Communications of the Association for Information Systems

Volume 57 Paper 13

8-5-2025

# Privacy in Smart Health Monitoring: A Systematic Review and Research Directions

Jingjing Zhang
*Auckland University of Technology*, jingjing.zhang@autuni.ac.nz

Farkhondeh Hassandoust
*The University of Auckland*

Allen C. Johnston
*The University of Alabama*



Recommended Citation
Zhang, J., Hassandoust, F., & Johnston, A. C. (2025). Privacy in Smart Health Monitoring: A Systematic Review and Research Directions. Communications of the Association for Information Systems, 57, 318-364. https://doi.org/10.17705/1CAIS.05713

# Privacy in Smart Health Monitoring: A Systematic Review and Research Directions

## Cover Page Footnote

This manuscript underwent peer review. It was received 05/05/2025 and was with the authors for 12 months for three revisions. Stephen McCarthy served as Associate Editor.

Communications of the Association for Information Systems

Research Article DOI: 10.17705/1CAIS.05713 ISSN: 1529-3181

# Privacy in Smart Health Monitoring: A Systematic Review and Research Directions

**Jingjing Zhang**
Department of Management, Technology, and Organization
Auckland University of Technology
New Zealand
*jingjing.zhang@autuni.ac.nz*
0000-0002-6842-3291

**Farkhondeh Hassandoust**
Department of Information Systems and Operation Management
The University of Auckland
New Zealand
0000-0001-7190-9527

**Allen C. Johnston**
Department of Information Systems, Statistics, & Management Science
Culverhouse College of Business
The University of Alabama
USA
0000-0003-0301-4187

**Abstract:**

Privacy concerns related to surveillance technologies are a primary deterrent for consumers hesitant to share their health data with service providers in smart health monitoring systems (SHMSs). These concerns can impede the adoption and operational success of SHMSs, leading to dissatisfaction among both consumers and service providers. Despite the significance of privacy, existing literature on SHMSs tends to offer a somewhat fragmented exploration of this concept due to the complex nature of surveillance and the involvement of multiple stakeholders. To address this gap, this study develops a contextual framework based on a systematic review of 49 peer-reviewed articles, offering valuable insights for scholars seeking to understand the multifaceted privacy concerns in SHMS contexts. The findings emphasize the importance of integrating theoretical perspectives that better capture the intricate dynamics of smart health environments, helping healthcare providers and policymakers identify and address potential privacy issues when developing and implementing surveillance systems for personal health information. Additionally, the study highlights existing knowledge gaps and proposes six research avenues to achieve a deeper understanding of privacy in SHMSs.

**Keywords:** Privacy, Contextualization, Smart Health Monitoring, Stakeholders, Surveillance, Systematic Literature Review.

This manuscript underwent peer review. It was received 05/05/2025 and was with the authors for 12 months for three revisions. Stephen McCarthy served as Associate Editor.

# 1 Introduction

Digital surveillance technologies, such as facial recognition systems and data-tracking algorithms, leverage sophisticated methods to collect, process, and exploit personal data used by both governments and corporations to monitor individuals, predict behaviors, and target consumers (Clarke, 2019). The emergence of these technologies has had significant implications for the global economy, introducing new business models, processes, and stakeholders that collect and analyze data to form an understanding of individuals' electronic behaviors (Clarke, 2019; Lyon, 2003, 2007). Recent estimates valued the global digital surveillance market at USD $81.68 billion in 2024, and it is projected to reach USD $145.38 billion by 2029, growing at a compound annual growth rate (CAGR) of 12.22% during the forecasted period. This rapid expansion underscores the growing demand for digital surveillance technologies across various sectors, driven by heightened security needs and advancements in artificial intelligence (AI) and the Internet of Things (IoT) (Grand View Research, 2023; Mordor Intelligence, 2024).

One particularly pervasive form of digital surveillance technologies is smart health monitoring systems (SHMSs), which use real-time surveillance and sensor-based smart health applications to monitor the vital signs and daily health status of their users (Alabdulatif et al., 2019; Almujally et al., 2023; Zuboff, 2019). SHMSs have seen significant growth in recent years due to their anticipated advantages, such as promoting communication between patients and doctors, improving diagnostic and treatment processes, reducing professional visit costs, and enhancing personal care quality (Akmandor & Jha, 2018; Greco et al., 2020). It is estimated that the global SHMS market will reach USD $474 billion by 2032 (GlobeNewswire, 2023; Market.Us, 2023).

Despite significant investments in SHMSs and their anticipated advantages, these systems also raise significant privacy concerns due to the embedded surveillance technologies that monitor and collect personal health data. Digital surveillance impacts individuals both psychologically and socially, as intensive surveillance discourages certain behaviors, erodes personal autonomy, and limits the space for self-determination (Clarke, 1994, 2019). Moreover, concerns about data privacy resulting from these surveillance technologies have led to low adoption levels among both consumers and health professionals (Arbabi et al., 2022; Essén, 2008; Peek et al., 2016). Multiple global reports (e.g., Accenture.com, 2020; Capterra.com, 2021; Fortune.com, 2023; New Zealand IoT Alliance, 2017) point to consumers' privacy concerns related to SHMSs as the key reason preventing them from using health monitoring applications and sharing their health data with health professionals. These surveillance technologies include devices such as electrocardiogram ECG monitors and blood glucose wearables, which are essential to the efficacy of SHMSs (Rashidi & Mihailidis, 2013; Stavropoulos et al., 2020), but evoke confusion or uncertainty among SHMS consumers about who bears responsibility in the event of the loss of their health data, and how the proper protection and usage of this data within the surveillance framework can be guaranteed (Accenture.com, 2020; Duckert & Barkhuus, 2022; Princi & Krämer, 2020).

For scholars, the juxtaposition of the growth and potential of SHMSs with consumer concerns for privacy represents an intriguing phenomenon to research. However, while investigations into the impact of consumers' privacy concerns on their willingness to adopt and utilize SHMSs may seem appealing, the extant SHMS literature available to inform such work presents a rather limited and fractured perspective on privacy in the context of surveillance and monitoring. Privacy is a multidisciplinary concept (Smith et al., 2011), and privacy researchers in the general field of information systems (IS) have embraced diverse perspectives in defining and investigating various privacy issues for different purposes. For instance, privacy has been defined as a *right* to be alone from a legal perspective (Warren & Brandeis, 1890), as a *commodity* that can be traded for benefits in an economic sense (Campbell & Carlson, 2002; Smith et al., 2011), as a *control* over the acquisition and use of personal information, signifying an individual's ability to manage these aspects (Culnan & Bies, 2003), and as a *state* or condition that indicates restricted access to personal information (Schoeman, 1984). This plurality of perspectives has served the IS discipline well, but in terms of understanding privacy as a byproduct concern of SHMS surveillance activities, prior researchers do not identify their perspective(s) of interest. As a result, the overall body of literature that informs SHMS privacy research seems incomplete and incoherent.

Privacy in SHMSs is a complex, multifaceted issue that cannot be fully understood through a single lens. Our study identifies four dominant privacy perspectives—privacy as a *right, control, commodity,* and *state*—that structure how privacy concerns are framed in SHMS research. These perspectives matter because they shape the assumptions, research questions, and policy implications of studies in this

domain. Without explicit recognition of these perspectives, the field remains fragmented, making it difficult for future research to build on prior work in a systematic way. By synthesizing these perspectives into a structured framework, this study provides a foundation for theoretical consistency and empirical comparability in SHMS privacy research.

While the plurality of privacy conceptualizations has enriched IS research, the absence of explicit theoretical positioning presents challenges. Studies that do not clarify their privacy perspective risk theoretical inconsistencies, making it difficult to compare findings across contexts or build cumulative knowledge (Newell, 1995; Shen et al., 2019). In SHMS research, this issue is especially pronounced, as privacy concerns extend beyond individual preferences to include the roles of healthcare providers, regulatory agencies, and technology designers. Without an explicitly stated perspective, research may overlook the ethical, legal, and technical complexities of health data protection, resulting in fragmented insights and inconsistent policy recommendations. The ambiguity may also lead to inconsistent operationalizations (Dinev et al., 2013; Xu & Zhang, 2022), where similar terminology like “privacy concerns” can mask fundamentally different constructs, misaligned theoretical frameworks, and unclear designs or policy implications. This study addresses this gap by systematically analyzing how privacy is conceptualized in SHMS research and proposing a structured framework to enhance theoretical clarity and practical applicability.

Privacy is also a context-dependent concept (Smith et al., 2011). Contexts represent differentiated social spheres serving as organizing principles that shape individual expectations of privacy (Nissenbaum, 2018; Zuboff, 2015). Individuals strive to keep perceived sensitive information private in accordance with the context of the social, professional, or institutional environment in which they are operating (Bantan & Shawosh, 2024; Nissenbaum, 2010). While individual privacy expectations vary in these environments, SHMSs represent a particularly complex context where privacy concerns are amplified by the integration of surveillance technologies. SHMSs not only monitor personal health data but also engage multiple stakeholders, including consumers, healthcare providers, government authorities, and smart technology providers, each with potentially conflicting privacy concerns (Winter & Davidson, 2019). Consumers may be primarily concerned about data misuse, while healthcare providers focus on regulatory compliance (OECD, 2015; Peek et al., 2016; Swinkels et al., 2018). Technology providers, on the other hand, may prioritize innovation over stringent data protection, further complicating the privacy landscape. As the number of stakeholders increases, so does the risk of privacy loss due to conflicting interests or concerns Swinkels et al., 2018).

Although several studies have explored individual privacy concerns in specific contexts, such as consumer surveillance worries (Chadborn et al., 2019) and medical practitioners' attitudes toward smart healthcare (Pan et al., 2019), there remains a gap in research that examines how these diverse stakeholder concerns collectively influence SHMSs. Given its critical importance to scholars and recent discourse on digital surveillance highlighting the urgent need to address the privacy risks associated with these technologies (Clarke, 2019), a contextual framework for SHMS privacy research is proposed. This framework accommodates the diverse perspectives and contextual nuances of privacy within the context of SHMSs. It is developed through a systematic review of the IS literature, revealing the existing understanding of privacy, which is then contextualized to the unique environment of SHMSs and its multiple stakeholder perspectives. The research question guiding the review process is:

**RQ: What are the key insights provided by the existing IS privacy literature that can inform the perspective on privacy in the SHMS context?**

The proposed framework for SHMS privacy research offers valuable insights to scholars interested in understanding the contextual nuances of privacy in SHMS settings. This framework can also assist both healthcare providers and policymakers in addressing privacy issues surrounding personal health information when developing and implementing healthcare surveillance systems. Furthermore, the findings uncover existing knowledge gaps and identify potential research avenues for future investigation. These avenues also respond to the existing research agenda on investigating concerns about the threats inherent in digital surveillance and formulating appropriate approaches against the backdrop of the digital surveillance economy (Clarke, 2019).

The remainder of this paper is organized as follows. First, the related work is presented to set the stage for the review, highlighting the importance of contextual clarity in IS research and the gaps where existing review articles could benefit from further exploration. Next, the systematic literature review methodology is

outlined, including article selection and coding process. Finally, the findings are presented, followed by a discussion of future implications and concluding remarks.

## 2 Related Work

Privacy researchers often assume that privacy concerns in the context of SHMSs can be mitigated through improved technology and data governance (e.g., Ahmed et al., 2024; Jaime et al., 2023). However, this view seems to overlook a comprehensive understanding of the complex nature of surveillance contexts in healthcare and its socio-ethical implications. Traditionally, the literature on SHMSs has tended to focus on a few key assumptions: that privacy can be safeguarded through technological enhancements alone (Butpheng et al., 2020), and that the primary stakeholders are often viewed as patients and healthcare providers (Renukappa et al., 2022). These assumptions could be either keen on implementing privacy protection measures and securing the healthcare system (Field assumption), fail to consider the broader socio-ethical dimensions and the diverse array of stakeholders involved in SHMSs (in-house assumption), or merely quantify privacy-related constructs to determine how well privacy is managed in the system (Methodological assumption). More additional assumptions in the context of SHMSs can be found in Table 1. Yet, as Davison and Martinsons (2016) argue, research remains incomplete unless there is a clear specification of the context for conducting the research and where the findings could be reasonably applicable. Alvesson and Sandberg (2011) advocate for a problematization approach that challenges these taken-for-granted assumptions. Based on that approach, the present study questions the adequacy of technical solutions in addressing privacy concerns. It highlights the need for a more contextual and holistic perspective that includes regulatory bodies, technology developers, and the patients themselves.

