studies.

Predominant Theme	Number of publications	Percentage
Internet of Things (IoT)	48	26.8%
SNS (incl. social media, instant messengers on mobile or websites)	29	16.2%
Mobile (incl. apps, location-based services, mobile e-commerce)	20	11.2%
Artificial Intelligence (AI)	20	11.2%
Big Data	9	5.0%
Website (incl. e-commerce)	9	5%
Augmented Reality	7	3.9%
Other (unspecified)	37	20.7%
(In e-commerce)	7	3.9%
(General online privacy concerns)	30	16.8%
Total	179	100%

Analysis of context

Table 3 shows the results of the analysis of contexts (i.e., information flows) used to study privacy concerns in the age of cutting-edge technologies (i.e., AI, IoT, Big Data and AR). Results for each contextual dimension are discussed further below.

Table 3. Number of contextual dimensions (i.e., information flow parameters) of analyzed studies.

Contextual Dimension	Code	Number of Publications	Percentage
Subject	User (IoT)	50	27.90%
	User (Online)	37	20.70%
	User (SNS)	30	16.80%
	User (AI)	18	10.10%
	User (Mobile)	18	10.10%
	Shopper (E-Commerce)	13	7.30%
	User (AR)	7	3.90%
	Citizen	2	1.10%
	User (Big Data)	2	1.10%
	Employee	2	1.10%
Total		179	100%
Sender	IoT	51	27.90%
	SNS	28	15.60%
	Website	26	14.50%
	Mobile	24	13.40%
	AI	18	10.10%
	Online/offline general total	23	12.80%
	multiple sender	5	2.80%
Total		179	100%
Recipient (actor)	analyzed with varying sensitivity	26	14.50%
	not analyzed for sensitivity	123	68.70%
	not specified	30	16.80%
Total		179	100%
Type of Information (attribute) ^a	general & unspecified personal information	74	41.30%
	specified personal information total	97^a	54.2% ^a
	not specified (i.e., not mentioned)	13	7.30%
Total		184^a	
Transmission Principle ^a	specified	50 ^a	28.4%^a
	not specified	142	79.30%
Total		192^a	

^aNumber & percentage in table indicates how often a parameter was found in a paper. The same paper may belong to multiple categories in a given dimension. Percentage calculated with base

value of 179. For example, in 79.3% of papers, no transmission principle was specified.

Individuals (subjects) whose data is being collected

Data collection subjects were categorized into ten groups based on how articles delineated their respondents within study designs. For instance, a user could be perceived as a generic online user [85], an IoT device user [61], or a citizen interacting with an e-government platform [86,87]. A substantial majority of studies closely adhere to the device employed in study designs (i.e., the sender) and implicitly or explicitly define users accordingly. Exceptions included extracted codes for designs specifically focusing on employees ($n = 2$, 1.1%), e-commerce shoppers ($n = 13$, 7.3%), and citizens ($n = 2$, 1.1%). The three most prominent types were IoT users ($n = 50$, 27.9%), generic online users ($n = 37$, 20.7%), and SNS users ($n = 30$, 16.8%). These results largely align with expectations.

However, the low counts for AR users were unexpected, given that the terms "augmented" and "virtual reality" were part of the initial search query. The impressive market growth rates and relevance across multiple sectors also suggested higher academic significance [6,88]. Moreover, it is worth noting that, despite our up-to-date dataset, SNS continue to attract considerable attention, even though they were not included in our initial search query [89–92]. To maintain manageable results, we opted against coding with even greater granularity. For example, a few studies concentrated on specific demographic groups such as children [93,94], teenagers [95], or individuals with low socioeconomic status [96]. The majority of studies in our dataset controlled for demographics and incorporated corresponding variables, such as age or gender.

Devices (sender) used to transmit personal information

The sender parameter results offer a detailed perspective on the specific technologies examined by papers in our dataset. In accordance with findings in the user category, we observe that IoT senders represent the most substantial share in this dimension ($n = 51$, 27.9%). However, when employing a more intricate coding, we notice differences in the particular device types. For example, the most prominent single sender type is not an IoT device but rather SNS ($n = 28$, 15.6%), followed by websites ($n = 26$, 14.5%) and mobile devices ($n = 14$, 13.4%). IoT smart assistants ranked as the fourth most prevalent device type within the dataset ($n = 21$, 11.7%). The high occurrence of SNS senders in the sender parameter was unexpected, prompting further investigation. The majority of analyzed SNS studies in our contemporary sample focused on Facebook users [89–92]. Despite their popularity and growth rates, Instagram and TikTok played no role in the SNS studies within our

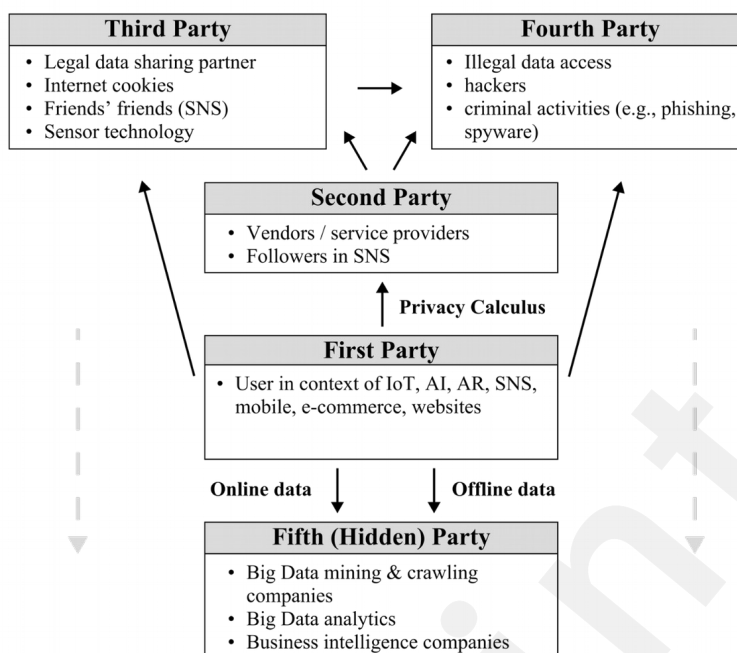
dataset.

Notably, only five studies (2.8%) investigated two different sender types concurrently, and merely one of them incorporated four distinct devices in its study design. This is in spite of recent evidence suggesting that user devices can impact privacy concerns, such as smartphones increasing privacy disclosure intentions compared to PCs [97,98]. Additionally, 23 papers (12.8%) did not explicitly define a sender and offered a more general level of analysis. Upon closer examination, we found that the absence of a sender type definition was frequently associated with a relatively early publication year [99–101]. Another reason was the investigation of another contextual dimension, necessitating control for other dimensions like information sensitivity [18,102,103]. Over recent years, the privacy literature has arguably developed a more nuanced understanding concerning the definition of the sender dimension in studies [24].

Recipient of personal information

A particularly intriguing contextual dimension concerning cutting-edge technologies pertains to the recipient of personal information, as the methods of data collection and sharing with second, third, fourth, or even fifth parties are rapidly evolving (Figure 2; [24]). The concept previously referred to as the "data food chain" [40] highlights the significance and complexity of incorporating this dimension into study designs. Through big data mining, data aggregation, and data analytics, organizations can now predict online and offline behavior using vast, seemingly unrelated data points [24,61,62,104].

Figure 2. Five-party model of personal information privacy [24].



However, only Hermes et al. [105] and Xie and Karan [92] have explicitly examined the so-called hidden fifth party ($n = 2$, 1.1%). The majority of articles ($n = 146$, 81.6%) primarily focus on the direct transaction between a user (first party) and the manufacturer or provider of a device or service (second party). Contrary to findings in Yun et al. [24], the intended or unintended sharing with third parties was not as prevalently studied in our dataset as anticipated ($n = 22$, 12.2%). Nevertheless, we observed a similar trend to the cited study, with more recent articles beginning to investigate illegal, unauthorized secondary access by fourth-party entities ($n = 9$, 5%). Moreover, a mere 26 papers (14.5%) in the sample considered varying the sensitivity of the data recipient while examining privacy concerns, such as altering the sharing of personal information with device manufacturers or third-party advertisers (notable examples include: Abdi et al., [61]; Lee & Kobsa, [106]; Leom et al., [39]; Lutz & Newlands, [107]; Marmion et al., [108]; Martin & Nissenbaum, [19]). However, almost 70% ($n = 123$) of the analyzed articles did not investigate users' varying perceived sensitivity towards recipients of their personal information, despite the increasing importance of this dimension, particularly in the IoT, AI, AR, and Big Data era [24]. The implications of this will be discussed later in the paper.

Type of information being shared

The idea that variations in privacy behavior may also depend on the type of information shared with an entity was introduced relatively early in the literature [109,110]. Our analysis reveals that over half of the studies mention a specific type of information being collected in their experiments or designs ($n = 97$, 54%). Several studies in this set either focus on a particular

information type exclusively ($n = 37$, 20.7%) or investigate multiple information types without further categorization (i.e., examining credit card details and purchase history, among other things, without classifying them as 'financial' or 'transactional' information; $n = 22$, 12.3%). Although a significant number of articles do not specify the type of personal information collected ($n = 74$, 41.3%), we observed a trend indicating that an increasing number of researchers are varying the sensitivity of information types to obtain more meaningful and comprehensive results ($n = 38$, 21.2%). In fact, 24 out of the 38 studies that experiment with variation in this parameter were published within the last five years. Notable examples among these include Abdi et al. [61]; Apthorpe et al. [17]; Carignani and Gemmo [111]; Cichy et al. [112]; Leom et al. [39]; Markos et al. [18]; Markos et al. [113]; Marmion et al. [108].

Transmission principles in data sharing situations

The principles governing data transmission relate to the why and under what conditions personal information is being shared with recipients. For instance, Abdi et al. [61] discovered that the acceptability of data sharing scenarios is contingent upon factors such as the retention duration, user notification regarding data usage, and assurances of anonymity and confidentiality. Lee and Kobsa [106,114] corroborate these findings, highlighting the significance of the rationale behind personal data collection in shaping users' judgments. For instance, users may perceive data collection for safety-related purposes as less acceptable than for health-related purposes [114]. Moreover, Internet of Things (IoT) devices, such as smart home assistants, are constantly monitoring for voice commands (e.g., "Hey Google", "Siri"), prompting a limited number of studies ($n = 4$, 2.2%) to explore potential differences in user reactions to continuous versus one-time monitoring [115]. The context in which data is transferred, specifically public versus private settings, also influences privacy concern assessments [43,98,116]. A significant aspect of data transmission principles, particularly in the context of advanced technologies, pertains to the mode of data collection—whether it occurs covertly or overtly. This distinction hinges on whether users are aware of or can observe the data collection process [89,117–119].