**Table 1. Additional Assumptions of Privacy in SHMSs**

| Current Assumption | Category | Alternative Assumption |
|---|---|---|
| Privacy can be effectively safeguarded through technological enhancements alone (such as encryption, access controls, and anonymization—without requiring broader social or institutional interventions). | Field | Privacy is not merely an individual concern or a technical concern, but a complex construct shaped by the broader interplay among the fields of healthcare systems, technological infrastructures, policy frameworks, and societal norms. |
| Privacy is shaped by the internal norms, standards, and objectives within the organization or team implementing SHMSs. | In-house | Privacy is understood as a broader construct governed by a diverse range of external stakeholders—including patients, healthcare providers, policymakers, technologists, and regulators—each exerting influence over how privacy is defined, negotiated, and enforced within SHMSs. |
| Although privacy is inherently difficult to measure, it can be quantitatively examined through privacy proxies and relative constructs when aiming to determine how effectively privacy is managed within SHMSs. | Methodological (Paradigm) | Privacy is assumed as a holistic construct in mixed-methods research. By integrating quantitative and qualitative techniques, researchers can capture a more nuanced and comprehensive understanding of privacy in SHMSs. |
| Privacy is a legal concept rooted in fundamental human rights, encompassing the right of individuals to be left alone. | Ontological (Paradigm) | Privacy can be assumed as a state or a condition that indicates restricted access to personal information. |
| It is often assumed that all the involved stakeholders share a uniform understanding of privacy. | Epistemological (Paradigm) | People hold diverse understandings of privacy. Privacy can be viewed as contextual knowledge, shaped by individuals' specific circumstances, cultural background, and the particular technologies they interact with. |
| Privacy is primarily conceptualized as a technical issue stemming from the surveillance technologies that serve as a significant contextual factor in enabling real-time health data collection. | Ideology | Privacy can be approached as a multi-contextual construct shaped by critical contextual factors such as surveillance mechanisms, interactions among diverse stakeholders, and other situational conditions. |

| | | |
|---|---|---|
| In the context of SHMSs, health data is often seen as a valuable resource. Privacy concerns emerge primarily when this data is collected, shared, or monetized, raising issues around consent, security, and control. | Root metaphor | Privacy itself is assumed as a tradable commodity or resource. Within this metaphor, privacy becomes an asset that individuals may choose to sell, relinquish, or safeguard, depending on the personal value they assign to it. |

Despite the importance of studying privacy from a more contextual and holistic perspective, a recent re-evaluation of the existing review studies (conducted by the current researchers) supports the assumption of an incomplete understanding of privacy issues in SHMSs (see Section 2.1). Among those review studies, the review criteria (transparency and research agenda) were not consistently reported, and the insights into privacy phenomena in healthcare surveillance contexts were relatively underexplored. Our assumptions of an incomplete understanding of privacy align with the challenges identified by other IS privacy researchers, who, in the existing literature, suggested that the specification of a context is only emphasized through a post hoc descriptive style rather than empirically examined or theoretically formulated (Xu & Zhang, 2022). To adequately contextualize privacy within SHMSs, this review begins by examining contextualized definitions of privacy. Then, this study examines contextual richness by exploring the antecedents and outcomes of privacy in SHMSs, as well as the theories and methodologies utilized in the previous literature. Considering their contextual significance, the review also pays particular attention to surveillance and stakeholders to provide a complete picture of privacy contextualization within the context of smart health monitoring.

As part of this context-specific exploration, the existing review studies on privacy issues in the smart health monitoring context were re-evaluated. These review articles were scoped using search terms related to ‘privacy’ and ‘smart health.’ In brief, this meta-review showed that the review criteria (transparency and research agenda) were not consistently provided. Establishing criteria such as search strategy and formulating a research agenda are foundational elements of methodological transparency. They are essential for the advancement of knowledge in a particular research field and for maximizing research impact (Paré et al., 2016; Wagner et al., 2021). As shown in Table A1 (in Appendix A), these review papers offer valuable avenues for understanding privacy phenomena in healthcare surveillance contexts, though opportunities remain for deeper exploration. For example, only a few review papers analyzed the contextual definitions of privacy in their study settings. The underlying theoretical models and theories were not evaluated. Few papers reviewed antecedents and outcomes of privacy, and even fewer discussed research agendas. The meta-review findings strongly underscore the need for a more comprehensive review to address the above-mentioned gaps in previous review studies, allowing researchers and stakeholders (e.g., practitioners) to derive a more informed interpretation and conclusion on privacy concerns related to SHMSs. This review study aims to rectify these gaps in the literature by providing a comprehensive review of privacy contextualization in SHMSs. It includes examining privacy definitions from various perspectives and reviewing antecedents and outcomes of privacy, relevant theories, methodological transparency, research agenda, and other pertinent scopes.

# 3 Method

A literature review helps address broad questions through a holistic review approach, providing a complete picture of the prevalence of research on a focal topic (Grant & Booth, 2009). It is “a form of secondary study that uses a well-defined methodology to identify, analyze and interpret all available evidence related to a specific research question in a way that is unbiased and (to a degree) repeatable” (Kitchenham & Charters, 2007, p. vi). It also ensures accuracy and impartiality in the search and retrieval process while supporting the development of future research guidelines or directions that professionals can use (Fernández-Alemán et al., 2013). To answer the research question posited in this review and identify directions for future research, a systematic literature review focusing on privacy in smart health monitoring studies was conducted. Completing a systematic literature review is an iterative process that depends on the quality and scope of the included studies (Moher et al., 2009). Based on the Preferred Reporting Items for Systematic Review (PRISMA) guidelines (Moher et al., 2009), the search strategy, study selection, and the data collection and thematic analysis process are explained in the following sections.

## 3.1 Search Strategy

The present study focused on peer-reviewed journal articles and conference papers written in English. Given that the concept of smart health monitoring emerged in early 2000 (Meier et al., 2013; Pan et al.,

2019), this study considered articles published between January 2000 and February 2024. The search utilized the databases of Scopus, Science Direct, JSTOR, IEEE Xplore, Emerald Insight, EBSCO-host, ACM Digital Library, and AIS eLibrary. Other sources, including PubMed and OVID, were also used to identify relevant articles. Using keywords aligned with the research question, the search primarily targeted articles related to 'privacy' and 'smart health.' Given the distinctive feature of smart health monitoring technology, the search was purposefully focused on the term 'surveillance.' However, 'surveillance' may be excessively restrictive since many articles can use alternative terms for surveillance such as 'monitor,' 'track,' or 'detect.' Thus, the term 'monitor' was also searched as it is widely used, in order to identify as many potentially relevant studies as possible. In sum, the search query strings were 'privacy,' 'smart health,' 'surveillance,' and 'monitor.' Details of inclusion and exclusion criteria are presented in Table 2. To further enhance the clarity of the data collection strategy and processes, a 27-item checklist is provided in Appendix B in accordance with the PRISMA guidelines (Page et al., 2021).

**Table 2. Inclusion and Exclusion Criteria**

| | **Inclusion criteria** | **Exclusion criteria** |
|---|---|---|
| Language | English | Non-English |
| Full text availability | Full text | Full text not available |
| Source type | Empirical and peer-reviewed journal and conference papers | Review, conceptual, and editorial articles, book sections, Master and PhD theses and dissertations |
| Subject area | A focus on privacy issues (mainly or partially) using a non-technical perspective | Lack of focus on privacy, or focusing on technical perspectives |
| Type of system | Smart health, e.g., wearable healthcare, IoT-based smart homes, healthcare surveillance, etc. | Systems not focusing on personal data sharing with other stakeholders, e.g., self-monitoring application |
| Study setting | Services based on health data | Not health data setting |
| Participants | Stakeholders such as individual users, healthcare professionals, government authorities, smart technology providers | Parties not contributing to the subject area |
| The findings of the study | Relevance to a better privacy understanding in terms of definition, factors, or outcomes of privacy in the study setting | Findings on a different focus rather than privacy |

## 3.2 Study Selection

A review reporting guideline is essential in literature reviews as it helps modify the original review protocol and enables changes to be reported as appropriate throughout the process. Moreover, it can be used to mitigate the risk of overlooking any potentially eligible studies. Following the PRISMA guidelines (Moher et al., 2009), a four-phase process consisting of identification, screening, eligibility, and inclusion was conducted, as shown in Figure 1. In the identification phase, 364 records were initially found by searching for keywords in the database. After removing duplicates, 347 records remained. Screening the title and abstract resulted in a preliminary list of 99 records. However, a few studies were excluded according to the inclusion and exclusion criteria. For instance, studies were removed if they included the search keywords but lacked a clear focus on privacy (e.g., Cristiano et al., 2022; Grill et al., 2016; Rahman et al., 2022). Studies were also excluded if they only focused on technical aspects – for example, a study focusing on creating a system architecture for a sensor-based smart-health framework that can minimize privacy concerns (Rahman et al., 2022). In addition, articles were excluded if their main focus was not on smart health monitoring, for example, post-Covid public health surveillance (e.g., Seberger & Patil, 2021; Yang, 2022). In the eligibility process, articles in the preliminary list were further assessed with a full-text screen by applying the exclusion criteria, and 43 records were included accordingly. In the last process, six relevant studies were revealed through forward and backward searches of references in the citations of included articles (Webster & Watson, 2002). A total of 49 records were obtained from a final examination separately conducted by this study's three authors.

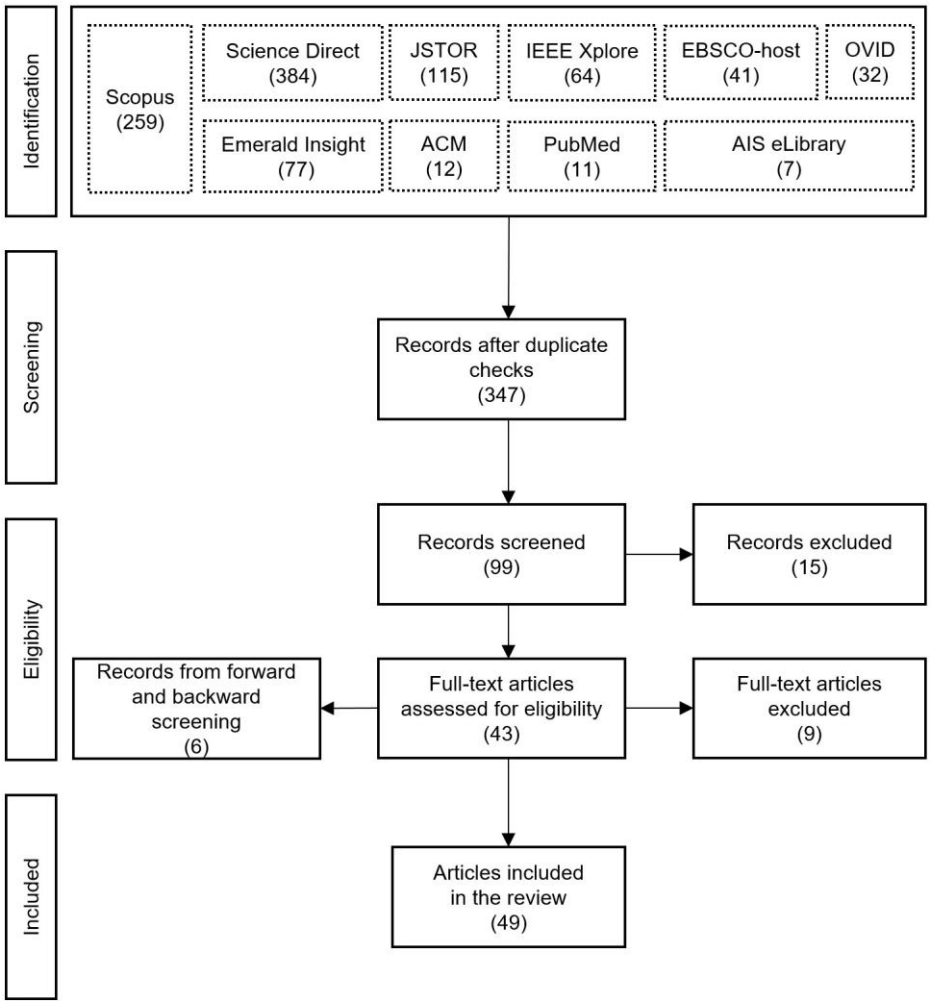


**Figure 1. Four-phase Study Selection Process Guided by the PRISMA Flow Diagram**

## 3.3 Data Collection and Thematic Analysis

A thematic analysis approach was adopted, involving multiple rounds to ensure thoroughness. Initial codes were developed inductively from the data using Excel software, and these codes were refined through three rounds of analysis to consistently capture emerging themes. Sample codes are provided in Appendix C. Initial open coding was applied to identify how privacy was framed in the reviewed articles. Codes were iteratively grouped into broader categories, reflecting common theoretical perspectives—privacy as a right, control, commodity, or state. Two independent coders (the first and second authors), reviewed the categorizations to enhance reliability, and discrepancies were resolved through discussion. Both authors completed the preliminary coding work using the inclusion and exclusion criteria and then discussed it with other authors to ensure all conflicts and discrepancies were resolved. This structured approach ensures that privacy perspectives in SHMS research are systematically classified, providing a clear foundation for the proposed framework.