Despite existing evidence that these data transmission principles influence participants' judgments in data sharing situations, the literature on this subject remains limited. A review of empirical studies in the field reveals that 79.3% ($n = 142$) do not explicitly address this contextual dimension. The majority of these studies tend to implicitly explore certain principles by examining a specific service, such as Facebook, whose privacy policy articulates some transmission principles. However, only a handful of studies incorporate reading privacy policies or cookie notifications into their research design [120]. Consequently, future research should more explicitly incorporate and

investigate data transmission principles as a parameter [98].

Antecedents and outcomes

We analyzed a subset of our sample more closely to investigate which antecedents, outcomes and theories have been considered in the literature on cutting-edge technologies, thus addressing our second main research objective. We extracted studies coded with a predominant theme of IoT, AI, AR, or Big Data (see Table 2). Our subset of 68 studies is mainly composed of articles that were published no later than 2017. We synthesized findings and subsequently categorized study results into antecedents, privacy concerns, and outcomes (see Figure 3). Some constructs such as trust, perceived risks or perceived benefits were found to act as antecedents or outcomes.

Building upon and extending the work of Yun et al. [24,121], we categorize antecedents into six distinct classifications: individual factors, privacy calculus-related elements (i.e., the perceived risks and benefits users evaluate in their risk-benefit analysis prior to data disclosure), additional privacy-related aspects, organizational and task-related factors, macro-environmental influences, and contextual variables. Our integrative and succinct model uncovers previously unexplored findings from privacy research in the context of emerging technologies. For example, we observe the emergence of novel antecedents such as perceived physical risks (e.g., users' apprehensions regarding physical harm or intrusion into their personal space), which have been largely overlooked in past research [121]. As technological advancements progress, so do the contexts and human behaviors in which they are embedded. The notion of physical risk exemplifies this interrelationship, as it is intimately connected to the unique features of IoT, AR, and AI devices [122]. In this regard, Cichy et al. [112] demonstrate that drivers of connected and autonomously driven vehicles are increasingly anxious about their physical well-being, as concerns about the safety of autonomous driving are evoked. Similarly, Pal et al. [121] underscore the significance of physical risks for users of smart home devices. The integration of these novel IoT technologies within a user's personal space generates apprehension about surveillance and fosters fear of losing control over one's private environment [121].

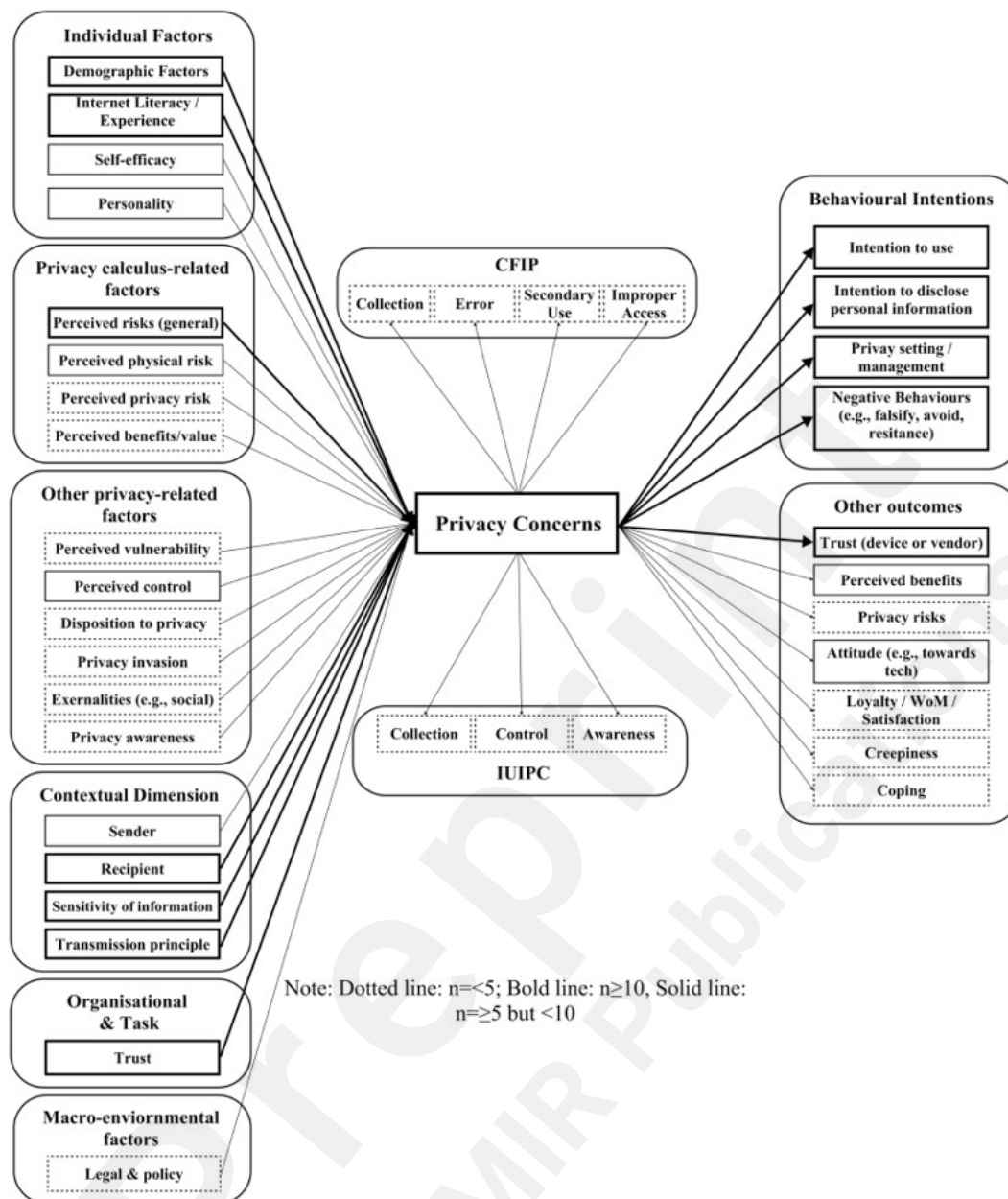
In examining the outcomes of privacy disclosure within the realm of emerging technologies, our analysis categorizes findings into two groups: behavioral intentions and other outcomes [24]. Several novel constructs have surfaced in recent years that were previously unaddressed [24], and these are intrinsically connected to the unique attributes of cutting-edge technologies. For instance, Rajaobelina et al. [123] demonstrate how privacy concerns can heighten users' sense of unease or "creepiness" during interactions with AI-based chatbots. Marakhimov and Joo [124] present

empirical evidence indicating that user privacy concerns related to wearable health devices prompt coping mechanisms (i.e., attempts to reinterpret or alleviate negative emotions), potentially explaining the abandonment of wearables by users within months of acquisition [125]. Moreover, our analysis reveals an increasing number of studies that explore a wider array of outcome variables, extending beyond direct links to usage intentions. For example, Cheng and Jiang [126] discover that perceived privacy risks associated with chatbots can lead to diminished satisfaction, while Rajaobelina et al. [123] highlight the influence of privacy concerns on customer loyalty, mediated by factors such as creepiness, trust, and negative emotions.

Taken together, we discern several notable trends within our subset of recent articles focusing on emerging technologies. First, a significant number of studies investigate personality traits as antecedents [34,127]. The examination of personality factors as antecedents of privacy concerns is a relatively nascent trend, initially identified by Yun et al. [24], which has since proliferated throughout the broader literature.

Second, numerous contextual factors have been incorporated into examinations of privacy concerns as they relate to IoT, AI, AR, or Big Data technologies. Notably, sensitivity of information emerges as a frequently incorporated antecedent within our 68-study subset. This finding aligns with prior results in the overall sample (see Table 3). Contextual dimensions have evidently gained prominence in contemporary empirical inquiries of privacy concerns in the context of cutting-edge technologies.

Figure 3. Count of antecedents and outcomes of privacy concerns in the context of IoT, AI, AR, and Big Data.



Third, it is noteworthy that none of the papers in our subset explicitly explore cultural values. While sample recruitment spanned countries such as Jordan [128], Saudi Arabia [129], Turkey [130], India [131], and China [132], no article in our subset examined privacy concerns in the context of IoT, AR, AI, or Big Data across national boundaries. However, such studies are present in our complete dataset of 179 articles when the focus on cutting-edge technology is removed. For instance, Pentina et al. [133] conducted a cross-cultural comparison in the context of mobile app adoption, while Markos et al. [113] explored differences in perceived sensitivity and willingness to disclose between U.S. and Brazilian online users. Lastly, we observe that trust as an antecedent and the outcome construct of behavioral intention are the most prevalent themes within the analyzed subset, yielding the majority of results. This propensity has persisted in the privacy literature, as

demonstrated by Yun et al.'s chronological review [24] encompassing a sample of studies from 1996 to 2017.

Theories in the context of IoT, AI, AR, and Big Data

In our investigation, we also examined the frameworks and theories employed to study IoT, AI, AR, and Big Data technologies. Drawing on Barth and de Jong [13], we classified theories into three categories. The first category encompassed theories predicated on the assumption that users' underlying risk-benefit evaluations are primarily rational. The second category comprised theories positing that rational privacy valuations are occasionally influenced by irrational biases (e.g., heuristics, immediate gratifications, habits). Finally, the third category, labeled "other" was designated for theories adopting alternative approaches to explain behavior in information-sharing situations. Table 4 provides a summary of the theories identified in our 68-study subsample.

Table 4. Overview and categorization of theories in analyzed subset (IoT, AI, AR and Big Data).