In preparation for addressing the research question, definitions of privacy in smart health monitoring contexts were coded and categorized in the existing definitional perspectives, i.e., *privacy as a right* (Warren & Brandeis, 1890)*, a commodity to exchange* (Campbell & Carlson, 2002)*, an ability to control* (Culnan & Bies, 2003)*,* and *a state* (Schoeman, 1984). Privacy proxies, antecedents, and outcomes were then coded and sorted into several categories according to coding rules and definitions from the previous literature. New codes for the antecedents and outcomes were developed when the existing categories of codes could not be captured. The results were analyzed based on the following themes: 1) whether the study highlighted surveillance issues; 2) how surveillance was described; 3) which stakeholder(s) was involved in the study; and 4) whether the study investigated more than one stakeholder. Then, the theories and methods used to identify the antecedents and outcomes were also coded. Through thematic

analysis, patterns and themes related to privacy issues in SHMSs were identified and synthesized into a coherent framework. This iterative process involved refining the framework based on data from the reviewed articles. For instance, privacy definitions were categorized into several conceptual perspectives – rights, commodity, control, and state – which were then incorporated into the framework. The framework will be presented and illustrated in the Findings section which follows.

# 4 Findings

In this section, the framework is first introduced, which highlights the resulting themes derived from the thematic analysis in the early section. Next, a general descriptive overview of the characteristics of the reviewed articles is provided, along with findings on the theories and methods used in the articles. After that, key findings are presented on the basis of the components of the framework: privacy definitions and contextualization, privacy-related proxies, antecedents of privacy, privacy outcomes, as well as the context matters of surveillance and stakeholder dynamics in the reviewed articles.

## 4.1 Privacy Framework in Smart Health Monitoring

A hybrid model, which is effective for examining events that drive changes in outcomes or states, was used to provide a comprehensive understanding of the information systems field (Burton-Jones et al., 2015; de Guinea & Webster, 2017). Inspired by the hybrid model and the antecedents → privacy concerns → outcomes (APCO) model of information privacy (Smith et al., 2011), a high-level contextual framework was developed to present the synthesized results, as shown in Figure 2. This framework was developed inductively from the data, meaning it emerged directly from the analysis (Suddaby, 2006). While frameworks are typically introduced after the findings and discussion sections, it is presented upfront in this work, in line with the recommendations of Suddaby (2006) and Pool et al. (2024), to inform readers early about the critical theoretical dimensions and impacts. This framework advances prior literature by systematically integrating these privacy conceptualizations within a SHMS-specific context. It further contributes by linking these perspectives to a multi-level analysis of proxies, antecedents, and outcomes derived from the synthesized data. Thus, it is important to note that the framework is the outcome of our synthesis. The following paragraph provides a detailed explanation of the framework's development process and illustrates how the empirical findings support each of its components.

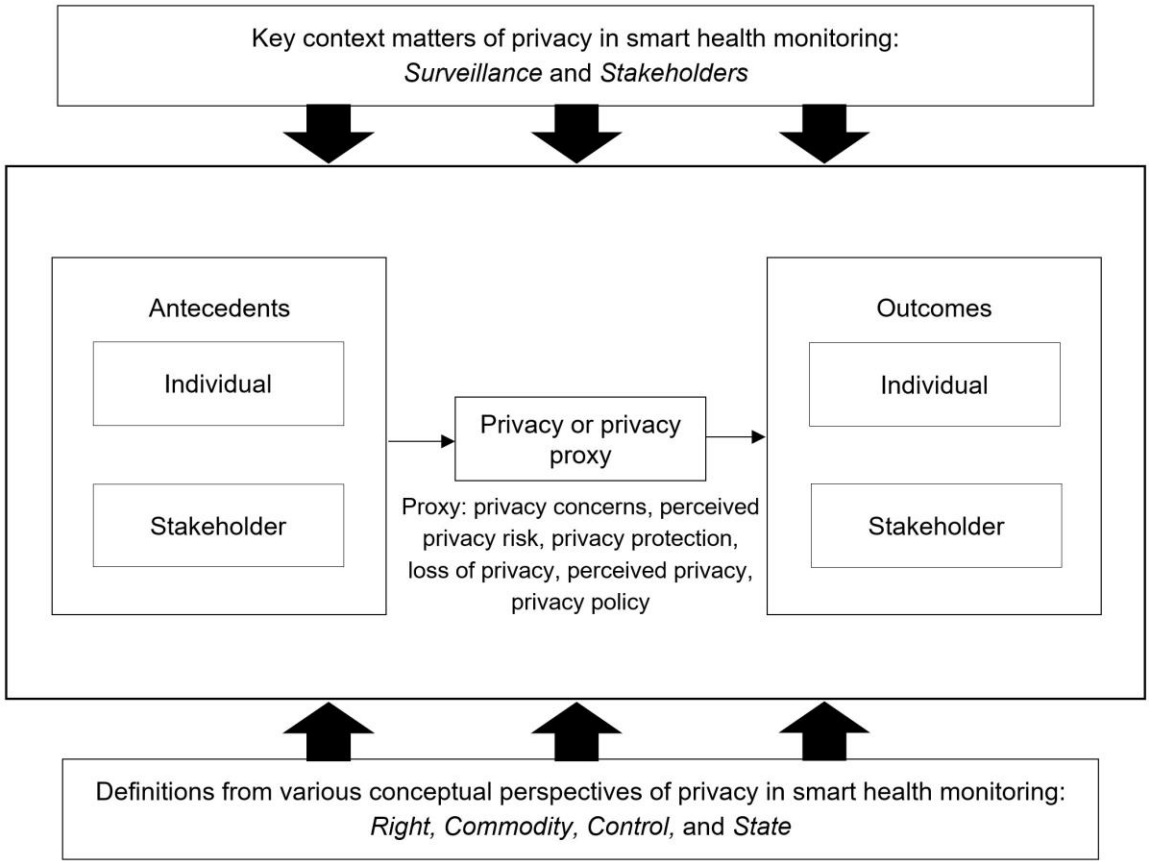


**Figure 2. A Contextual Framework of Privacy in Smart Health Monitoring**

Acknowledging the multidisciplinary nature of privacy (Smith et al., 2011), the framework presents privacy conceptualizations by analyzing the data through mainstream perspectives such as *right* (e.g., Fritz et al., 2016), *commodity* (e.g., Princi & Krämer, 2020), *control* (e.g., Burrows et al., 2018), and *state* (e.g., Papa et al., 2020) while remaining open to incorporating relevant minority viewpoints when they were identified through the data. The summary of the four perspectives was drawn from prior literature, as outlined in an earlier section. Furthermore, the framework highlights a variety of privacy proxies revealed through the synthesized data. For example, *privacy concerns* (e.g., Choi & Kim, 2024; Zhu et al., 2022) *and perceived privacy risk* (e.g., Karahoca et al., 2018; Zhang et al., 2019) were identified as proxies for examining individual perceptions and behaviors related to privacy within smart health monitoring contexts. In addition, the framework highlights antecedents at the individual and stakeholder levels. For instance, *regulatory expectation* was identified as an individual-based antecedent leading to privacy risk (e.g., Wiegard & Breitner, 2019), while *stakeholders' positive experiences with mHealth* were identified as stakeholder-based antecedents that affect privacy risks. The framework also reflects outcomes at the individual and stakeholder levels. For instance, *continuous use* as an individual-based outcome influenced by perceived privacy was examined in the context of consumer health wearables (Matt et al., 2019), while *stakeholder attitudes to adopting smart healthcare services* were explored as a stakeholder-based outcome in relation to privacy risks in a smart healthcare context (Pan et al., 2019). Finally, surveillance and stakeholders are two key context matters of privacy highlighted in this framework.

Our analysis demonstrates that many SHMS studies discuss privacy concerns without explicitly identifying the theoretical perspective they adopt. This gap of clear theoretical positioning contributes to conceptual fragmentation, making it difficult to synthesize empirical findings and translate them into actionable policy recommendations. The proposed framework addresses this issue by systematically categorizing privacy conceptualizations, enabling future research to adopt more theoretically grounded approaches. By clarifying how privacy is framed in SHMS research, this study enhances theoretical consistency, improves the comparability of empirical studies, and provides a foundation for more effective policy and system design in smart health monitoring.

## 4.2 Overview of the Articles' Characteristics

A total of 49 articles on privacy and smart health were reviewed, covering 2006 to 2024 (see Table 3). Notably, the majority (63%) were published between 2020 and 2024. Studies from the Asia-Pacific and Europe regions significantly outnumbered those from North America. The most frequently investigated systems were smart homes and smart wearables. The literature showed a near-equal distribution between quantitative and qualitative methods, with limited use of mixed-method approaches. Eight studies specifically explored multiple stakeholder groups using group-level analysis.

**Table 3. Summary of the Articles' Characteristics**

| | Number of articles | Percentage |
|---|---|---|
| **Year of publication** | | |
| 2020-2024 | 31 | 63% |
| 2015-2019 | 16 | 33% |
| 2006-2014 | 2 | 4% |
| **Source type** | | |
| Journal article | 44 | 90% |
| Conference paper | 5 | 10% |
| **Region** | | |
| Asia-Pacific | 18 | 37% |
| Europe | 17 | 35% |
| North America | 8 | 16% |
| Multiple countries | 6 | 12% |
| **Type of system** | | |
| Smart home | 15 | 31% |
| Wearable | 12 | 24% |
| MHealth/eHealth/remote health | 11 | 22% |
| Smart health | 8 | 16% |
| IoT | 3 | 6% |
| **Method** | | |
| Quantitative | 23 | 47% |
| Qualitative | 21 | 43% |
| Mixed methods | 5 | 10% |
| **Participant** | | |
| Consumers/patients/residents/users | 37 | 76% |
| Multiple groups of stakeholders | 8 | 16% |
| Healthcare providers | 4 | 8% |

### 4.2.1 Theories Used in the Published Articles

Overall, the technology acceptance model (TAM), the unified theory of acceptance and use of technology (UTAUT), and the privacy calculus theory (PCT) emerged as the most popular theories in the literature for explaining the antecedents and outcomes of privacy issues. However, not all the identified antecedents and outcomes were explained by theory. Six theories were used to analyze the antecedents of privacy issues (see Table C1, in Appendix C): the mobile users' information privacy concerns model (MUIPC), PCT, the theory of communicative action, categorization theory, the theory of contextual integrity (CI), and notions of borders. In contrast, theories employed in the outcome literature were more diverse (see Table C2, in Appendix C). In particular, multiple theories were found to aim at one outcome – such as the use of PCT and the theory of planned behavior (TPB) to predict subsequent actual behavior surrounding privacy concerns (Princi & Krämer, 2020), and the use of TAM, innovation diffusion theory (IDT), protection motivation theory (PMT), and PCT to explore behavior intention affected by perceived privacy risks

(Karahoca et al., 2018). In turn, one theory (or a set of theories) was used to identify multiple outcomes of privacy issues – for example, the use of TAM to identify outcomes of attitude toward adoption, perceived usefulness, and perceived ease of use (Papa et al., 2020), and the use of PCT and the concept of risk-risk tradeoff as a set of theories to identify outcomes of perceived value and application usage (Tran & Nguyen, 2021).

### 4.2.2 Methods Used in the Published Articles

Most of the quantitative studies used questionnaire survey methods (e.g., Liu & Tao, 2022), while some studies conducted experiments (e.g., Princi & Krämer, 2020) (see Table C3, in Appendix C). Nearly half of the qualitative studies adopted the interview approach to address their research questions (e.g., Alzahrani et al., 2021), while focus groups were the second most popular approach (e.g., Ghorayeb et al., 2021). A few qualitative studies employed the case study method (e.g., Ravishankar et al., 2015). Only five studies used a mixed-methods design. The purposes of mixed-method research can be summarized into several categories such as *developmental*, *diversity*, *completeness*, and so on (Venkatesh et al., 2016). For developmental purposes, two studies collected qualitative information prior to conducting quantitative surveys, allowing questions from one phase to inform the hypotheses tested in the next phase (Cristiano et al., 2022; Wiegard & Breitner, 2019). For diversity purposes, two studies conducted surveys and interviews to analyze the preferences and needs of smart home technologies, to obtain divergent views of the same phenomenon (Arar et al., 2021; Balta-Ozkan et al., 2013). Focusing on the completeness purpose, one study conducted a two-month feasibility assessment based on a questionnaire and interviews at three different time points, ensuring a comprehensive understanding of older adults' initial perspectives on IoT smart home devices (Choi et al., 2020).

## 4.3 Privacy Definitions and Contextualizations

Privacy is a multidisciplinary concept rooted in diverse justifications (Smith et al., 2011). Consistent with the framework, the definitions of privacy in the literature were extracted from the main perspectives – *right*, *commodity*, *control*, and *state*. Of the 49 studies, only 17 (35%) explicitly defined privacy or privacy proxies in the context of SHMSs. This indicates that 32 studies (65%) did not provide a privacy definition. Among these 17 studies providing definitions shown in Table C4 – Appendix C, 8 studies (16%) used more than one conceptualized perspective to explain privacy. Privacy was characterized as both a *control* and a *commodity* in varied smart health contexts. For example, Princi and Krämer (2020) defined the key to privacy in using an eHealth device as the control over personal data. Meanwhile, it highlighted privacy that can be traded off in the context of using IoT in healthcare due to the privacy calculus theory. For those defining privacy from a single view, 6 studies (12%) viewed privacy as a *control*. For example, Hassandoust et al. (2021) described that individuals' privacy concerns are related to their sensitive health data sharing and their ability to control their lifestyles. Two studies (4%) viewed privacy as a *state*. For example, Deng et al. (2018) explained that privacy risk refers to the possibility of information abuse, such as information theft and leakage due to using mHealth services. A further study (i.e., Kennedy et al. (2021), (2%), was coded 'N/A' representing 'not applicable,' based on its suggestion that different people rate the importance of privacy differently for a myriad of reasons across a number of circumstances. Therefore, it was difficult to classify this study into any existing conceptual perspectives.