Category	Theory	Authors	Exemplary studies
Risk-Benefit calculation guided by rationality	Justice Theory	Deutsch[134]	Pizzi and Scarpi [135]
	Multidimensional Development Theory (MDT)	Laufer and Wolfe [136]	Pal et al. [121]
	Privacy calculus	Culnan and Armstrong [100]	Attié and Meyer-Waarden [137]; Cheng et al. [2] ; Gao et al. [138]; Hermes et al. [105]; Kang and Jung [139]; Kim et al. [140]; Lavado-Nalvaiz et al. [141]; Liu et al. [132]; Willems et al. [142]
	Protection Motivation Theory (PMT)	Rogers [143]	Alashoor et al. [144]; Gao et al. [138]; Thongmak [145]; Williams et al. [146]
	Social Exchange Theory	Blau [147]; Homans [148]	Uysal et al. [149]
	Technology Acceptance Model (TAM)	Davis [150]	Attié and Meyer-Waarden [137]; Liu and Tao [151]; Park et al. [152]; Pizzi

			and Scarpi [135]; Yavuz et al. [130]
	Theory of Planned Behavior (TPB)	Ajzen [153]	Alashoor et al. [144]; Attié and Meyer-Waarden [137]; Hermes et al. [105]
	Theory of Reasoned Action (TRA)	Ajzen and Fishbein [154]; Fishbein and Ajzen [155]	Attié and Meyer-Waarden [137]; Bawack et al. [156]
	Unified Theory of Acceptance and Use of Technology (UTAUT)	Venkatesh et al. [157]	Attié and Meyer-Waarden [137]; Easwara Moorthy and Vu [116]; Gao et al. [138]; Vimalkumar et al. [158]
	Communication Privacy Management (CPM) / Information Boundary Theory (IBT)	Petronio [159–161]	Cao and Wang [162]; Kang and Jung [139]; Kathuria and Kathuria [163]
Biased risk assessment within the risk- benefit calculation	Contextual Integrity	Nissenbaum [15]	Abdi et al. [61]; Agesilaou and Kyza [93]; Apthorpe et al. [17]; Harborth and Pape [164]; Lutz and Newlands [107]
	Coping theory	Lazarus and Folkman [165]	Cheng et al. [2] ; Marakhimov and Joo [124]
	Heuristic- systematic model of information processing (HSM)	Chaiken [166]	Shin [167]
	Innovation Resistance Theory	Ram [168,169]	Liu et al. [132]; Pal et al. [121]

Others	Prospect theory	Kahneman and Tversky [170,171]	Jain et al. [172]
	Signalling theory	Spence [173]	Jain et al. [172]
	Social Cognition Theory	Bandura [174]	Cao et al. [162]
	Uncanny Valley Theory	Mori [175,176]	Lavado-Nalvaiz et al. [141]; Willems et al. [142]
	Uses and Gratification theory	Katz and Blumler [177]; Katz et al. [178]	Attíe and Meyer-Waarden [137]; Jain et al. [172]; McLean and Osei-Frimpong [179]; Rauschnabel et al. [180]
	Mind Perception Theory	Gray et al. [181]	Uysal et al. [149]
	Query theory	Johnson et al. [182]	Sun et al. [183]
	Theory of Diffusion of Innovation (DOI)	Rogers [184]; Rogers et al. [185]	Attíe and Meyer-Waarden [137]

Our findings indicate that the majority of theories in our subsample were also recognized by Barth and de Jong [13]. However, formerly prominent theories such as the theory of incomplete information [186] and the theory of bounded rationality [187] were not detected in our analysis, despite employing a broader search scope than Barth and de Jong [13]. Conversely, new theories have emerged, including the uncanny valley theory [175,176] and the theory of contextual integrity [15]. The former is explicitly connected to the perceived anthropomorphism of robots (i.e., the degree of human-likeness) and thus aligns with our emphasis on cutting-edge technologies. This theory appears to be the most prevalent framework in studies investigating the context-dependency of privacy disclosure, a research focus that has gained traction in recent years [17,61,107,164]

In sum, we observe an equitable distribution between theories focused on rational risk-benefit calculations and those addressing biased evaluations due to human cognitive limitations and exploited heuristics (see Table 4). Within the rationality-based school of thought, the privacy calculus

theory [100] and technology acceptance models (TAM by Davis [150] or UTAUT by Venkatesh et al. [157]) are most frequently employed as the theoretical frameworks in our subsample. Regarding the second group, we find that Petronio's [161] Communication Privacy Management (CPM) and the previously mentioned theory of contextual integrity [15] emerge as the most prominent within their category.

Privacy behavior in the context of IoT, AI, AR, and Big Data

In the final stage of our investigation, we wanted to elucidate whether privacy-oriented behaviors, such as the privacy paradox, in emergent technologies tend to diverge from prior findings in other technological domains, including websites, mobile applications, social networking sites (SNS), and e-commerce. The majority of extant studies corroborate the existence of the privacy paradox. For example, Lavado-Nalvaiz et al. [141] and Lutz and Tamó-Larrieux [188] highlight the paradox's pervasiveness within the realm of social robots. Similarly, Willems et al. [142] substantiate its presence in the context of citizens' adoption intentions concerning AI-based public service applications. Furthermore, Chaparro Osman et al. [189], Aleisa et al. [129], Jaspers and Pearson [190], and Pal et al. [191] provide support for the privacy paradox among users of domestic Internet of Things (IoT) devices. Thus, the literature affirms the persistence of the privacy paradox across various technological contexts.

However, a more comprehensive examination of our analysis unveils intriguing findings in the literature on state-of-the-art technologies. For instance, Menard and Bott [192] discovered that privacy concerns for IoT users are addressed differently compared to those in e-commerce settings. In the latter, users typically react to heightened awareness of data collection with increased privacy concerns and consequently, protective behavior. In contrast, the authors reveal an inverse relationship in an IoT context, where awareness of data collection by the IoT device leads to greater disclosure intentions [192]. They postulate that this relationship may arise because a user's information disclosure is intrinsically linked to the utility of IoT devices, which provide optimized and automated recommendations [192]. IoT devices possess minimal functionality unless users supply the requisite personal information, an assertion corroborated by Pal et al. [191].

In a similar vein, Sun et al. [183] demonstrated in an IoT experiment – comparing participants' actual behavior with stated intentions – that participants disclosed less personal information than they initially claimed they would. The privacy paradox typically implies an intention-behavior gap in the opposite direction (i.e., individuals divulging more information in behavioral conditions than intention conditions). The authors propose that the reversed intention-behavior gap they observed could be attributed to the abstract nature of IoT devices, rendering the concept of IoT less salient

than, for example, commerce [183]. Another plausible explanation for the reversed intention-behavior gap lies in users' unfamiliarity with novel IoT technologies, leading to inaccurate risk and benefit assessments due to a lack of knowledge [183,193]. Comparable effects were demonstrated by Chaparro Osman et al. [189], Hermes et al. [105], and Alashoor et al. [144] in IoT and Big Data contexts, respectively. Therefore, further research to examine the aforementioned claims is richly deserving.

Discussion

Contributions to theory and directions for future research

Privacy has emerged as one of the most pressing concerns of our era and will require heightened attention with the mainstream adoption of cutting-edge technologies, including IoT, AI, AR and Big Data. Despite over two decades of scholarly research on privacy, a comprehensive and context-dependent theory remains elusive. Consequently, a research gap persists regarding the differing standards individuals apply to data protection across various contexts [32,79]. In response, the present systematic literature review, encompassing 179 research studies, offers several theoretical contributions.

By examining state-of-the-art technologies, we present a timely and distinctive perspective on how constructs and theories have evolved and been contextualized within existing privacy research. Our synthesis of findings contributes to the literature by unveiling gaps and unanticipated relationships between privacy concerns and behaviors in the era of ubiquitous computing, which could potentially guide future research. This study substantiates the notion that contextual factors have been largely overlooked in privacy research on cutting-edge technologies (our first main research question). Merely five studies in our dataset explicitly defined items aligning with most of Nissenbaum's [15] five parameters of information flows. An analysis of perceived information sensitivity degrees was most prevalent in studies employing contextualization ($n = 97$, 54.2%). These results may support Solove's [21] and Kokolakis' [22] assertions that the dichotomy between privacy concerns and behavioral intentions is not paradoxical but rather has not been comprehensively understood in a holistic and context-contingent manner, which could provide logical explanations for this seemingly inconsistent behavior (also Martin & Murphy [59]). Following Xu and Zhang [37], our findings therefore also suggest that as long as no context-contingent theory is provided and widely accepted, future researchers must employ careful theory-driven contextualization to achieve more generalizability and interpretability of findings.

Future research may thus focus on examining additional information-sharing situations with

emerging technologies to delineate context-dependency in privacy behavior. Specifically, additional research is needed to explore the role of institutional trust in shaping privacy concerns, as patient perceptions of trusted organizations like national health institutions versus commercial entities significantly influence their willingness to share sensitive data [23]. This is particularly important because these technologies often operate ubiquitously without an individual's awareness, becoming increasingly pertinent in numerous aspects of daily life, such as healthcare and e-government.

As recommended by Yun et al. [24] future studies on privacy concerns could also concentrate on these underexplored fields of application or investigate how the ubiquity and unique attributes of novel technologies alter user privacy behaviors. Our analysis demonstrates that results are frequently connected to users who are not yet familiar with emerging technologies. We encourage future research to examine how these findings evolve as new technologies become more widely adopted, and users inevitably become more accustomed to these devices in their daily lives. Additionally, we advocate for more studies to incorporate a broader array of specified principles in research designs, as well as examine actual behavior rather than intentions. Both aspects have been largely neglected in the literature, yet they significantly influence study outcomes [194].

Our findings further indicate that most antecedent and outcome constructs, along with underlying theories, have been transferred from research on websites, social media, or e-commerce to the context of cutting-edge technologies (our second key research question). We observe that the literature continues to develop or employ novel constructs and theories frequently associated with unique characteristics of IoT, AR, or AI devices (e.g., physical risks). While the ongoing expansion of constructs may be necessary to comprehend new technologies, it simultaneously introduces further divergence in a field already replete with theoretical approaches [24].

Our study supports the call for developing context-contingent insights specific to emerging technologies and work that enhances user engagement and well-being [22,24,195–204], as well as converging towards more generalizable, robust, and underlying theories that systematically operate across diverse contexts [24,37]. The limited privacy literature on cutting-edge technologies reveals that previously identified results in other domains, such as e-commerce, do undergo alterations when study designs are recontextualized into IoT, AR, AI, or Big Data (our third key research question). More context-specific studies on privacy concerns in cutting-edge technology scenarios are needed to reach a critical mass to allow a theoretical synthesis of findings [37]. As previously mentioned, these studies must be theory-grounded to allow generalizability. We argue that using the five parameters of Nissenbaum's contextual integrity theory [15] in future research will allow a synthesis towards a context-contingent understanding of privacy. We posit that individuals' privacy concerns

and behaviors are dependent upon a complex interplay of contextual dimensions inherent to IoT, AI, AR, and Big Data technologies rather than a rational risk-benefit analysis. Specifically, these dimensions include the individuals whose data is being collected, the devices transmitting personal information, the recipient of the information, the type of information shared, and the principles governing data transmission. We thus suggest that the dynamics within contextual dimensions of emerging technologies contribute to shaping individuals' privacy attitudes, intentions, and behaviors, leading to unique patterns that may differ from traditional contexts.

Implications

First, the results underscore the critical role of contextual dimensions in shaping user privacy concerns, emphasizing the need for companies and device manufacturers to investigate these dimensions thoroughly. Context-aware privacy considerations can inform the design and marketing of new digital health technologies, enabling products that align with user preferences and ethical standards. For example, the development of transparent and accessible privacy policies tailored to user needs can address significant user concerns, as demonstrated in prior studies on the impact of clear privacy policies on user trust and adoption [9,10]. In addition, the use of conversational AI in healthcare has been shown to mitigate privacy concerns by streamlining user engagement while ensuring data security, as evidenced by recent implementations [205].

Adopting a "privacy by design" approach might ensure that products, such as wearable health devices or telehealth platforms, offer granular control over sensitive data without overwhelming users with excessive opt-in choices [206]. Overloading users with consent requests may lead to decision fatigue, reducing their sense of control and trust in the system [207]. Instead, default privacy-preserving options can effectively guide user behavior while minimizing intrusiveness, particularly for less sensitive data streams [208]. Healthcare-focused applications of IoT and AI, such as remote monitoring devices, could integrate these insights to enhance usability and compliance while safeguarding patient data. For example, enabling users to manage privacy settings for specific contexts—such as sharing data with healthcare providers but not with third-party advertisers—can improve trust and engagement with these technologies.

Marketing and customer service teams in the digital health space can benefit from a deeper understanding of user privacy concerns in specific scenarios. By acknowledging the perceived risks associated with IoT devices, especially in healthcare (e.g., fears of data breaches or misuse of sensitive health data), companies can develop targeted educational campaigns to address these concerns. Clear, transparent communication about data usage, security protocols, and user controls can alleviate anxiety, fostering higher levels of trust, satisfaction, and loyalty. Enhanced trust in

digital health platforms can translate into increased adoption rates and long-term engagement, ultimately benefiting both users and organizations [209,210].

From a policy-making perspective, our findings highlight the need to revise and refine privacy regulations to address the contextual nuances of privacy behavior. Policymakers should mandate that privacy policies explicitly outline all five contextual parameters proposed by Nissenbaum [15,38] ensuring that users understand how their data is collected, shared, and used in specific contexts. This is particularly important for digital health technologies, where sensitive health information often flows through complex data ecosystems, involving multiple parties. Transparent policies that restrict information sharing to essential second- or third-party recipients can reduce unauthorized data flows and prevent misuse [17].

Moreover, regulators should establish standards for "privacy by design" in the development of new health technologies, requiring restrictive default settings and clear consent mechanisms. For example, IoT-enabled medical devices could be required to limit data sharing to approved healthcare providers, reducing the risk of exposure to unintended parties. Additionally, ethical guidelines for predictive analytics, such as algorithms that infer health conditions from user behavior, should ensure that these insights are used responsibly and transparently, avoiding harm to users or erosion of trust.

Conclusion

The current study underscores the critical importance of adopting a context-sensitive lens to understand privacy concerns in the rapidly evolving landscape of emerging. By synthesizing existing studies, this work uncovers significant research gaps and emphasizes the need for more holistic, context-sensitive approaches that consider the dynamic interaction between psychological antecedents, behavioral outcomes, and technological attributes. Our findings have important implications for researchers, practitioners, and policymakers alike. For researchers, they provide a foundation for advancing theories that are adaptable to diverse and complex privacy scenarios. For practitioners and technology developers, the insights offer a pathway to designing user-centric technologies that integrate privacy as a core feature rather than an afterthought. For policymakers, this work emphasizes the necessity of revising privacy frameworks to address the contextual dimensions of data sharing and ensure ethical and transparent practices. In domains such as digital health, where the stakes are particularly high, such an approach can build trust, enhance user engagement, and support the ethical deployment of technologies that improve health outcomes and empower individuals. By bridging gaps in the literature and paving the way for context-driven solutions, this study contributes to the broader goal of fostering a digital ecosystem that balances innovation with user privacy and trust.

Conflicts of Interest

There are no conflict of interest to report.

Abbreviations

IoT: Internet of things

AI: Artificial intelligence

AR: Augmented reality

Communication Privacy Management

E-commerce: Electronic commerce

International Data Corporation

Information technology

Massachusetts Institute of Technology

Personal Computer

SNS: Social Networking Sites

Technology Acceptance Model

Unified Theory of Acceptance and Use of Technology

References

1. Metz R. Yes, Alexa is recording mundane details of your life, and it's creepy as hell. MIT Technology Review. 2018. Available from: <https://www.technologyreview.com/2018/05/25/142713/yes-alexa-is-recording-mundane-details-of-your-life-and-its-creepy-as-hell/> [accessed Aug 4, 2022]
2. Cheng X, Su L, Luo X, Benitez J, Cai S. 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* 2021;1–25. PMID:148013989
3. Grewal D, Guha A, Satornino CB, Schweiger EB. Artificial Intelligence: The light and the darkness. *J Bus Res* 2021;136:229–236. doi: 10.1016/j.jbusres.2021.07.043
4. Li W, Yigitcanlar T, Erol I, Liu A. Motivations, barriers and risks of smart home adoption: From systematic literature review to conceptual framework. *Energy Res Soc Sci* 2021;80:102211. doi: 10.1016/j.erss.2021.102211
5. Transforma Insights. Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030, by vertical (in millions). Statista: Statista Inc.; 2022. Available from: <https://www-statista-com.iclibezp1.cc.ic.ac.uk/statistics/1194682/iot-connected-devices-vertically/> [accessed Aug 4, 2022]
6. IDC, Statista. Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2025 (in zettabytes). statista.com: IDC Statista Inc.; 2021. Available from: <https://www-statista-com.iclibezp1.cc.ic.ac.uk/statistics/871513/worldwide-data-created/> [accessed Aug 4, 2022]
7. Ziegeldorf JH, Morchon OG, Wehrle K. Privacy in the Internet of Things: threats and challenges. *Security and Communication Networks* John Wiley & Sons, Ltd; 2014;7(12):2728–2742. doi: 10.1002/sec.795
8. Kumar A, Braud T, Tarkoma S, Hui P. Trustworthy AI in the age of pervasive computing and big data. 2020 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops) 2020. p. 1–6. doi: 10.1109/PerComWorkshops48775.2020.9156127

9. Bardus M, Al Daccache M, Maalouf N, Al Sarih R, Elhajj IH. Data management and privacy policy of COVID-19 contact-tracing apps: systematic review and content analysis. *JMIR Mhealth Uhealth* JMIR Publications Inc.; 2022 Jul 1;10(7). PMID:35709334
10. Alhammad N, Alajlani M, Abd-Alrazaq A, Epiphaniou G, Arvanitis T. Patients' perspectives on the data confidentiality, privacy, and security of mHealth apps: systematic review. *J Med Internet Res*. JMIR Publications Inc.; 2024. PMID:38820572
11. Baruh L, Popescu M. Big data analytics and the limits of privacy self-management. *New Media Soc* SAGE Publications; 2017;19(4):579–596. doi: 10.1177/1461444815614001
12. Lehtiniemi T, Kortensniemi Y. Can the obstacles to privacy self-management be overcome? Exploring the consent intermediary approach. *Big Data Soc* 2017;4(2):2053951717721935. doi: 10.1177/2053951717721935
13. Barth S, de Jong MDT. The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics* 2017;34(7):1038–1058. doi: 10.1016/j.tele.2017.04.013
14. Gerber N, Gerber P, Volkamer M. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Comput Secur* 2018;77:226–261. doi: 10.1016/j.cose.2018.04.002
15. Nissenbaum H. Privacy as contextual integrity. *Wash L Rev* 2004;79:119.
16. Abaquita D, Bahirat P, Badillo-Urquiola KA, Wisniewski P. Privacy norms within the internet of things using contextual integrity. *Companion of the 2020 ACM International Conference on Supporting Group Work* 2020. p. 131–134. doi: 10.1145/3323994.3369891
17. Apthorpe N, Shvartzshnaider Y, Mathur A, Reisman D, Feamster N. Discovering smart home internet of things privacy norms using contextual integrity. 2018. doi: 10.1145/3214262
18. Markos E, Labrecque LI, Milne GR. A new information lens: the self-concept and exchange context as a means to understand information sensitivity of anonymous and personal identifying information. *Journal of Interactive Marketing* 2018;42:46–62. doi: 10.1016/j.intmar.2018.01.004
19. Martin K, Nissenbaum H. Measuring privacy: An empirical test using context to expose confounding variables. *Columbia Science and Technology Law Review*, Forthcoming 2016;18:176.
20. Nicholas J, Shilton K, Schueller SM, Gray EL, Kwasny MJ, Mohr DC. The role of data type and recipient in individuals' perspectives on sharing passively collected smartphone data for mental health: cross-sectional questionnaire study. *JMIR Mhealth Uhealth* 2019;7(4):e12578. PMID:30950799
21. Solove DJ. The myth of the privacy paradox. *George Washington Law Review* 2021;89:1. doi: 10.2139/ssrn.3536265
22. Kokolakis S. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Comput Secur* 2017;64:122–134. doi: 10.1016/j.cose.2015.07.002
23. Aggarwal R, Farag S, Martin G, Ashrafian H, Darzi A. Patient perceptions on data sharing and applying artificial intelligence to health care data: Cross-sectional survey. *J Med Internet Res*. JMIR Publications Inc.; 2021. PMID:34236994
24. Yun H, Lee G, Kim DJ. A chronological review of empirical research on personal information privacy concerns: An analysis of contexts and research constructs. *Information & Management* 2019;56(4):570–601. PMID:136241254
25. Dienlin T, Trepte S. Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *Eur J Soc Psychol* John Wiley & Sons, Ltd; 2015;45(3):285–297. doi: 10.1002/ejsp.2049
26. Tomasz G. Consumer resistance to the Internet of Things: A privacy perspective. *Competition, Strategy, and Innovation* Routledge; 2021. p. 133–150. ISBN:1003204341
27. Gambino A, Kim J, Sundar SS, Ge J, Rosson MB. User disbelief in privacy paradox: Heuristics that determine disclosure. *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems* 2016; doi: 10.1145/2851581.2892413