## 4.4 Privacy-related Proxies

It is widely acknowledged that privacy cannot be directly measured (Smith et al., 2011). Therefore, most empirical privacy research uses measurable privacy-related proxies (Pavlou, 2011; Smith et al., 2011). Nearly half of the studies (23, 47%) did not use a proxy to investigate privacy (see Table C5 – Appendix C). For example, privacy itself was reported as a significant issue in the use of IoT in healthcare systems (Dadhich et al., 2022). Among the studies that did use proxies (26, 53%), the most common was 'privacy concerns,' which appeared in nine studies. This proxy relates to an individual's self-protection, sense of boundary, and control (Zhu et al., 2022). 'Privacy risk,' or 'perceived privacy risk,' was used in seven studies and refers to the potential for information abuse, such as theft or leakage, resulting from SHMS use (Deng et al., 2018). It also represents the possibility of personal health information (PHI) being disclosed through smart health products (Karahoca et al., 2018). Other proxies included privacy protection, perceived risk, loss of privacy, perceived privacy, and privacy policy. Privacy protection refers to consumers' perception of how well smart product providers safeguard health data during digital transfers (Nelson et al., 2016). Perceived risk reflects concerns among doctors about technology limitations and privacy issues with SHMSs (Pan et al., 2019), including factors like learning efforts,

inadequate privacy measures, and lack of information (del Río-Lanza et al., 2020). In SHMS contexts, loss of privacy refers to the perception that using smart healthcare services will violate individual privacy (Liu & Tao, 2022). Perceived privacy captures users' attitudes toward PHI disclosure, encompassing subthemes like perceived severity, relativity, and control (Matt et al., 2019). Finally, privacy policy governs how and when personal data will be collected, retained, or shared with third parties (Aljedaani et al., 2023). In three studies, privacy risk was embedded within the perceived risk variable, alongside psychological and financial risks (del Río-Lanza et al., 2020; Pan et al., 2019; Seiferth & Schaarschmidt, 2020).

## 4.5 Antecedents and Outcomes of Privacy and Propositions

In this section, antecedents and outcomes associated with privacy proxies are presented, followed by the related propositions. The findings reveal that antecedents and outcomes beyond individual-level factors, particularly those involving multi-stakeholder engagement, remain underexplored.

### 4.5.1 Antecedents of Privacy

The thematic analysis results identified nine antecedents among seven studies contributing to privacy issues in smart health monitoring environments. These antecedents were placed into two categories – *individual* and *stakeholder* – after consulting previous studies (Li, 2011; Miltgen & Peyrat-Guillard, 2014; Smith et al., 2011). Table 4 presents the identified antecedents and outcomes of privacy, along with the proxies for privacy used in the reviewed articles.

**Table 4. Extracted Antecedents and Outcomes of Privacy Issues**

| Category | Constructs/Themes | Proxy | Articles |
|---|---|---|---|
| **Antecedents of Privacy** | | | |
| Individual | Perceived health information sensitivity | Privacy risk (or perceived) | Wiegard and Breitner (2019) |
| | Surveillance concerns | N/A | Chadborn et al. (2019) |
| | Regulatory expectation | Privacy risk (or perceived) | Wiegard and Breitner (2019) |
| | Individual trust in business operators | Privacy protection | Shimizu et al. (2022) |
| | Mobile users' information privacy concerns | Privacy risk (or perceived) | Wiegard and Breitner (2019) |
| | Cultural differences | N/A | Kulyk et al. (2020) |
| Stakeholder | Stakeholders' concerns about surveillance | N/A | Beaudin et al. (2006) |
| | Stakeholders' positive experiences with mHealth | Perceived risk (including privacy risk) | Pan et al. (2019) |
| | Implementation of data mechanisms | N/A | Burrows et al. (2018) |
| **Outcomes of Privacy** | | | |
| Individual | Adoption/use/participation | Privacy concerns (or perceived): Choi and Kim (2024)<br>Privacy risk (or perceived): Tran and Nguyen (2021) | Alzahrani et al. (2021); Beaudin et al. (2006); Choi and Kim (2024); Fritz et al. (2016); Hassandoust et al. (2021); Sayibu et al. (2022); Tran and Nguyen (2021) |
| | Continuous use | Perceived privacy: Matt et al. (2019) | Burrows et al. (2018); Matt et al. (2019) |

| | | | |
|---|---|---|---|
| | Intention to adopt/use | Privacy concerns (or perceived): Choi et al. (2020), Mettler and Wulf (2020), Princi and Krämer (2020), Zhu et al. (2022).<br>Privacy risk (or perceived): Deng et al. (2018), Esmaeilzadeh (2023), Karahoca et al. (2018), Lu et al. (2021), Zhang et al. (2019).<br><br>Loss of privacy: Liu and Tao (2022) | Arar et al. (2021); Bhatt and Chakraborty (2020); Choi et al. (2020); Dadhich et al. (2022); Deng et al. (2018); Esmaeilzadeh (2023); Karahoca et al. (2018); Li et al. (2021); Liu and Tao (2022); Lu et al. (2021); Mettler and Wulf (2020); Princi and Krämer (2020); Zhang et al. (2019); Zhu et al. (2022) |
| | Attitude toward adoption | Privacy concerns (or perceived): Ghorayeb et al. (2021)<br>Perceived risk (including privacy risk): del Río-Lanza et al. (2020)<br>Privacy protection: Shimizu et al. (2022)<br>Loss of privacy: Papa et al. (2020) | del Río-Lanza et al. (2020); Ghorayeb et al. (2021); Kwiecień et al. (2020); Papa et al. (2020); Shimizu et al. (2022); Shimizu et al. (2021) |
| | Willingness to disclose/share data | Perceived risk (including privacy risk): Seiferth and Schaarschmidt (2020).<br>Privacy policy: Aljedaani et al. (2023) | Aljedaani et al. (2023); Kwiecień et al. (2020); Seiferth and Schaarschmidt (2020) |
| | Trust in smart technology/services | Privacy risk (or perceived): Deng et al. (2018)<br>Loss of privacy: Liu and Tao (2022) | Deng et al. (2018); Liu and Tao (2022) |
| | Perceived value | Privacy risk (or perceived) | Tran and Nguyen (2021); Wiegard and Breitner (2019) |
| | Perceived usefulness (of smart wearable healthcare) | Loss of privacy: Papa et al. (2020) | Papa et al. (2020); Sayibu et al. (2022) |
| | Perceived ease of use (of smart wearable healthcare) | Loss of privacy | Papa et al. (2020) |
| | Feelings of health empowerment | Privacy protection | Nelson et al. (2016) |
| Stakeholder | Attitudes to adopting smart healthcare services | Perceived risk (including privacy risk) | Pan et al. (2019) |
| | Implementation of smart health services | Privacy protection: Shimizu et al. (2022) | Peek et al. (2016); Shimizu et al. (2022); Xing et al. (2021) |
| | Designing smart health systems | Privacy concerns (or perceived): Cristiano et al. (2022) | Cristiano et al. (2022); LeBaron et al. (2020); Ravishankar et al. (2015) |
| | Stakeholders' use of wearable monitoring technology | Privacy concerns (or perceived) | Runkle et al. (2019) |
| | Smart home development | Privacy concerns (or perceived): Kim et al. (2018) | Balta-Ozkan et al. (2013); Kennedy et al. (2021); Kim et al. (2018); Suman (2017) |

***Individual-level antecedents related to user perceptions*** encompass a category of factors primarily associated with the characteristics, attitudes, attributes, and behaviors of individuals in relation to specific privacy issues in the smart health technology context (Dinev & Hart, 2004; Li, 2011; Xu, 2019). Several antecedents relevant to the individual-level category were identified: *perceived health information sensitivity* (Wiegard & Breitner, 2019), *surveillance concerns* (Chadborn et al., 2019), *regulatory expectation* (Wiegard & Breitner, 2019), and *individuals' trust in business operators* (Shimizu et al., 2022).

Moreover, *mobile users' information privacy concerns* were coded as an antecedent that directly influences the perceived privacy risks or uncertainties of mobile users in a health information monitoring context (Wiegard & Breitner, 2019). The degree of transparency in data collection, processing, and sharing mechanisms within SHMSs significantly influences users' trust and their subsequent privacy concerns (Awad & Krishnan, 2006; Esmaeilzadeh, 2019; Finch & Tene, 2014). This relationship is impacted by users' technological literacy, suggesting that enhancing transparency and educating users about SHMS technologies could mitigate privacy concerns (Esmaeilzadeh, 2019; Someh et al., 2019; Zhang et al., 2017). Thus, the following proposition is suggested:

**Proposition 1a. Technological transparency can influence individuals' trust and privacy concerns in the context of smart health monitoring.**

***Individual-level antecedents related to cultural differences*** encompass cultural factors that shape how individuals perceive privacy (Dinev et al., 2006; Smith et al., 2011). Similarly, in SHMSs, cultural differences were identified as an influential factor in privacy concerns analyzed at the individual level (Kulyk et al., 2020). Researchers found that people from Southern European countries perceive data disclosure as a personal choice, while people from Eastern European countries feel forced to disclose personal data. Overall, cultural and societal norms concerning health information privacy shape SHMS use (Li, 2011; Miltgen & Peyrat-Guillard, 2014). Cross-cultural differences in privacy expectations necessitate tailored SHMS privacy practices that align with local privacy norms and values, indicating a need for context-specific privacy management strategies. Thus, the following proposition is suggested:

**Proposition 1b: Contextual privacy norms across cultures can influence individuals' privacy concerns in the context of smart health monitoring.**

***Stakeholder-level antecedents*** emphasize the ways in which a specific industry and its stakeholders utilize information, encompassing their actions and attitudes toward safeguarding personal data, which, if compromised, could erode personal privacy (Tallon, 2013). In the existing literature, three stakeholder-level antecedents were identified in SHMSs: *healthcare providers' concerns about surveillance* (Beaudin et al., 2006), *healthcare providers' experience of using mHealth* (Pan et al., 2019), and *implementation of data mechanisms* (Burrows et al., 2018). Healthcare providers' concerns about surveillance are related to expressed skepticism toward smart home monitoring due to the perceptions of privacy issues by a group of various professionals including general practitioners, nurses, caregivers, and social workers (Beaudin et al., 2006). Moreover, healthcare providers' positive experiences with mHealth were found to reduce their perceived privacy risks associated with smart healthcare services while enhancing their intention to adopt these services (Pan et al., 2019). Additionally, studies suggested that privacy issues and relevant challenges can result from the failure or lack of meaningful awareness of mechanisms implemented by various stakeholders (Burrows et al., 2018; Jakobi et al., 2019). Thus, the implementation of data mechanisms was included as another stakeholder-related antecedent because it is a powerful influencer that controls privacy by negotiating existing boundaries and borders (Burrows et al., 2018). The alignment (or misalignment) of privacy expectations among SHMS stakeholders (e.g., users, healthcare providers, technology providers, and regulators) plays a critical role in shaping the ecosystem's privacy landscape (Lyles et al., 2021; Windasari et al., 2021). Misalignment may lead to privacy tensions and breaches, suggesting that a collaborative approach to establishing shared privacy norms and expectations is critical for the success of SHMSs (Lyles et al., 2021). Thus, the following proposition is suggested:

**Proposition 2: Stakeholder dynamics and privacy expectation alignment can influence individuals' privacy concerns in the context of smart health monitoring.**

### 4.5.2 Outcomes of Privacy

Fifteen privacy outcomes were identified among 41 studies (91%), coded in *individual* and *stakeholder*-related categories (as shown in Table 4 above).

***Individual-related outcomes*** are the most noticeable impact of privacy issues and refer to individuals' subsequent behaviors and beliefs (Miltgen & Peyrat-Guillard, 2014; Smith et al., 2011). This group of outcomes reflects the relevance and impact of privacy concerns on individuals' behaviors, attitudes, and perceptions in relation to smart health monitoring systems. These factors pertain especially to the outcomes related to the characteristics or actions of individual people rather than broader group outcomes. Studies found that privacy significantly impacts the adoption (e.g., Beaudin et al., 2006; Fritz et al., 2016) and continuous use of a healthcare-based smart service (e.g., Burrows et al., 2018; Matt et al., 2019). Additionally, instead of examining users' actual behavior, a large number of studies examined

users' intentions to use an SHMS service based on the theory of reasoned action (TRA) which suggests that behaviors match actual intentions (e.g., Fishbein & Ajzen, 1977; Smith et al., 2011). For instance, perceived privacy risk was found to be negatively related to the intention to use smart healthcare devices (Lu et al., 2021). Moreover, the desire to preserve privacy was found to affect individuals' perceptions in terms of attitude toward adoption (e.g., Ghorayeb et al., 2021), willingness to share personal data (e.g., Kwiecień et al., 2020), trust in smart technology (e.g., Deng et al., 2018), and perceived value of smart healthcare applications (e.g., Wiegard & Breitner, 2019).