28. Sundar SS, Kang H, Wu M, Go E, Zhang B. Unlocking the privacy paradox: Do cognitive heuristics hold the key. CHI '13 Extended Abstracts on Human Factors in Computing Systems Paris, France; 2013. p. 811–816. doi: 10.1145/2468356.2468501
29. Sundar SS, Kim J. Machine heuristic: When we trust computers more than humans with our personal information. Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems 2019. p. 1–9. doi: 10.1145/3290605.3300768
30. Acquisti A, Taylor C, Wagman L. The economics of privacy. J Econ Lit 2016 Jun;54(2):442–492. doi: 10.1257/jel.54.2.442
31. Fernandes T, Pereira N. Revisiting the privacy calculus: Why are consumers (really) willing to disclose personal data online? Telematics and Informatics 2021;65:101717. doi: 10.1016/j.tele.2021.101717
32. Lasarov W, Hoffmann S. Paradoxes datenschutzverhalten. HMD Praxis der Wirtschaftsinformatik 2021;58(6):1535–1551. doi: 10.1365/s40702-021-00706-2
33. Acquisti A, Grossklags J. Privacy and rationality in individual decision making. IEEE Secur Priv 2005;3(1):26–33. doi: 10.1109/MSP.2005.22
34. Bawack RE, Wamba SF, Carillo KDA. Exploring the role of personality, trust, and privacy in customer experience performance during voice shopping: Evidence from SEM and fuzzy set qualitative comparative analysis. Int J Inf Manage 2021;58:102309. doi: 10.1016/j.ijinfomgt.2021.102309
35. Pomfret L, Previte J, Coote L. Beyond concern: socio-demographic and attitudinal influences on privacy and disclosure choices. Journal of Marketing Management Routledge; 2020;36(5–6):519–549. doi: 10.1080/0267257X.2020.1715465
36. Buck C, Horbel C, Germelmann C, Eymann T. The unconscious app consumer: Discovering and comparing the information-seeking patterns among mobile application consumers. ECIS 2014 Proceedings - 22nd European Conference on Information Systems 2014.
37. Xu H, Zhang N. From contextualizing to context theorizing: assessing context effects in privacy research. Manage Sci INFORMS; 2022; doi: 10.1287/mnsc.2021.4249
38. Nissenbaum H. Privacy in context: technology, policy, and the integrity of social life. Stanford, CA: Stanford University Press; 2009. ISBN:9780804752374
39. Leom M Di, Deegan G, Martini B, Boland J. Information disclosure in mobile device: Examining the influence of information relevance and recipient. Proceedings of the 54th Hawaii International Conference on System Sciences 2021. p. 4632. doi: 10.24251/HICSS.2021.562
40. Nissenbaum H. Contextual integrity up and down the data food chain. Theoretical Inquiries in Law 2019;20(1):221–256. doi: 10.1515/til-2019-0008
41. Acquisti A, John LK, Loewenstein G. What is privacy worth? J Legal Stud 2013;42(2):249–274. doi: 10.1086/671754
42. John LK, Acquisti A, Loewenstein G. Strangers on a plane: context-dependent willingness to divulge sensitive information. Journal of consumer research 2011;37(5):858–873. doi: 10.1086/656423
43. Naeini PE, Bhagavatula S, Habib H, Degeling M, Bauer L, Cranor LF, Sadeh N. Privacy expectations and preferences in an IoT world. Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017) 2017. p. 399–412.
44. Eisingerich AB, Chun H, Liu Y, Jia H (Michael), Bell S. Why recommend a brand face-to-face but not on Facebook? How word-of-mouth on online social sites differs from traditional word-of-mouth. Journal of Consumer Psychology 2015 Jan;25. doi: 10.1016/j.jcps.2014.05.004
45. Merlo O, Eisingerich AB, Hoyer W. Immunizing customers against negative brand-related information. J Acad Mark Sci 2023 Mar 11;52:140–163. doi: 10.1007/s11747-023-00929-3
46. Merlo O, Eisingerich AB, Gillingwater R, Cao J. Exploring the changing role of brand archetypes in customer-brand relationships: Why try to be a hero when your brand can be more? Bus Horiz 2022 Nov 1;66. doi: 10.1016/j.bushor.2022.11.001
47. Park C, Eisingerich AB, Park J. Attachment–Aversion (AA) model of customer–brand relationships.

- Journal of Consumer Psychology 2013 Apr 1;23:229–248. doi: 10.1016/j.jcps.2013.01.002
48. Bell S, Eisingerich AB. The paradox of customer education: Customer expertise and loyalty in the financial services industry. *European Journal of Marketing* - EUR J MARK 2007 Jun 5;41:466–486. doi: 10.1108/03090560710737561
 49. Bell S, Auh S, Eisingerich AB. Unraveling the customer education paradox: when, and how, should firms educate their customers? *J Serv Res* 2017 Feb 15;20:109467051769184. doi: 10.1177/1094670517691847
 50. Eisingerich AB, Bell S. Perceived service quality and customer trust: does enhancing customers' service knowledge matter? *Journal of Service Research - J SERV RES* 2008 Feb 1;10:256–268. doi: 10.1177/1094670507310769
 51. Wittes B, Liu JC. The privacy paradox: The privacy benefits of privacy threats. Center for Technology Innovation at Brookings 2015;1–21.
 52. Merlo O, Eisingerich AB, Auh S. Why customer participation matters. *MIT Sloan Manag Rev* 2013;54. Available from: <https://sloanreview.mit.edu/article/why-customer-participation-matters/> [accessed Jan 16, 2025]
 53. Merlo O, Eisingerich AB, Auh S, Levstek J. The benefits and implementation of performance transparency: The why and how of letting your customers 'see through' your business. *Bus Horiz* 2017 Oct 1; doi: 10.1016/j.bushor.2017.09.007
 54. Kim J, Sung Y. Artificial Intelligence is safer for my privacy: interplay between types of personal information and agents on perceived privacy risk and concerns. *Cyberpsychol Behav Soc Netw* 2022;25(2):118–123. PMID:155187215
 55. Parmar N, Dong L, Eisingerich AB. Connecting with your dentist on Facebook: patients' and dentists' attitudes towards social media usage in dentistry. *J Med Internet Res* 2018;20(6):e10109. doi: 10.2196/10109
 56. Bélanger F, Crossler RE. Privacy in the digital age: a review of information privacy research in information systems. *MIS Quarterly Management Information Systems Research Center, University of Minnesota*; 2011;35(4):1017–1041. doi: 10.2307/41409971
 57. Smith HJ, Dinev T, Xu H. Information privacy research: an interdisciplinary review. *MIS Quarterly Management Information Systems Research Center, University of Minnesota*; 2011;35(4):989–1015. doi: 10.2307/41409970
 58. Saura JR, Ribeiro-Soriano D, Palacios-Marqués D. Setting privacy “by default” in social IoT: theorizing the challenges and directions in big data research. *Big Data Research* 2021;25:100245. doi: 10.1016/j.bdr.2021.100245
 59. Martin K, Murphy P. The role of data privacy in marketing. *J Acad Mark Sci Springer Nature*; 2017;45(2):135–155. PMID:121264032
 60. Beke FT, Eggers F, Verhoef PC. Consumer informational privacy: current knowledge and research directions. *Foundations and Trends® in Marketing Now Publishers*; 2018;11(1):1–71. doi: 10.1561/17000000057
 61. Abdi N, Zhan X, Ramokapane KM, Such J. Privacy norms for smart home personal assistants. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. Yokohama, Japan: Association for Computing Machinery; 2021. p. Article 558. doi: 10.1145/3411764.3445122
 62. Winter JS, Davidson E. Big data governance of personal health information and challenges to contextual integrity. *The Information Society Routledge*; 2019;35(1):36–51. doi: 10.1080/01972243.2018.1542648
 63. Matzner T. Why privacy is not enough privacy in the context of “ubiquitous computing” and “big data.” *Journal of Information, Communication and Ethics in Society Emerald Group Publishing Limited*; 2014;12(2):93–106. doi: 10.1108/JICES-08-2013-0030
 64. Wang Y, Kosinski M. Deep neural networks are more accurate than humans at detecting sexual orientation from facial images. *J Pers Soc Psychol* 2018;114(2):246. doi: 10.1037/pspa0000098
 65. Vassallo M. The privacy paradox in the big data era? No thanks, we are the e-people: the e-people in

- the big data era. *International Journal of Cyber Behavior, Psychology and Learning (IJCBLP)* 2019;9(3):32–47. doi: 10.4018/IJCBLP.2019070103
66. Solove DJ. Introduction: privacy self-management and the consent dilemma. *Harv Law Rev Harvard Law Review Association*; 2013;126(7):1880–1903. PMID:87598584
67. Aljeraisy A, Barati M, Rana O, Perera C. Privacy laws and privacy by design schemes for the Internet of Things: a developer's perspective. *ACM Comput Surv Association for Computing Machinery*; 2021;54(5):1–38. PMID:151371530
68. Jacobs B, Popma J. Medical research, Big Data and the need for privacy by design. *Big Data Soc* 2019;6(1):2053951718824352. doi: 10.1177/2053951718824352
69. Frank H, Hatak I. Doing a research literature review. In: Fayolle A, Wright M, editors. *How to get published in the best entrepreneurship journals* Cheltenham: Edward Elgar; 2014. p. 94–117. doi: 10.4337/9781782540625.00012
70. Fisch C, Block J. Six tips for your (systematic) literature review in business and management research. *Management Review Quarterly* 2018;68(2):103–106. doi: 10.1007/s11301-018-0142-x
71. Watson RT. Beyond being systematic in literature reviews in IS. *Journal of Information Technology* 2015;30(2):185–187. doi: 10.1057/jit.2015.12
72. Cook DJ, Greengold NL, Ellrodt AG, Weingarten SR. The relation between systematic reviews and practice guidelines. *Ann Intern Med* 1997;127(3):210–216. PMID:9245227
73. Mustak M, Jaakkola E, Halinen A, Kaartemo V. Customer participation management: Developing a comprehensive framework and a research agenda. *Journal of Service Management* 2016; doi: 10.1108/JOSM-01-2015-0014
74. Rowley J, Keegan BJ. An overview of systematic literature reviews in social media marketing. *J Inf Sci* 2020;46(6):725–738. doi: 10.1177/0165551519866544
75. Booth A, Sutton A, Clowes M, Martyn-St James M. *Systematic approaches to a successful literature review* (third edition). SAGE; 2022. ISBN:9781529759648
76. Tricco AC, Tetzlaff J, Sampson M, Fergusson D, Cogo E, Horsley T, Moher D. Few systematic reviews exist documenting the extent of bias: a systematic review. *J Clin Epidemiol* 2008;61(5):422–434. doi: 10.1016/j.jclinepi.2007.10.017
77. Horsley T, Dingwall O, Sampson M. Checking reference lists to find additional studies for systematic reviews. *Cochrane Database of Systematic Reviews* John Wiley & Sons, Ltd; 2011;(8). PMID:MR000026
78. Bilal A. Rise of technomoral virtues for Artificial Intelligence-based emerging technologies' users and producers: threats to personal information privacy, the privacy paradox, trust in emerging technologies, and virtue ethics. 2022. doi: 10.13140/RG.2.2.23285.04327
79. Mariani MM, Perez-Vega R, Wirtz J. AI in marketing, consumer research and psychology: a systematic literature review and research agenda. *Psychol Mark* 2022;39(4):755–776. doi: 10.1002/mar.21619
80. Smith G. Artificial Intelligence and the privacy paradox of opportunity, big data and the digital universe. 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE) 2019. p. 150–153. doi: 10.1109/ICCIKE47802.2019.9004264
81. Yang Y, Zheng X, Guo W, Liu X, Chang V. Privacy-preserving fusion of IoT and big data for e-health. *Future Generation Computer Systems* 2018;86:1437–1455. PMID:130223170
82. Conger S, Pratt JH, Loch KD. Personal information privacy and emerging technologies. *Information Systems Journal* 2013;23(5):401–417. doi: 10.1111/j.1365-2575.2012.00402.x
83. Acquisti A, Brandimarte L, Loewenstein G. Privacy and human behavior in the age of information. *Science* (1979) 2015;347(6221):509–514. doi: 10.1126/science.aaa1465
84. Harzing A-W. *Journal Quality List*. 69 Edition. 2022. Available from: <https://harzing.com/resources/journal-quality-list> [accessed Aug 4, 2022]
85. Mothersbaugh DL, Foxx WK, Beatty SE, Wang S. Disclosure antecedents in an online service context: the role of sensitivity of information. *J Serv Res* SAGE Publications Inc; 2011;15(1):76–98.

- doi: 10.1177/1094670511424924
86. Beldad A, de Jong M, Steehouder M. I trust not therefore it must be risky: Determinants of the perceived risks of disclosing personal data for e-government transactions. *Comput Human Behav* 2011;27(6):2233–2242. doi: 10.1016/j.chb.2011.07.002
 87. Van Zoonen L. Privacy concerns in smart cities. *Gov Inf Q* 2016;33(3):472–480. PMID:118421862
 88. The Insight Partners. Augmented reality and virtual reality market size & share report 2028. The Insight Partners; 2022. Available from: <https://www.theinsightpartners.com/reports/augmented-reality-and-virtual-reality-market> [accessed Aug 4, 2022]
 89. Hayes JL, Brinson NH, Bott GJ, Moeller CM. The influence of consumer–brand relationship on the personalized advertising privacy calculus in social media. *Journal of Interactive Marketing* 2021;55(1):16–30. doi: 10.1016/j.intmar.2021.01.001
 90. Rychwalska A, Roszczyńska-Kurasińska M, Domaradzka A. Right to privacy in the context of the privacy paradox and data collection patterns: exploratory study of polish Facebook users. *Proceedings of the 55th Hawaii International Conference on System Sciences* 2022. doi: 10.24251/HICSS.2022.338
 91. Wirth J, Maier C, Laumer S, Weitzel T. Laziness as an explanation for the privacy paradox: a longitudinal empirical investigation. *Internet Research* 2022;32(1):24–54. PMID:154834846
 92. Xie W, Karan K. Consumers' privacy concern and privacy protection on social network sites in the era of big data: empirical evidence from college students. *Journal of Interactive Advertising* Routledge; 2019;19(3):187–201. PMID:140940080
 93. Agesilaou A, Kyza EA. Whose data are they? Elementary school students' conceptualization of data ownership and privacy of personal digital data. *Int J Child Comput Interact* 2022;33:100462. doi: 10.1016/j.ijcci.2022.100462
 94. Keen C. Apathy, convenience or irrelevance? Identifying conceptual barriers to safeguarding children's data privacy. *New Media Soc* 2022;24(1):50–69. doi: 10.1177/1461444820960068
 95. Xie W, Kang C. See you, see me: Teenagers' self-disclosure and regret of posting on social network site. *Comput Human Behav* 2015;52:398–407. doi: 10.1016/j.chb.2015.05.059
 96. Marwick A, Fontaine C, Boyd D. “Nobody sees it, nobody gets mad”: social media, privacy, and personal responsibility among low-SES youth. *Soc Media Soc* 2017;3(2):2056305117710455. doi: 10.1177/2056305117710455
 97. Melumad S, Meyer R. Full disclosure: how smartphones enhance consumer self-disclosure. *J Mark* 2020;84(3):28–45. doi: 10.1177/0022242920912732
 98. Puntoni S, Reczek RW, Giesler M, Botti S. Consumers and Artificial Intelligence: an experiential perspective. *J Mark SAGE Publications Inc*; 2020;85(1):131–151. doi: 10.1177/0022242920953847
 99. Bartel Sheehan K. An investigation of gender differences in on-line privacy concerns and resultant behaviors. *Journal of Interactive Marketing* 1999;13(4):24–38. doi: 10.1002/(sici)1520-6653(199923)13:4<24::Aid-dir3>3.0.Co;2-o
 100. Culnan MJ, Armstrong PK. Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization science* 1999;10(1):104–115. doi: 10.1287/orsc.10.1.104
 101. Dinev T, Hart P. Internet privacy concerns and their antecedents - measurement validity and a regression model. *Behaviour & Information Technology* Taylor & Francis; 2004;23(6):413–422. doi: 10.1080/01449290410001715723
 102. Milne GR, Pettinico G, Hajjat FM, Markos E. Information sensitivity typology: Mapping the degree and type of risk consumers perceive in personal data sharing. *Journal of Consumer Affairs* John Wiley & Sons, Ltd; 2017;51(1):133–161. doi: 10.1111/joca.12111
 103. Swani K, Milne GR, Slepchuk AN. Revisiting trust and privacy concern in consumers' perceptions of marketing information management practices: replication and extension. *Journal of Interactive Marketing* 2021;56:137–158. doi: 10.1016/j.intmar.2021.03.001
 104. Wieringa J KPMXRTRHSB. Data analytics in a privacy-concerned world. *J Bus Res* 2021;122:915–925. doi: 10.1016/j.jbusres.2019.05.005

105. Hermes S, Sutanrikulu A, Schreieck M, Krcmar H. Who quits privacy-invasive online platform operators? a segmentation study with implications for the privacy paradox. 54th Hawaii International Conference on Systems Sciences Kauai, Hawaii, USASS; 2021. p. 1–10. doi: 10.24251/HICSS.2021.564
106. Lee H, Kobsa A. Understanding user privacy in Internet of Things environments. 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT) Reston, VA, USA; 2016. p. 407–412. doi: 10.1109/WF-IoT.2016.7845392
107. Lutz C, Newlands G. Privacy and smart speakers: A multi-dimensional approach. *Information Society* 2021;37(3):147–162. PMID:150389309
108. Marmion V, Millard DE, Gerding EH, Stevenage S V. The willingness of crowds: cohort disclosure preferences for personally identifying information. *Proceedings of the International AAAI Conference on Web and Social Media* 2019;13(01):358–368. doi: 10.1609/icwsm.v13i01.3236
109. Malhotra NK, Kim SS, Agarwal J. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information systems research INFORMS*; 2004;15(4):336–355. doi: 10.1287/isre.1040.0032
110. Phelps J, Nowak G, Ferrell E. Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing American Marketing Association*; 2000;19(1):27–41. doi: 10.1509/jppm.19.1.27.16941
111. Carignani A, Gemmo V. New media and privacy the privacy paradox in the digital world: i will not disclose my data. Actually, i will... it depends. *International Journal of Computer (IJC)* 2018;27(1):201–212.
112. Cichy P, Salge TO, Kohli R. Privacy concerns and data sharing in the internet of things. Mixed methods evidence from connected cars. *MIS Quarterly MIS Quarterly*; 2021;45(4):1863–1891. PMID:153886347
113. Markos E, Milne GR, Peltier JW. Information sensitivity and willingness to provide continua: a comparative privacy study of the United States and Brazil. *Journal of Public Policy & Marketing* 2017;36(1):79–96. doi: 10.1509/jppm.15.159
114. Lee H, Kobsa A. Privacy preference modeling and prediction in a simulated campuswide IoT environment. 2017 IEEE International Conference on Pervasive Computing and Communications (PerCom) 2017. p. 276–285. doi: 10.1109/PERCOM.2017.7917874
115. Brough AR, Norton DA, Sciarappa SL, John LK. The bulletproof glass effect: unintended consequences of privacy notices. *Journal of Marketing Research* 2022;59(4):739–754. doi: 10.1177/00222437211069093
116. Easwara Moorthy A, Vu K-PL. Privacy concerns for use of voice activated personal assistant in the public space. *Int J Hum Comput Interact Taylor & Francis Ltd*; 2015;31(4):307–335. PMID:101893134
117. Aguirre E, Mahr D, Grewal D, de Ruyter K, Wetzels M. Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness. *Journal of Retailing* 2015;91(1):34–49. doi: 10.1016/j.jretai.2014.09.005
118. Xu H, Luo X, Carroll JM, Rosson MB. The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decis Support Syst* 2011;51(1):42–52. doi: 10.1016/j.dss.2010.11.017
119. Zarifis A, Kawalek P, Azadegan A. Evaluating if trust and personal information privacy concerns are barriers to using health insurance that explicitly utilizes AI. *Journal of Internet Commerce Taylor & Francis Ltd*; 2021;20(1):66–83. PMID:148277461
120. Bornschein R, Schmidt L, Maier E. The effect of consumers' perceived power and risk in digital information privacy: the example of cookie notices. *Journal of Public Policy & Marketing* 2020;39(2):135–154. doi: 10.1177/0743915620902143
121. Pal D, Zhang X, Siyal S. Prohibitive factors to the acceptance of Internet of Things (IoT) technology in society: A smart-home context using a resistive modelling approach. *Technol Soc*