The findings showed that perceived privacy assurance, derived from effective privacy protection mechanisms and clear communication of these protections, fundamentally shapes users' engagement with SHMSs by influencing their adoption/use, continuous use, and intention to adopt/use (Bansal et al., 2015; Chalhoub et al., 2024; Xu et al., 2011). When users perceive strong privacy assurances, their trust in smart technologies/services increases, leading to a positive shift in their attitude toward adoption and a greater willingness to disclose/share data (Bansal et al., 2015; Chalhoub et al., 2021). Furthermore, perceived privacy assurances enhance the perceived value and usefulness of smart wearable healthcare technologies, making them more appealing for adoption. This comprehensive impact of perceived privacy assurance on individual-level factors highlights the critical need for SHMS developers and policymakers to prioritize privacy as a core component of technology design and user communication strategies, thereby enhancing user engagement and empowerment in managing their health. Thus, the following proposition is suggested:

**Proposition 3: The integral role of perceived privacy assurance can result in shaping user engagement and trust in SHMSs.**

***Stakeholder-related outcomes*** refer to outcomes or consequences that are relevant to the key stakeholders involved in the privacy issues resulting from the use of smart health technologies over a broad range, covering economic, social, and environmental aspects from the stakeholders' collective perspective (Ruhlandt, 2018; Valle-Cruz, 2019). In addition to individuals (e.g., patients and users), the key stakeholders of smart health monitoring systems often include *healthcare providers*, *smart technology providers*, and *government authorities* (OECD, 2015; Peek et al., 2016; Swinkels et al., 2018). According to the review results, stakeholder-related (non-individual stakeholders) outcomes in the context of smart health monitoring include *stakeholders' attitudes to adopting smart healthcare services* (e.g., Pan et al., 2019), *implementation of smart health services* (e.g., Peek et al., 2016), *designing smart health systems* (e.g., Cristiano et al., 2022), *stakeholders' use of wearable monitoring technology* (e.g., Runkle et al., 2019), and the overall *smart home development* driven by multiple stakeholders (e.g., Kennedy et al., 2021).

Effective stakeholder collaboration in the design, implementation, and promotion of SHMSs acts as a critical catalyst for overcoming privacy concerns, fostering innovation, and enhancing the adoption and continuous use of these technologies (Thiebes et al., 2023; Ullah et al., 2021). Integration of diverse stakeholder perspectives – including those of healthcare providers, technology developers, users, and regulatory bodies – into the development and governance of SHMSs leads to more privacy-centric designs and policies (Miyachi & Mackey, 2021; Ullah et al., 2021). Such collaborative efforts result in smart health services and wearable technologies that are not only more aligned with end-user privacy expectations but also with the operational and ethical standards of healthcare providers and the regulatory frameworks of government authorities (Renwick & Gleasure, 2021). This integrated approach facilitates the creation of SHMSs that are perceived as more trustworthy and valuable by all stakeholders, thereby improving attitudes toward adoption, enabling smoother implementation processes, promoting more innovative system designs, and ultimately driving the development of smart homes and healthcare environments that are both technologically advanced and privacy-respecting. Therefore, the following proposition is suggested:

**Proposition 4: Stakeholder collaboration can be a catalyst for privacy-centric SHMS innovation and adoption.**

## 4.6 Matter of Context

In IS research, the most cited contexts for privacy are related to *technological applications*, *the use of information by sector*, *types of information* collected from individuals, and *political factors* (Smith et al., 2011). Given that the type of information is well acknowledged in the smart health monitoring context and political contexts can be emotionally charged through the presentation of authors' beliefs in different

causes (Smith et al., 2011), the present review work emphasizes 'surveillance and stakeholder' matters to compile a full picture of privacy contextualization in the smart health monitoring context.

***Surveillance*** involves the collection and processing of personal data to manage or influence individuals (Fox, Clohessy, et al., 2021). Keywords were categorized into three groups to assess how surveillance effectiveness was addressed: *Highlight*, *Mention*, and *Not Mention* (see Table C6, in Appendix C). Most studies fell into the Highlight group, indicating strong recognition of surveillance in privacy evaluations within smart healthcare. For example, Choi et al. (2020) examined how privacy risks deter users from choosing monitoring devices. The *Mention* group briefly touched on surveillance without much detail (Kim et al., 2018), while the *Not Mention* group ignored the issue altogether. Common keywords included *monitoring* (e.g., Chadborn et al., 2019; Choi et al., 2020) and *tracking* (e.g., Beaudin et al., 2006; Li et al., 2021). A few studies used *intrusiveness* (e.g., Etemad-Sajadi & Dos Santos, 2019) and *intervention* (e.g., Fritz et al., 2016; Shimizu et al., 2022) to explain the negative feelings related to monitoring or surveillance activities. Notably, some studies also explored the surveillance effectiveness of different monitoring devices – the *video camera* was ranked first with the highest negative effect (e.g., Arar et al., 2021; Balta-Ozkan et al., 2013).

***Stakeholders*** in smart health monitoring systems include individuals, healthcare providers, technology developers, and government authorities (OECD, 2015; Peek et al., 2016). The stakeholder context was reviewed by examining whether a study involved multiple stakeholders or focused on a single group. Few studies explored privacy in the context of multiple stakeholders (e.g., Peek et al., 2016), while most focused on one group, such as individuals or healthcare professionals (see Table C7, in Appendix C). For example, privacy was less of a concern for some stakeholders, like older adults, compared to technology developers (Alzahrani et al., 2021). In single-stakeholder studies, individual concerns were often overlooked due to conflicting goals between individuals and other stakeholders (Chadborn et al., 2019; Chen et al., 2021; del Río-Lanza et al., 2020; Hunter et al., 2020; Ravishankar et al., 2015; Suman, 2017).

# 5 Discussion

This section aims to discuss privacy definitions and contextualizations, along with their antecedents and outcomes, by leveraging the contextual framework in Figure 2 as a guiding structure. Our findings highlight that privacy in SHMSs is conceptualized in multiple ways, yet these conceptualizations are not always made explicit. By categorizing privacy research into four dominant perspectives—privacy as a *right, control, commodity*, and *state*—we provide a structured way for future researchers to engage with privacy in a more systematic manner. These perspectives are not only relevant for SHMSs but also align with broader IS privacy discourse, as they influence research methods, policy implications, and technological solutions. Without clear articulation of these perspectives, privacy research risks remain fragmented, preventing the field from developing cumulative knowledge. This study contributes to closing this gap by integrating these perspectives into a structured framework, allowing researchers to better compare, build upon, and refine privacy studies in SHMS research and beyond.

***Privacy definitions and contextualizations****:* The findings reveal that while privacy definitions varied across SHMS studies, there was some inconsistency in their application. Establishing unified frameworks would enhance future research and theory development. Three key aspects should be considered by future researchers. First, clarifying the definition of privacy from one or multiple perspectives can enrich the understanding of privacy in multidisciplinary environments like smart health monitoring. This will help researchers focus their studies and select suitable theoretical frameworks. For instance, defining privacy from a state perspective allows for the use of theories like the balance theory to explore whether privacy, consumers, and health insurance providers form a balanced triadic relationship (e.g., Hassandoust et al., 2021; Liu & Tao, 2022). Second, selecting a specific perspective enables researchers to adopt existing measurement items from studies using the same perspective. For example, Princi and Krämer (2020) adopted items from Smith et al. (1996) as both studies used a *control* perspective on privacy. Third, privacy is not a one-size-fits-all concept – it evolves based on context and individual experiences, especially in complex systems like smart health monitoring (Pang et al., 2020; Solove, 2007). Researchers should consider integrating diverse perspectives to capture these nuances.

***Proxies, antecedents, and outcomes****:* The review findings indicate that proxies, antecedents, and outcomes related to privacy in smart health monitoring are underdeveloped, and stronger linkages are needed. This highlights the need to further explore the interplay between privacy and other concepts using a measurable framework. It is crucial to identify clear proxies for privacy, as measuring privacy often relies

on perceptions rather than rational assessments (Smith et al., 2011). Encouragingly, some studies suggested examining privacy proxies beyond just privacy concerns, which can carry negative connotations and may not fully capture the concept of privacy (Dinev et al., 2013; Fox, van der Werff, et al., 2021). For instance, in one reviewed study, privacy protection was used as a proxy to measure its positive impact on health empowerment in smart wristbands (Nelson et al., 2016). Furthermore, using multiple proxies can provide a more comprehensive understanding, as explained by Wiegard and Breitner (2019), which examined the relationship between mobile users' privacy concerns and perceived privacy risks. Ultimately, a more precise measurement of privacy, tailored to the specific research context, is needed to advance the literature (Stewart & Segars, 2002).

Currently, the connections between antecedents and privacy outcomes in SHMS contexts are vague and require more investigation. Specifically, more research is needed to determine how different antecedents lead to specific privacy outcomes. Most of the reviewed studies focused on individual-level antecedents and outcomes, with few exploring how individual- or stakeholder-level factors influence broader group-level outcomes. The majority of SHMS studies examined antecedents at the individual level but with very little antecedent analysis at the stakeholder or other levels. Privacy is of growing concern when involving multiple stakeholders (Smith et al., 2011), and the introduction of smart healthcare services has often generated resistance from service providers (e.g., clinicians) during the adoption process (Pan et al., 2019). Privacy researchers should be cautious as focusing solely on the perceptions of individual customers may introduce bias and overlook the perspectives and experiences of other individuals (aside from customers), consequently failing to identify group-level privacy issues (Bélanger & Crossler, 2011). It is encouraging to see that a few researchers explored stakeholder-level perceptions among healthcare professionals who offer monitoring services through smart devices. For example, a perception of privacy-related risk was found to negatively impact doctors' personal attitudes toward using smart healthcare services, which could eventually affect the implementation of the service (Pan et al., 2019). In addition, the antecedents from other levels, such as societal, environmental, cross-cultural, or national levels should be effectively addressed in future empirical studies, due to their significant impact on individuals' information privacy.

SHMSs strive to generate co-created outcomes of value for both the individual users and the community at large (Janamian et al., 2016; Ramaswamy & Ozcan, 2014). In terms of outcomes for individual users, although the theory of reasoned action (TRA) suggests that behaviors match actual intentions, it should be cautioned that the relationship between privacy and stated intentions does not always reflect actual behaviors (Smith et al., 2011). Future studies could target actual behaviors and thoroughly investigate contextual factors that may predict those behaviors (Plangger & Montecchi, 2020). Moreover, SHMSs involve collaborative healthcare service communities and multiple stakeholders (Alabdulatif et al., 2019; Deloitte, 2019). It is important to explore the behavioral outcomes at the stakeholder level, such as stakeholders' attitudes (e.g., Pan et al., 2019) and their use of smart health systems (e.g., Runkle et al., 2019). It is equally important for organizations and policymakers to explore organizational and regulatory outcomes to effectively manage privacy issues in SHMSs (Manyika et al., 2011; Winter & Davidson, 2022). This would enable organizations to identify innovation opportunities and develop new products, services, and processes that prioritize privacy and security (Xu, 2019). Companies that demonstrate a strong commitment to privacy can gain a competitive advantage by attracting privacy-conscious customers and partners (Smith et al., 2011). By emphasizing the regulatory outcomes influenced by privacy concerns, companies can ensure compliance with relevant laws and regulations, avoiding costly penalties and legal actions (Esmaeilzadeh, 2019), while policymakers can rely on research and evidence to inform the development of laws and regulations related to privacy and data protection (Solove, 2006; Someh et al., 2019).

***Theories****:* Overall, several of the reviewed studies did not apply a theory that could help explain the complex nature of privacy more effectively. The absence of relevant theories raises questions about the validity and value of the research (Sutton & Staw, 1995). A theory is a linguistic device used to parsimoniously organize and clearly communicate concepts in a complex empirical world (Bacharach, 1989). It helps explain underlying processes and provides an understanding of the systematic reasons for a specific occurrence or non-occurrence (Sutton & Staw, 1995). Therefore, it is important to use an appropriate theory or (theories) to solidify the research motivations and assumptions when examining privacy-related constructs. It was common for the reviewed studies to employ theoretical frameworks like TAM, UTAUT, and UTAUT 2 to understand how people adopt and use health information technologies (e.g., Bhatt & Chakraborty, 2020; Liu & Tao, 2022; Zhu et al., 2022). However, these models have faced criticism for being overly simplistic and limited (Shachak et al., 2019). Prior researchers have also argued

that the contributions of those frameworks to knowledge in this area have reached a plateau (Rouidi et al., 2022; Shachak et al., 2019). Moreover, the review of the research showed that one of the key barriers to the successful implementation of digital health devices is both their low level of acceptance and resistance by healthcare professionals (Cilliers & Flowerday, 2014; Pan et al., 2019; Rouidi et al., 2022).