- 2021;66:101683. doi: 10.1016/j.techsoc.2021.101683
122. Jeon H, Lee C. Internet of Things technology: balancing privacy concerns with convenience. *Telematics and Informatics* 2022;70:101816. doi: 10.1016/j.tele.2022.101816
123. Rajaobelina L, Prom Tep S, Arcand M, Ricard L. Creepiness: Its antecedents and impact on loyalty when interacting with a chatbot. *Psychol Mark* 2021;38(12):2339–2356. PMID:153385698
124. Marakhimov A, Joo J. Consumer adaptation and infusion of wearable devices for healthcare. *Comput Human Behav* 2017;76:135–148. doi: 10.1016/j.chb.2017.07.016
125. Casselman J, Onopa N, Khansa L. Wearable healthcare: Lessons from the past and a peek into the future. *Telematics and Informatics* 2017;34(7):1011–1023. doi: 10.1016/j.tele.2017.04.011
126. Cheng Y, Jiang H. How do AI-driven chatbots impact user experience? Examining gratifications, perceived privacy risk, satisfaction, loyalty, and continued use. *J Broadcast Electron Media* 2020;64(4):592–614. PMID:148772709
127. Maltseva K, Lutz C. A quantum of self: A study of self-quantification and self-disclosure. *Comput Human Behav* 2018;81:102–114. doi: 10.1016/j.chb.2017.12.006
128. Faqih KMS. Factors influencing the behavioral intention to adopt a technological innovation from a developing country context: The case of mobile augmented reality games. *Technol Soc* 2022;69:101958. doi: 10.1016/j.techsoc.2022.101958
129. Aleisa N, Renaud K, Bongiovanni I. The privacy paradox applies to IoT devices too: A Saudi Arabian study. *Comput Secur* 2020;96:101897. doi: 10.1016/j.cose.2020.101897
130. Yavuz M, Çorbacioğlu E, Başoğlu AN, Daim TU, Shaygan A. Augmented reality technology adoption: Case of a mobile application in Turkey. *Technol Soc* 2021;66:101598. doi: 10.1016/j.techsoc.2021.101598
131. Gupta S, Kamboj S, Bag S. Role of risks in the development of responsible artificial intelligence in the digital healthcare domain. *Information Systems Frontiers* 2021; doi: 10.1007/s10796-021-10174-0
132. Liu Y, Yan W, Hu B. Resistance to facial recognition payment in China: The influence of privacy-related factors. *Telecomm Policy* 2021;45(5):N.PAG-N.PAG. PMID:150083802
133. Pentina I, Zhang L, Bata H, Chen Y. Exploring privacy paradox in information-sensitive mobile app adoption: A cross-cultural comparison. *Comput Human Behav* 2016;65:409–419. doi: 10.1016/j.chb.2016.09.005
134. Deutsch M. *Distributive justice: A social-psychological perspective*. New Haven: Yale University Press; 1985. ISBN:0300032900
135. Pizzi G, Scarpi D. Privacy threats with retail technologies: A consumer perspective. *Journal of Retailing and Consumer Services* 2020;56:102160. doi: 10.1016/j.jretconser.2020.102160
136. Laufer RS, Wolfe M. Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of social Issues* 1977;33(3):22–42. doi: 10.1111/j.1540-4560.1977.tb01880.x
137. Attié E, Meyer-Waarden L. The acceptance and usage of smart connected objects according to adoption stages: an enhanced technology acceptance model integrating the diffusion of innovation, uses and gratification and privacy calculus theories. *Technol Forecast Soc Change* 2022;176:121485. doi: 10.1016/j.techfore.2022.121485
138. Gao Y, Li H, Luo Y. *An empirical study of wearable technology acceptance in healthcare*. Industrial Management & Data Systems Emerald Group Publishing Limited; 2015;115(9):1704–1723. doi: 10.1108/IMDS-03-2015-0087
139. Kang H, Jung EH. *The smart wearables-privacy paradox: A cluster analysis of smartwatch users*. Behaviour & Information Technology Taylor & Francis; 2021;40(16):1755–1768. doi: 10.1080/0144929X.2020.1778787
140. Kim D, Park K, Park Y, Ahn J-H. Willingness to provide personal information: Perspective of privacy calculus in IoT services. *Comput Human Behav* 2019;92:273–281. doi: 10.1016/j.chb.2018.11.022
141. Lavado-Nalvaiz N, Lucia-Palacios L, Pérez-López R. The role of the humanisation of smart home

- speakers in the personalisation–privacy paradox. *Electron Commer Res Appl* 2022;53:101146. doi: 10.1016/j.elerap.2022.101146
142. Willems J, Schmid MJ, Vanderelst D, Vogel D, Ebinger F. AI-driven public services and the privacy paradox: do citizens really care about their privacy? *Public Management Review* 2022;1–19. PMID:156274710
143. Rogers RW. A protection motivation theory of fear appeals and attitude change1. *J Psychol* Routledge; 1975;91(1):93–114. doi: 10.1080/00223980.1975.9915803
144. Alashoor T, Han S, Joseph RC. Familiarity with big data, privacy concerns, and self-disclosure accuracy in social networking websites: an APCO model. *Communications of the Association for Information Systems Association for Information Systems*; 2017;41:62–96. PMID:124670672
145. Thongmak M. Protecting privacy in Pokémon Go: A multigroup analysis. *Technol Soc* 2022;70:101999. doi: 10.1016/j.techsoc.2022.101999
146. Williams M, Nurse JRC, Creese S. (Smart) watch out! encouraging privacy-protective behavior through interactive games. *Int J Hum Comput Stud* 2019;132:121–137. doi: 10.1016/j.ijhcs.2019.07.012
147. Blau PM. Exchange and power in social life. 2nd ed. New York: Routledge; 1986. ISBN:9780887386282
148. Homans GC. Social behavior and its elementary forms. New York: Harcourt, Brace and World; 1961. ISBN:9780710074829
149. Uysal E, Alavi S, Bezençon V. Trojan horse or useful helper? A relationship perspective on artificial intelligence assistants with humanlike features. *J Acad Mark Sci* 2022;1–23. PMID:155890408
150. Davis FD. A technology acceptance model for empirically testing new end-user information systems: Theory and results. Massachusetts Institute of Technology; 1985.
151. Liu K, Tao D. The roles of trust, personalization, loss of privacy, and anthropomorphism in public acceptance of smart healthcare services. *Comput Human Behav* 2022;127:107026. doi: 10.1016/j.chb.2021.107026
152. Park SS, Tung CD, Lee H. The adoption of AI service robots: A comparison between credence and experience service settings. *Psychol Mark* John Wiley & Sons, Inc.; 2021;38(4):691–703. PMID:149132716
153. Ajzen I. From intentions to actions: A theory of planned behavior. *Action control* Heidelberg: Springer; 1985. p. 11–39. ISBN:9783642697487
154. Ajzen I, Fishbein M. Understanding attitudes and predicting social behavior. Englewood Cliffs, NJ: Prentice-Hall; 1980. ISBN:013050369X
155. Fishbein M, Ajzen I. Belief, attitude, intention, and behavior: An introduction to theory and research. *Philosophy and Rhetoric* 1977;10(2). doi: 9780201020892
156. Bawack RE, Wamba SF, Carillo KDA. Exploring the role of personality, trust, and privacy in customer experience performance during voice shopping: Evidence from SEM and fuzzy set qualitative comparative analysis. *Int J Inf Manage* 2021;58:102309. doi: 10.1016/j.ijinfomgt.2021.102309
157. Venkatesh V, Morris MG, Davis GB, Davis FD. User acceptance of information technology: toward a unified view. *MIS Quarterly Management Information Systems Research Center, University of Minnesota*; 2003;27(3):425–478. doi: 10.2307/30036540
158. Vimalkumar M, Sharma SK, Singh JB, Dwivedi YK. ‘Okay google, what about my privacy?’: User’s privacy perceptions and acceptance of voice based digital assistants. *Comput Human Behav* 2021;120:106763. doi: 10.1016/j.chb.2021.106763
159. Petronio S. Communication boundary management: A theoretical model of managing disclosure of private information between marital couples. *Communication theory* 1991;1(4):311–335. doi: 10.1111/j.1468-2885.1991.tb00023.x
160. Petronio S. Boundaries of privacy: Dialectics of disclosure. Suny Press; 2002. ISBN:0791455157
161. Petronio S. Communication boundary management: A theoretical model of managing disclosure of