***Methods**:* The findings show that much of the research employed a single-method approach to explore the privacy phenomenon in SHMS contexts. Both single-method and mixed-methods approaches offer distinct advantages in exploring privacy issues, with the choice depending on the specific objectives of the research. A mixed-methods design offers an opportunity to develop fresh theoretical perspectives by combining the strengths of qualitative and quantitative methods and is particularly useful for providing a holistic understanding of a phenomenon at an early research stage (Venkatesh et al., 2013; Venkatesh et al., 2016). Moreover, it is a well-suited approach when the nature of the context changes frequently and researchers face difficulty drawing meaningful insights from existing perspectives (Califf et al., 2020). The nature of the healthcare context frequently changes and involves contextually relevant challenges (such as the technological complexity associated with users) (Califf et al., 2020). Thus, using a mixed-methods design is appropriate to better explore the underlying layers of privacy issues in healthcare-related domains (Califf et al., 2020; Fox & James, 2021).

***Context matters**:* Context matters are dynamic forces and factors embedded within an entity and have been used as important predictors to measure a proposed relationship in an entity (Edwards & Steins, 1999; Shah & Ward, 2003; Shalley et al., 2004). Since these forces span multiple levels that are not relevant to a user (or a user group) (Kaplan et al., 2010; Shalley et al., 2004), several attempts have been made by privacy researchers to distinguish contextual factors from other sets of factors (such as individual factors and macro factors) (Li, 2014; Miltgen & Peyrat-Guillard, 2014; Ozdemir et al., 2017). Surveillance also emerged as an important theme in the literature review, with many studies highlighting the influence of surveillance in the smart health system. However, research on influencing factors stemming from surveillance has yet to be developed. The range of topics explored in the literature review was narrow and straightforward. For example, a large number of studies focused on the participants' acceptance of a surveillance device installed in their homes (e.g., Arar et al., 2021; Chadborn et al., 2019; Zhu et al., 2022). Researchers who focus on surveillance as a matter of context should employ a measurable predictor to more deeply understand how privacy is affected by surveillance. Regarding stakeholders, only a small portion of the research in the reviewed literature focused on entities beyond individual users. The resistance of healthcare professionals to smart health systems due to their privacy concerns could be a key barrier to the successful implementation of digital health (Pan et al., 2019). Smart health monitoring can be seen as a dynamic community relying on multi-stakeholders (Aghdam et al., 2020). Thus, unlike personal devices, the success of a smart health service hinges on the cooperation of multiple stakeholders, not merely on individuals' usage (Aghdam et al., 2020; Deloitte, 2019). It is recommended that research attention be shifted to the stakeholder level by evaluating contextual factors related to the context of collaborative stakeholders.

## 5.1 Implications for Stakeholders and Practice

Implementing privacy protection in smart monitoring services is challenging due to the intricate network of stakeholders and their diverse protection mechanisms. The participation of various stakeholders was found to provoke privacy issues among individuals (e.g., Beaudin et al., 2006; Pan et al., 2019), serving as a significant antecedent factor and outcome of privacy. This review highlights four key stakeholders of SHMSs.

***Individuals***: Individuals include any end-users of smart health applications. In the dynamic environment of smart health monitoring, where collaboration among stakeholders is paramount, it is crucial for individual users to recognize themselves not only as beneficiaries but also as vital stakeholders, given their active involvement. Individuals' perceptions of privacy and surveillance concerns were found to block them from using health monitoring technologies and sharing their health data with other stakeholders in smart health monitoring systems. However, individuals should understand the duality of privacy and surveillance in smart health monitoring applications. Smart health monitoring systems and surveillance technologies are forming new contexts of health data flow. In complex environments like this, multiple stakeholders naturally interact and collaborate across different disciplines and levels, working across various data domains to ensure individuals receive healthcare benefits. Hence, individuals should acknowledge the dual nature of privacy and surveillance in smart health monitoring systems and actively engage in smart health monitoring services in order to empower their health through the system.

***Healthcare providers***: Stakeholders in this category refer to clinicians such as doctors and nurses, caregivers, volunteers, and emergency personnel, among others, and involve healthcare facilities ranging from hospitals and health systems, ambulatory surgery centers, long-term care facilities, home health agencies, ancillary providers, to community group homes. The adoption of smart health monitoring technologies can offer advantages to healthcare providers, including enhanced operational efficiency, cost reductions in patient care delivery, improved quality measurement, and expanded reporting capabilities. However, concerns about privacy and associated challenges may arise if healthcare providers encounter difficulties in implementing effective data governance mechanisms or if there is a lack of meaningful awareness among this group of stakeholders. Data governance in healthcare services has been given significant prominence in recent years, based on its aim to maximize the value of data assets and manage data-related risks in the system. Since data governance can diffuse tension in terms of privacy and data sharing, mitigate risks, and balance interests within the multidisciplinary contexts of data sharing, healthcare providers should develop data governance mechanisms for their privacy activities. Moreover, the framework can assist healthcare organizations to better understand how privacy is perceived and operationalized by different actors in the SHMS ecosystem. By using the framework, healthcare providers can align their privacy practices with stakeholder expectations and improve collaboration across clinical, administrative, and technological domains.

***Smart technology providers***: Smart technology providers often encompass developers, vendors, and suppliers who focus on providing and maintaining smart health devices, service apps, and smart health monitoring service platforms by means of various information and communication technologies (ICTs), including sensing and surveillance. These technology providers are at the forefront of introducing surveillance technologies in smart health monitoring applications. Privacy issues have been demonstrated to influence the design, strategies, and development of functionalities within smart health systems when considered from a design thinking lens. There is a significant amount of literature on privacy-focused technologies in smart health monitoring applications. However, relatively little research has explored the negative impacts of privacy concerns on smart technology providers. Therefore, smart technology providers are encouraged to utilize the proposed framework of this study to gain a deeper understanding of the privacy concerns associated with their technologies. By considering the contextual factors, stakeholder perspectives, and identified privacy proxies outlined in the framework, they can better anticipate potential privacy risks and align their design and deployment strategies with stakeholder expectations and regulatory requirements. Technology providers have an ethical responsibility to protect the privacy and confidentiality of users' health data. Adhering to privacy regulations and laws is crucial for smart technology providers to avoid legal repercussions. Mishandling of privacy issues can lead to negative publicity and damage the reputation of developers and providers. By prioritizing privacy and implementing robust data protection measures, they can protect the brand reputation of technology providers.

***Government authorities***: Government authorities include government agencies, policymakers, and legislators that help achieve better data governance among stakeholders. Only a few of the reviewed studies investigated the efforts of government authorities regarding the privacy issues of smart health monitoring. However, antecedents, including individual-level *regulatory expectations* and *trust in business operators* and stakeholder-level *health tracking data mechanisms*, are all associated with the active involvement of government authorities. Moreover, smart health initiatives, like the development of smart homes, are intricately linked with the overarching objective of smart city development pursued by local government authorities. Therefore, it is imperative for government bodies to prioritize the management of individuals' privacy concerns by enhancing regulatory frameworks and fostering collaboration with other stakeholders involved in these systems. Government authorities and policymakers can use the framework to evaluate privacy risks in light of surveillance-intensive healthcare technologies. For example, in the rollout of digital health initiatives involving AI or IoT, the framework’s emphasis on surveillance context and stakeholder-specific outcomes provides a structured lens for developing responsive privacy policies and regulatory mechanisms.

## 5.2 Implications for Future Research Avenues

Based on the review of the existing literature, this study provides six research avenues (as shown in Table 5) along with a number of research questions for future research.

**Table 5. An Overview of Future Research Avenues**

| Avenue# | Description | Future research questions |
|---|---|---|
| #1 Contextualized definition | Clarifying the contextual and dynamic nature of privacy through a clarified definition | • How is privacy defined among various SHMS stakeholders?<br>• How do different cultural contexts affect users' understanding of privacy concerns caused by surveillance-based healthcare technologies?<br>• What are the dimensions of privacy in the context of SHMSs? |
| #2 Multi-level analysis | Exploring phenomena at different levels of analysis, including individuals, groups, organizations, and communities | • How do individual characteristics, organizational practices, stakeholder dynamics, and societal influences interact to shape privacy conceptualizations in the context of smart health monitoring technologies?<br>• What are the key factors at the individual, organizational, stakeholder, societal, and technological levels that contribute to enhancing user acceptance of privacy features in SHMSs? |
| #3 Methods of analysis | Using a mixed-methods design rather than a single method | • How do ethnographic studies illuminate the nuances of privacy concerns in relation to smart health monitoring technologies, and how can these insights inform the development of more robust privacy policies and practices?<br>• What do rich qualitative interviews with stakeholders tell us about the organizational policies, procedures, and cultural norms surrounding privacy issues in the context of SHMSs?<br>• To what extent do methodological biases in sample selection impact the validity and generalizability of research on privacy issues in SHMSs, and what strategies can be employed to mitigate these biases? |
| #4 Stakeholder analysis | Delving into the stakeholders' ecosystem for privacy protection management | • How do the diverse values and objectives of stakeholders in SHMSs contribute to the effectiveness of implementing data privacy mechanisms?<br>• How can value co-creation strategies be employed within the stakeholder ecosystem of SHMSs to address privacy concerns and enhance user engagement and empowerment?<br>• How can privacy concerns be effectively managed within the complex stakeholder landscape of smart health monitoring projects? |
| #5 Contributing to the IS theories | Incorporating more influential theories and embracing a broader perspective | • How do individuals make decisions to disclose health data in SHMSs – thinking beyond privacy trade-off?<br>– How do psychological, socio-cultural, and technological factors collectively influence individuals' decisions to disclose health data in SHMSs?<br>– What alternative theoretical frameworks can better explain these influences beyond the traditional privacy trade-off model?<br>• How can customer-perceived value be reshaped in SHMSs from a multidimensional development theory perspective?<br>– In the context of SHMSs, how are different dimensions of customer-perceived value – comprising utility, trust, personalization, and privacy concerns – interrelated?<br>– How can multidisciplinary theoretical perspectives enhance our understanding of these relationships to improve user engagement and system design? |
| #6 Investigating less-explored aspects of emerging themes from this review | Focusing on the influencing factors arising from lesser-explored aspects of emerging themes, such as barriers to surveillance | • How can inappropriate traceability and monitoring affect individuals' willingness to share data in the context of smart health monitoring?<br>• How do perceived privacy risks influence the use of reward-based SHMSs?<br>• Does North America exhibit a greater tolerance for privacy breaches in SHMSs compared to European regions? |

***Avenue #1 – Contextualized definition****:* Clarifying the contextual and dynamic nature of privacy through a clarified definition is a pragmatic approach for accurately grasping and analyzing privacy issues (Solove, 2002; Xu & Bélanger, 2013; Zhang et al., 2017). A clear definition is essential as it serves as a foundational principle for facilitating transparent communication and fostering a coherent understanding of privacy (Dinev et al., 2013). Without a precise and consistent understanding, there is a risk of fragmented and ambiguous interpretations of privacy (Dinev et al., 2013). Moreover, integrating multiple perspectives

helps to enrich the conceptual understanding of privacy across disciplinary boundaries and analytical levels, particularly in complex environments such as SHMSs. The proposed framework encourages researchers to explicitly select and articulate the theoretical perspectives guiding their analysis of privacy. This approach not only supports theoretical precision but also addresses fragmentation in existing SHMS privacy literature, where conceptual underpinnings are often implicit or inconsistently applied. For example, Matt et al. (2019) explored how people's control over their data affects their willingness to use health monitoring devices, and then looked at the cost-benefit aspect of privacy and functionality in continuous usage. In doing this, models like privacy calculus theory can be applied to further explore users' trade-off decisions between the beneficial and adverse outcomes in a healthcare monitoring context. This structured application of perspectives facilitates cumulative theory development and fosters coherence across privacy-related SHMS studies. To fulfill the contextualized definition of privacy, researchers could answer the relevant research questions outlined in Table 5.

***Avenue #2– Multi-level analysis***: In general, multi-level research involves exploring phenomena at different levels of analysis, including individuals, groups, organizations, and communities (Blakely & Woodward, 2000; Smith et al., 2011). The community level, in particular, has garnered significant attention due to the advancements in remotely delivered virtual healthcare ecosystems (Schiavone et al., 2021). Multi-level research is essential for the mechanisms and reasons behind the occurrence of the privacy phenomenon (Ancona et al., 2001). It is able to provide a complete picture of privacy conceptualization with complexity across various levels (Mulligan et al., 2016). Our contextual framework enhances the theoretical landscape of privacy in SHMSs by broadening the focus from individual-level privacy concerns to include societal and stakeholder-level factors, thus filling a critical gap in the literature. To conduct a multi-level analysis, researchers could explore the corresponding research questions presented in Table 5.

***Avenue #3 – Methods of analysis***: Future researchers are encouraged to use a mixed-methods design rather than a single method in order to comprehensively investigate the privacy dynamic in the context of smart health monitoring. They are advised to explicitly delineate and/or recognize the purposes of their mixed-methods design, which could help readers better grasp the goals and outcomes of their mixed-methods research papers (Venkatesh et al., 2013). To achieve this, it is critical to be aware of the exact nature of mixed-methods designs and the wide range of purposes for using a mixed-methods approach (Venkatesh et al., 2013; Venkatesh et al., 2016). Several purposes (i.e., *developmental*, *diversity,* and *completeness*) appeared in the reviewed literature. Other purposes and examples (such as *complementarity*, *expansion*, *corroboration/confirmation*, and *compensation*) can be found in the work of Venkatesh et al. (2013). In addition, meta-inferences are narratives, theoretical statements, or a story inferred from the integration of findings from qualitative and quantitative and strands of mixed-methods research. Meta-inferences are central to mixed-methods research designs, as they enable researchers to move beyond single-strand conclusions and contribute to the development of substantive theory for the phenomenon under study (Polyviou et al., 2024; Venkatesh et al., 2013). It is hard to define a research program as truly being a mixed-methods research unless it combines findings from both qualitative and quantitative studies (Venkatesh et al., 2013). Thus, researchers using mixed-methods designs should offer an explicit discussion of meta-inferences. There are further potential research questions to explore, as presented in Table 5.

***Avenue #4 – Stakeholder analysis***: Future studies can concentrate on analyzing multi-stakeholder engagement, delving into the stakeholders' ecosystem for privacy protection management in smart health monitoring. True cooperation among stakeholders was argued to be far from reality in terms of users' active participation in advanced health systems (Suman, 2017). Individuals do not feel encouraged to use smart health devices (or services) to share health data because of their surveillance and privacy concerns stemming from inadequate cooperation amongst stakeholders. Researchers are recommended to deepen stakeholder-specific investigations in response to insufficient analysis of stakeholders in the literature. The investigation should also provide a clear description of the categories or types of stakeholders involved in the context. Stakeholders, including individuals, healthcare providers, smart technology providers, and government authorities (either individually or in groups), can be involved in the investigation based on various research aims. For example, an investigation of multiple stakeholders would help mitigate health data privacy concerns and allow users to regain control (Chadborn et al., 2019). Possible research questions are included in Table 5.

***Avenue #5 – Contributing to the IS theories****:* A theory is viewed as a system that logically connects its key components through propositions or hypotheses (Bacharach, 1989). It serves to elucidate the

relationships between phenomena by emphasizing causal connections and determining the sequencing and timing of such phenomena (Sutton & Staw, 1995). The significance of theory in IS lies in its ability to explain the what, why, and/or how of phenomena (Mueller & Urbach, 2017). However, given the intricate nature of privacy issues within smart health contexts, using overly simplistic theories like TAM often fails to address broader system-level issues that extend beyond individual user acceptance, including factors like multitasking, workflow and interruptions, and other operational complexities (Shachak et al., 2019). To contribute to IS theories and overcome the limitations of the current literature, future researchers could derive significant value from incorporating more influential theories and embracing a broader perspective that effectively addresses the complexity of smart health contexts.

Rather than prescribing specific theories, scholars are encouraged to consider theoretical pluralism and adopt theories that go beyond offering simple causal explanations. That is, scholars can consider dynamic and longitudinal perspectives using process theories/models and stage theories. In the IS field, process theories focus on the dynamic and temporal aspects of phenomena and explain how specific outcomes are gained through a series of actions or events (Markus & Robey, 1988). For instance, health empowerment theory emphasizes the ongoing process through which individuals gain control over their health and health-related activities in a broader sense, i.e., a professional community (Rissel, 1994; Spreitzer, 1995). It involves a series of activities and interactions that result in greater health empowerment within the community. Roger's diffusion of innovations theory highlights that diffusion is the process by which an innovation is transmitted through specific channels over time among the members of a social system (Rogers, 2003; Sahin, 2006). Moreover, as suggested in the work of Li (2012), integrating multiple theories in a study can yield more fruitful insights into privacy and related behaviors. Furthermore, it is essential for researchers to establish connections among theories when constructing an integrated theoretical framework (Li, 2012). For example, the privacy calculus theory is commonly employed as a central approach to analyzing individuals' behavior before incorporating other theories (e.g., Princi & Krämer, 2020; Tran & Nguyen, 2021; Wiegard & Breitner, 2019). While these different theories are used to interpret how privacy calculus is processed, the general findings support the central role of privacy calculus (Laufer & Wolfe, 1977; Li, 2012). Potential research questions are outlined in Table 5.

***Avenue #6 – Investigating less-explored aspects of emerging themes from this review****:* Researchers are encouraged to focus on the influencing factors arising from lesser-explored aspects of emerging themes, such as barriers to surveillance and difficulties in involving new stakeholders with new business plans, as well as the profound impact of emotional responses such as stress, anxiety, and discomfort stemming from privacy concerns (De Moya & Pallud, 2020; Degirmenci, 2020; Zhang et al., 2022). Although surveillance was recognized as an important theme in the reviewed literature, only a few studies explored surveillance-related contextual factors. Likewise, health insurance providers are emerging as stakeholders interested in subsidizing the purchase of wearable devices and implementing bonus programs. However, involving new stakeholders may heighten the complexity of privacy management. It is crucial to analyze the characteristics of these new stakeholders and their contextually relevant challenges in addressing the privacy concerns of individual customers.

Moreover, our findings reveal a notable disparity in the distribution of studies, with a substantial contribution from Asia-Pacific and European regions, while insights from North America remain relatively limited. Despite this, numerous reports highlight a concerning prevalence of privacy breaches associated with SHMSs in North America (e.g.,CNBC.com, 2022; Thelancet.com, 2023). This raises questions about whether North America might exhibit greater tolerance for privacy breaches in SHMSs compared to European regions, prompting an investigation into how these variations in cultural and regulatory contexts impact privacy perceptions and management strategies. Is this disparity potentially influenced by variations in regulatory frameworks and cultural perspectives? Researchers have found that people from Southern European countries perceive data disclosure as a personal choice, while people from Eastern European countries feel forced to disclose personal data. Overall, cultural and societal norms toward health information privacy shape SHMS use (Li, 2011; Miltgen & Peyrat-Guillard, 2014). Cross-cultural differences in privacy expectations necessitate tailored SHMS privacy practices that align with local privacy norms and values, indicating a need for context-specific privacy management strategies. Based on this review's findings, in addition to cultural factors, environmental and technological aspects have also been overlooked in the literature. Considering these contextual factors are essential for a better understanding of privacy contextualization in a specific SHMS project (Schlackl et al., 2022; Zaman et al., 2022; Zhang et al., 2023), researchers are encouraged to explore several potential research questions, such as the questions presented in Table 5.

### 5.3 Limitations

This review has some limitations. First, despite our broad search terms for surveillance, it is possible that some critical articles and concepts were overlooked. This may be due to previous researchers using alternative terminology to describe surveillance scenarios, such as 'surveillance,' 'monitor,' 'track,' or 'detect'. Second, a number of reviewed articles used various terms for smart health monitoring systems, such as eHealth, remote health, connected health, or smart home which may have caused inconsistencies in the article inclusion. Third, the review targeted key stakeholders only – individuals, healthcare providers, smart technology providers, and government authorities. Future literature reviews could include more novel stakeholders, for example, insurance service providers, that may be essential in smart health monitoring systems.

## 6 Conclusion

This study addressed the gap in the existing literature related to the less explored contextualization of privacy in SHMSs and answered the research question accordingly. It began by emphasizing the importance of contextual clarity in privacy research within SHMS contexts and highlighting that previous review articles have not consistently focused on this aspect. Through a systematic literature review encompassing 49 articles, the study proposed a contextual framework for SHMS privacy research, offering a comprehensive understanding of the current state of contextualized privacy in these systems. The proposed framework offers valuable insights for scholars seeking to grasp the nuanced aspects of privacy in SHMS settings. Furthermore, the study examined the theories and methods utilized in current SHMS research, advocating for scholars to consider multiple theoretical perspectives and adopt mixed-methods approaches. The findings can assist healthcare providers and policymakers in identifying potential privacy issues related to personal health information when collaborating on the development and implementation of healthcare surveillance systems. Additionally, our research identified existing knowledge gaps and outlined six potential research avenues to achieve a thorough understanding of privacy in SHMSs.

## Declaration of AI

This paper was not generated by any AI tool. AI tools (e.g., ChatGPT) were used solely for grammar checks and minor textual refinements.

## References


Accenture.com. (2020). *How can leaders make recent digital health gains last?* Retrieved from https://www.accenture.com/us-en/insights/health/leaders-make-recent-digital-health-gains-last

Aghdam, A. R., Watson, J., Cliff, C., & Miah, S. J. (2020). Improving the theoretical understanding toward patient-driven health care innovation through online value cocreation: Systematic review. *Journal of Medical Internet Research, 22*(4), 1–14.

Ahmed, S. F., Alam, M. S. B., Afrin, S., Rafa, S. J., Rafa, N., & Gandomi, A. H. (2024). Insights into Internet of Medical Things (IoMT): Data fusion, security issues and potential solutions. *Information Fusion, 102*, 1–20.

Akmandor, A. O., & Jha, N. K. (2018). Smart health care: An edge-side computing perspective. *IEEE Consumer Electronics Magazine, 7*(1), 29–37.

Alabdulatif, A., Khalil, I., Forkan, A. R. M., & Atiquzzaman, M. (2019). Real-time secure health surveillance for smarter health communities. *IEEE Communications Magazine, 57*(1), 122–129.

Aljedaani, B., Ahmad, A., Zahedi, M., & Babar, M. A. (2023). An empirical study on secure usage of mobile health apps: The attack simulation approach. *Information and Software Technology, 163*.

Almujally, N. A., Aljrees, T., Saidani, O., Umer, M., Faheem, Z. B., Abuzinadah, N., Alnowaiser, K., & Ashraf, I. (2023). Monitoring acute heart failure patients using internet-of-things-based smart monitoring system. *Sensors, 23*(10).

Al-Rawashdeh, M., Keikhosrokiani, P., Belaton, B., Alawida, M., & Zwiri, A. (2022). IoT adoption and application for smart healthcare: A systematic review. *Sensors, 22*(14), 1–20.

Al-Shaqi, R., Mourshed, M., & Rezgui, Y. (2016). Progress in ambient assisted systems for independent living by the elderly. *SpringerPlus, 5*(1).

Alvesson, M., & Sandberg, J. (2011). Generating research questions through problematization. *Academy of Management Review, 36*(2), 247–271.

Alzahrani, T., Hunt, M., & Whiddett, D. (2021). Barriers and facilitators to using smart home technologies to support older adults: Perspectives of three stakeholder groups. *International Journal of Healthcare Information Systems and Informatics, 16*(4), 1–14.

Ancona, D. G., Goodman, P. S., Lawrence, B. S., & Tushman, M. L. (2001). Time: A new research lens. *Academy of Management Review, 26*(4), 645–663.

Arar, M., Jung, C., Awad, J., & Chohan, A. H. (2021). Analysis of smart home technology acceptance and preference for elderly in Dubai, UAE. *Designs, 5*(4), 70.

Arbabi, M. S., Lal, C., Veeraragavan, N. R., Marijan, D., Nygård, J. F., & Vitenberg, R. (2022). A survey on blockchain for healthcare: Challenges, benefits, and future directions. *IEEE Communications Surveys & Tutorials*, 386–424.

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

Bacharach, S. B. (1989). Organizational theories: Some criteria for evaluation. *Academy of Management Review, 14*(4), 496–515.

Balta-Ozkan, N., Davidson, R., Bicket, M., & Whitmarsh, L. (2013). Social barriers to the adoption of smart homes. *Energy Policy, 63*, 363–374.

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

Bantan, M., & Shawosh, M. (2024). Chief privacy officer: A systematic literature review and future research directions. *Communications of the Association for Information Systems, 54*(1), 13.

Banville, M. C. (2020). Resisting surveillance: Responding to wearable device privacy policies. In *Proceedings of the 38th ACM International Conference on Design of Communication*.

Beaudin, J. S., Intille, S. S., & Morris, M. E. (2006). To track or not to track: User reactions to concepts in longitudinal health monitoring. *Journal of Medical Internet Research, 8*(4), 1–29.

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

Bhatt, V., & Chakraborty, S. (2020, October 7–9). Importance of trust in IoT based wearable device adoption by patient: An empirical investigation. In *2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)*.

Blakely, T. A., & Woodward, A. J. (2000). Ecological effects in multi-level studies. *Journal of Epidemiology & Community Health, 54*(5), 367–374.

Burrows, A., Coyle, D., & Gooberman-Hill, R. (2018). Privacy, boundaries and smart homes for health: An ethnographic study. *Health & Place, 50*, 112–118.

Burton-Jones, A., McLean, E. R., & Monod, E. (2015). Theoretical perspectives in IS research: From variance and process to conceptual latitude and conceptual fit. *European Journal of Information Systems, 24*(6), 664–679.