- private information between marital couples. *Communication Theory* 2006;1(4):311–335. doi: 10.1111/j.1468-2885.1991.tb00023.x
162. Cao G, Wang P. Revealing or concealing: privacy information disclosure in intelligent voice assistant usage- a configurational approach. *Industrial Management & Data Systems* 2022;122(5):1215–1245. PMID:156843002
163. Kathuria R, Kathuria V. Role of privacy management and human-centered Artificial Intelligence in driving customer engagement with smart speakers. In: Stephanidis C, Antona M, Ntoa S, editors. *HCI International 2022 Posters* Cham: Springer International Publishing; 2022. p. 412–418. doi: 10.1007/978-3-031-06417-3_55
164. Harborth D, Pape S. Investigating privacy concerns related to mobile augmented reality apps – a vignette based online experiment. *Comput Human Behav* 2021;122:106833. doi: 10.1016/j.chb.2021.106833
165. Lazarus RS, Folkman S. *Stress, appraisal, and coping*. Springer publishing company; 1984. ISBN:0826141927
166. Chaiken S. Heuristic versus systematic information processing and the use of source versus message cues in persuasion. *J Pers Soc Psychol* 1980;39(5):752–766. doi: 10.1037/0022-3514.39.5.752
167. Shin D. User perceptions of algorithmic decisions in the personalized AI system: perceptual evaluation of fairness, accountability, transparency, and explainability. *J Broadcast Electron Media* Routledge; 2020;64(4):541–565. doi: 10.1080/08838151.2020.1843357
168. Ram S. A model of innovation resistance. *ACR North American Advances* 1987; doi: 10.5130/AJCEB.v16i3.5164
169. Ram S. Successful innovation using strategies to reduce consumer resistance an empirical test. *Journal of Product Innovation Management: An International Publication of the Product Development & Management Association* 1989;6(1):20–34. doi: 10.1016/0737-6782(89)90011-8
170. Kahneman D, Tversky A. Prospect theory: An analysis of decision under risk. *Econometrica* [Wiley, Econometric Society]; 1979;47(2):263–291. doi: 10.2307/1914185
171. Kahneman D, Tversky A. Prospect theory: An analysis of decision under risk. *Handbook of the fundamentals of financial decision making: Part I* World Scientific; 2013. p. 99–127. doi: 10.2307/1914185
172. Jain S, Basu S, Dwivedi YK, Kaur S. Interactive voice assistants – Does brand credibility assuage privacy risks? *J Bus Res* 2022;139:701–717. PMID:154012186
173. Spence M. *Market signaling: Informational transfer in hiring and related screening processes*. Cambridge: Harvard University Press; 1974. ISBN:0674549902
174. Bandura A. *Social foundations of thought and action*. Englewood Cliffs, NJ. 1986. ISBN:9780138156145
175. Mori M. The uncanny valley: the original essay by Masahiro Mori. *IEEE Spectr* 1970;
176. Mori M, MacDorman KF, Kageki N. The uncanny valley [from the field]. *IEEE Robot Autom Mag* 2012;19(2):98–100. doi: 1109/MRA.2012.2192811
177. Katz E, Blumler JG. *The uses of mass communications: Current perspectives on gratifications research*. Beverly Hills, CA: Sage; 1974. ISBN:0803903405
178. Katz E, Blumler JG, Gurevitch M. *Uses and gratifications research*. *The public opinion quarterly* 1973;37(4):509–523. doi: 10.1086/268109
179. McLean G, Osei-Frimpong K. Hey Alexa ... examine the variables influencing the use of artificial intelligent in-home voice assistants. *Comput Human Behav* 2019;99:28–37. doi: 10.1016/j.chb.2019.05.009
180. Rauschnabel PA, He J, Ro YK. Antecedents to the adoption of augmented reality smart glasses: A closer look at privacy risks. *J Bus Res* 2018;92:374–384. doi: 10.1016/j.jbusres.2018.08.008
181. Gray HM, Gray K, Wegner DM. Dimensions of mind perception. *Science* (1979) 2007;315(5812):619. doi: 10.1126/science.1134475
182. Johnson EJ, Häubl G, Keinan A. Aspects of endowment: a query theory of value construction. *J Exp*

- Psychol Learn Mem Cogn 2007;33(3):461. doi: 10.1037/0278-7393.33.3.461
183. Sun Q, Willemsen MC, Knijnenburg BP. Unpacking the intention-behavior gap in privacy decision making for the internet of things (IoT) using aspect listing. *Comput Secur* 2020;97:101924. doi: 10.1016/j.cose.2020.101924
 184. Rogers EM. *Diffusion of innovations*. New York: Free Press of Glencoe; 1962. ISBN:0029266505
 185. Rogers EM, Singhal A, Quinlan MM. *Diffusion of innovations. An integrated approach to communication theory and research* Routledge; 2014. p. 432–448. ISBN:0203887018
 186. Harsanyi JC. Games with incomplete information played by “bayesian” players, I–III part I. the basic model. *Manage Sci* 1967;14(3):159–182. doi: 10.1287/mnsc.14.3.159
 187. Simon HA. *Models of bounded rationality: Empirically grounded economic reason*. MIT press; 1982. ISBN:0262193728
 188. Lutz C, Tamó-Larrieux A. The robot privacy paradox: Understanding how privacy concerns shape intentions to use social robots. *Human-Machine Communication* 2020;1:87–111. doi: 10.30658/hmc.1.6
 189. Chaparro Osman M, Nakushian A, Rebensky S, Prior T, Carroll M. User experience, knowledge, perceptions, and behaviors associated with Internet of Things (IoT) device information privacy. In: Moallem A, editor. *HCI for Cybersecurity, Privacy and Trust* Cham: Springer International Publishing; 2022. p. 107–123. doi: 10.1007/978-3-031-05563-8_8
 190. Jaspers EDT, Pearson E. Consumers’ acceptance of domestic Internet-of-Things: The role of trust and privacy concerns. *J Bus Res* 2022;142:255–265. PMID:155288753
 191. Pal D, Arpnikanondt C, Razzaque MA. Personal information disclosure via voice assistants: the personalization–privacy paradox. *SN Comput Sci* 2020;1(5):280. doi: 10.1007/s42979-020-00287-9
 192. Menard P, Bott GJ. Analyzing IOT users’ mobile device privacy concerns: Extracting privacy permissions using a disclosure experiment. *Comput Secur* 2020;95:101856. doi: 10.1016/j.cose.2020.101856
 193. Bandara R, Fernando M, Akter S. The privacy paradox in the data-driven marketplace: the role of knowledge deficiency and psychological distance. *Procedia Comput Sci* 2017;121:562–567. doi: 10.1016/j.procs.2017.11.074
 194. Barth S, de Jong MDT, Junger M, Hartel PH, Roppelt JC. Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and Informatics* 2019;41:55–69. doi: 10.1016/j.tele.2019.03.003
 195. Anto A, Basu A, Selim R, Foscht T, Eisingerich AB. Open-world games’ affordance of cognitive escapism, relaxation, and mental well-being among postgraduate students: mixed methods study. *J Med Internet Res* 2024;26:e63760. doi: 10.2196/63760
 196. Duffek B, Eisingerich AB, Merlo O. Why so toxic? A framework for exploring customer toxicity. *AMS Review* 2023 Jun 1;13:122–143. doi: 10.1007/s13162-023-00257-3
 197. Hartnup B, Dong L, Eisingerich AB. How an environment of stress and social risk shapes student engagement with social media as potential digital learning platforms: qualitative study. *JMIR Med Educ* 2018;4(2):e10069. doi: 10.2196/10069
 198. Heinberg M, Liu Y, Huang X, Eisingerich AB. A bad job of doing good: does corporate transparency on a country and company level moderate corporate social responsibility effectiveness? *Journal of International Marketing* 2020 Nov 25; doi: 10.1177/1069031X20981870
 199. Liu S, Guo LR. Data ownership in the AI-Powered integrative health care landscape. *JMIR Med Inform. JMIR Publications Inc.*; 2024. doi: 10.2196/57754
 200. Merlo O, Eisingerich AB, Shin HK, Britton RA. Avoiding the pitfalls of customer participation. *MIT Sloan Manag Rev* 2019;1:61. Available from: <https://sloanreview.mit.edu/article/avoiding-the-pitfalls-of-customer-participation/> [accessed Jan 16, 2025]
 201. Selim R, Basu A, Anto A, Foscht T, Eisingerich AB. Effects of Large Language Model–based offerings on the well-Being of students: qualitative study. *JMIR Form Res* 2024;8:e64081. doi: 10.2196/64081

202. Sun X, Foscht T, Kerschbaumer R, Eisingerich AB. "Pulling back the curtain": Company tours as a customer education tool and effects on pro-brand behaviors. *Journal of Consumer Behaviour* 2022 Jul 17;21. doi: 10.1002/cb.2088
203. Sun X, Eisingerich AB, Foscht T, Cui X, Schloffer J. Why do customers want to learn? Antecedents and outcomes of customer learning. *Eur J Mark* 2022 Mar 14;ahead-of-print. doi: 10.1108/EJM-04-2020-0302
204. Tudor-Sfetea C, Rabee R, Najim M, Amin N, Chadha M, Jain M, Karia K, Kothari V, Patel T, Suseeharan M, Ahmed M, Sherwani Y, Siddiqui S, Lin Y, Eisingerich AB. Evaluation of two mobile health apps in the context of smoking cessation: qualitative study of Cognitive Behavioral Therapy (CBT) versus non-CBT-based digital solutions. *JMIR Mhealth Uhealth* 2018;6(4):e98. doi: 10.2196/mhealth.9405
205. Rollwage M, Habicht J, Juechems K, Carrington B, Viswanathan S, Stylianou M, Hauser TU, Harper R. Using conversational AI to facilitate mental health assessments and improve clinical efficiency within psychotherapy services: Real-world observational study. *JMIR AI* JMIR Publications Inc.; 2023 Dec 13;2:e44358. doi: 10.2196/44358
206. Puntoni S, Reczek RW, Giesler M, Botti S. Consumers and artificial intelligence: An experiential perspective. *J Mark* 2021;85(1):131–151. doi: 10.1177/0022242920953847
207. Iyengar SS, Lepper MR. When choice is demotivating: Can one desire too much of a good thing? *J Pers Soc Psychol* 2000;79(6):995. doi: 10.1037/0022-3514.79.6.995
208. Thaler RH, Benartzi S. Save more tomorrowTM: Using behavioral economics to increase employee saving. *Journal of political Economy* 2004;112(S1):S164–S187. doi: 10.1086/380085
209. Lobschat L, Mueller B, Eggers F, Brandimarte L, Diefenbach S, Kroschke M, Wirtz J. Corporate digital responsibility. *J Bus Res* 2021;122:875–888. doi: 10.1016/j.jbusres.2019.10.006
210. Saeidi SP, Sofian S, Saeidi P, Saeidi SP, Saeidi SA. How does corporate social responsibility contribute to firm financial performance? The mediating role of competitive advantage, reputation, and customer satisfaction. *J Bus Res* 2015;68(2):341–350. doi: 10.1016/j.jbusres.2014.06.024

Supplementary Files

PRISMA checklist.

URL: <http://asset.jmir.pub/assets/6b4a3c236f4815e0ff5e252741f6eb77.docx>

Multimedia Appendixes

Untitled.

URL: <http://asset.jmir.pub/assets/9819dea8311a46ce3220280a9c94951c.docx>