Butpheng, C., Yeh, K.-H., & Xiong, H. (2020). Security and privacy in IoT-cloud-based e-health systems—A comprehensive review. *Symmetry, 12*(7), 1191.

Califf, C. B., Sarker, S., & Sarker, S. (2020). The bright and dark sides of technostress: A mixed-methods study involving healthcare IT. *MIS Quarterly, 44*(2).

Campbell, J. E., & Carlson, M. (2002). Panopticon.com: Online surveillance and the commodification of privacy. *Journal of Broadcasting & Electronic Media, 46*(4), 586–606.

Capterra.com. (2021). *New technologies for telehealth in Canada: 61% of Canadians want to implement AI.* Retrieved from https://www.capterra.ca/blog/2039/telehealth-in-canada-technology-ai

Carver, L. F., & Mackinnon, D. (2020). Health applications of gerontechnology, privacy, and surveillance: A scoping review. *Surveillance & Society, 18*(2), 216–230.

Chadborn, N. H., Blair, K., Creswick, H., Hughes, N., Dowthwaite, L., Adenekan, O., & Pérez Vallejos, E. (2019). Citizens' juries: When older adults deliberate on the benefits and risks of smart health and smart homes. *Healthcare, 7*(54), 1–17.

Chalhoub, G., Kraemer, M. J., & Flechais, I. (2024). Useful shortcuts: Using design heuristics for consent and permission in smart home devices. *International Journal of Human-Computer Studies, 182*, 103177.

Chalhoub, G., Kraemer, M. J., Nthala, N., & Flechais, I. (2021). "It did not give me an option to decline": A longitudinal analysis of the user experience of security and privacy in smart home products. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*.

Chen, Y., Zhang, L., & Wei, M. (2021). How does smart healthcare service affect resident health in the digital age? Empirical evidence from 105 cities of China. *Frontiers in Public Health, 9*, 1–9.

Choi, J. R., & Kim, S. (2024). Predicting individuals' privacy protection and self-tracking behaviors in the context of smart health. *Telematics and Informatics, 86*, 102069.

Choi, Y. K., Thompson, H. J., & Demiris, G. (2020). Use of an internet-of-things smart home system for healthy aging in older adults in residential settings: Pilot feasibility study. *JMIR Aging, 3*(2).

Cilliers, L., & Flowerday, S. (2014). User acceptance of telemedicine by health care workers: A case of the Eastern Cape Province, South Africa. *The Electronic Journal of Information Systems in Developing Countries, 65*(1), 1–10.

Clarke, R. (1994). Dataveillance by governments. *Information Technology & People, 7*(2), 46–85.

Clarke, R. (2019). Risks inherent in the digital surveillance economy: A research agenda. *Journal of Information Technology, 34*(1), 59–80.

CNBC.com. (2022). *The biggest security risks of using fitness trackers and apps to monitor your health.* Retrieved from https://www.cnbc.com/2022/11/26/the-biggest-risks-of-using-fitness-trackers-to-monitor-health.html

Cristiano, A., Musteata, S., De Silvestri, S., Bellandi, V., Ceravolo, P., Cesari, M., Azzolino, D., Sanna, A., & Trojaniello, D. (2022). Older adults' and clinicians' perspectives on a smart health platform for the aging population: Design and evaluation study. *JMIR Aging, 5*(1), e29623.

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues, 59*(2), 323–342.

Dadhich, M., Hiran, K. K., Rao, S. S., & Sharma, R. (2022). Factors influencing patient adoption of the IoT for e-health management systems (e-HMS) using the UTAUT model: A high order SEM-ANN approach. *International Journal of Ambient Computing and Intelligence, 13*(1), 1–18.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319–340.

Davison, R. M., & Martinsons, M. G. (2016). Context is king! Considering particularism in research design and reporting. *Journal of Information Technology, 31*, 241–249.

de Guinea, A. O., & Webster, J. (2017). Combining variance and process in information systems research: Hybrid approaches. *Information and Organization, 27*(3), 144–162.

De Moya, J. F., & Pallud, J. (2020). From panopticon to heautopticon: A new form of surveillance introduced by quantified-self practices. *Information Systems Journal, 30*(6), 940–976.

Degirmenci, K. (2020). Mobile users' information privacy concerns and the role of app permission requests. *International Journal of Information Management, 50*, 261–272.

del Río-Lanza, A.-B., Suárez-Vázquez, A., Suárez-Álvarez, L., & Iglesias-Argüelles, V. (2020). Mobile health (mHealth): Facilitators and barriers of the intention of use in patients with chronic illnesses. *Journal of Communication in Healthcare, 13*(2), 138–146.

Deloitte. (2019). *Smart health communities and the future of health*. Retrieved from https://www2.deloitte.com/us/en/insights/industry/health-care/smart-health-communities.html

Deng, Z., Hong, Z., Ren, C., Zhang, W., & Xiang, F. (2018). What predicts patients' adoption intention toward mHealth services in China: Empirical study. *JMIR Mhealth Uhealth, 6*(8), 1–14.

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents - Measurement validity and a regression model. *Behaviour & Information Technology, 23*(6), 413–422.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. (2006). Privacy calculus model in e-commerce – A study of Italy and the United States. *European Journal of Information Systems, 15*(4), 389–402.

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

Duckert, M., & Barkhuus, L. (2022). Protecting personal health data through privacy awareness: A study of perceived data privacy among people with chronic or long-term illness. *Proceedings of the ACM on Human-Computer Interaction, 6*(GROUP), 1–22.

Edwards, V. M., & Steins, N. A. (1999). A framework for analysing contextual factors in common pool resource research. *Journal of Environmental Policy & Planning, 1*(3), 205–221.

El-Masri, M., & Tarhini, A. (2017). Factors affecting the adoption of e-learning systems in Qatar and USA: Extending the unified theory of acceptance and use of technology 2 (UTAUT2). *Educational Technology Research and Development, 65*(3), 743–763.

Esmaeilzadeh, P. (2019). The process of building patient trust in health information exchange (HIE): The impacts of perceived benefits, perceived transparency of privacy policy, and familiarity. *Communications of the Association for Information Systems, 45*, 364–396.

Esmaeilzadeh, P. (2023). Older adults' perceptions about using intelligent toilet seats beyond traditional care: Web-based interview survey. *JMIR mHealth and uHealth, 11*(1).

Essén, A. (2008). The two facets of electronic care surveillance: An exploration of the views of older people who live with monitoring devices. *Social Science & Medicine, 67*(1), 128–136.

Etemad-Sajadi, R., & Dos Santos, G. G. (2019). Senior citizens' acceptance of connected health technologies in their homes. *International Journal of Health Care Quality Assurance, 32*(8), 1162–1174.

Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á. O., & Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. *Journal of Biomedical Informatics, 46*(3), 541–562.

Finch, K., & Tene, O. (2014). Welcome to the metropticon: Protecting privacy in a hyperconnected town. *Fordham Urban Law Journal, 41*(5), 1581–1616.

Fishbein, M., & Ajzen, I. (1977). Belief, attitude, intention, and behavior: An introduction to theory and research. *Philosophy and Rhetoric, 10*(2).

Fortune.com. (2023). The best technology to prevent falls, monitor safety, and help older adults age in place longer. Retrieved from https://fortune.com/well/2023/02/03/technology-can-help-older-adults-age-in-place-longer/

Fox, G., & James, T. L. (2021). Toward an understanding of the antecedents to health information privacy concern: A mixed methods study. *Information Systems Frontiers, 23*(6), 1537–1562.

Fox, G., Clohessy, T., van der Werff, L., Rosati, P., & Lynn, T. (2021). Exploring the competing influences of privacy concerns and positive beliefs on citizen acceptance of contact tracing mobile applications. *Computers in Human Behavior, 121*, 106806.

Fox, G., van der Werff, L., Rosati, P., Takako Endo, P., & Lynn, T. (2021). Examining the determinants of acceptance and use of mobile contact tracing applications in Brazil: An extended privacy calculus perspective. *Journal of the Association for Information Science and Technology*, *73*(7), 944-967.

Fritz, R. L., Corbett, C. L., Vandermause, R., & Cook, D. (2016). The influence of culture on older adults' adoption of smart home monitoring. *Gerontechnology, 14*(3), 146–156.

Ghorayeb, A., Comber, R., & Gooberman-Hill, R. (2021). Older adults' perspectives of smart home technology: Are we developing the technology that older people want? *International Journal of Human Computer Studies, 147*, 1–13.

GlobeNewswire. (2023). Smart medical devices market expecting to hit USD 474 Billion by 2032, with a CAGR of 12.3%. Retrieved from https://www.globenewswire.com/news-release/2023/12/13/2795357/0/en/Smart-Medical-Devices-Market-Expecting-to-Hit-USD-474-Billion-by-2032-with-a-CAGR-of-12-3-Market-us.html

Grand View Research. (2023). Video surveillance market size, share & trends analysis report by component, by system, by end use, by vertical, by region, and segment forecasts, 2023–2030. Retrieved from https://www.grandviewresearch.com/industry-analysis/video-surveillance-market-report

Grant, M. J., & Booth, A. (2009). A typology of reviews: An analysis of 14 review types and associated methodologies. *Health Information & Libraries Journal, 26*(2), 91–108.

Greco, L., Percannella, G., Ritrovato, P., Tortorella, F., & Vento, M. (2020). Trends in IoT based solutions for health care: Moving AI to the edge. *Pattern Recognition Letters, 135*, 346–353.

Grill, E., Müller, M., & Mansmann, U. (2016). Supplement issue: Health—Exploring complexity: An interdisciplinary systems approach. *European Journal of Epidemiology*, *32*(2), 167.

Hassan, A. H., Sulaiman, R. B., Abdulgabber, M. A., & Kahtan, H. (2023). Balancing technological advances with user needs: User-centered principles for AI-driven smart city healthcare monitoring. *International Journal of Advanced Computer Science and Applications, 14*(3), 365–376.

Hassandoust, F., Johnston, A., & Singh, T. (2021). Smart pay-as-you-live services in healthcare: A balance theory perspective. In *ICIS 2021 Proceedings*.

Hunter, I., Elers, P., Lockhart, C., Guesgen, H., Singh, A., & Whiddett, D. (2020). Issues associated with the management and governance of sensor data and information to assist aging in place: Focus group study with health care professionals. *JMIR Mhealth Uhealth, 8*(12), 1–10.

Ismail, L., Materwala, H., Karduck, A. P., & Adem, A. (2020). Requirements of health data management systems for biomedical care and research: Scoping review. *Journal of Medical Internet Research, 22*(7), N.PAG.

Jaime, F. J., Muñoz, A., Rodríguez-Gómez, F., & Jerez-Calero, A. (2023). Strengthening privacy and data security in biomedical microelectromechanical systems by IoT communication security and protection in smart healthcare. *Sensors (Basel, Switzerland), 23*(21).

Jakobi, T., Patil, S., Randall, D., Stevens, G., & Wulf, V. (2019). It is about what they could do with the data: A user perspective on privacy in smart metering. *ACM Transactions on Computer-Human Interaction, 26*(1), 2:1–2:44.

Janamian, T., Crossland, L., & Jackson, C. L. (2016). Embracing value co-creation in primary care services research: A framework for success. *Medical Journal of Australia, 204*(S7), S5–S11.

Kaplan, H. C., Brady, P. W., Dritz, M. C., Hooper, D. K., Linam, W. M., Froehle, C. M., & Margolis, P. (2010). The influence of context on quality improvement success in health care: A systematic review of the literature. *The Milbank Quarterly, 88*(4), 500–559.

Karahoca, A., Karahoca, D., & Aksöz, M. (2018). Examining intention to adopt to internet of things in healthcare technology products. *Kybernetes, 47*(4), 742–770.

Kennedy, M.-R., Huxtable, R., Birchley, G., Ives, J., & Craddock, I. (2021). "A question of trust" and "a leap of faith"—Study participants' perspectives on consent, privacy, and trust in smart home research: Qualitative study. *JMIR Mhealth Uhealth, 9*(11), e25227.

Keshta, I. (2022). AI-driven IoT for smart health care: Security and privacy issues. *Informatics in Medicine Unlocked, 30*, 100903.

Kim, B., Kam, H. J., Park, Y. R., Yoo, S., Oh, J. S., Kim, Y.-H., & Lee, J.-H. (2018). Enchanted life space: Adding value to smart health by integrating human desires. *Healthcare Informatics Research, 24*(1), 3–11.

Kitchenham, B., & Charters, S. (2007). *Guidelines for performing systematic literature reviews in software engineering*. Retrieved from https://legacyfileshare.elsevier.com/promis_misc/525444systematicreviewsguide.pdf

Kulyk, O., Reinheimer, B., Aldag, L., Mayer, P., Gerber, N., & Volkamer, M. (2020). Security and privacy awareness in smart environments–A cross-country investigation. In *Proceedings of AsiaUSEC 2020, Financial Cryptography and Data Security*.

Kumar, R., Singh, D., Srinivasan, K., & Hu, Y. C. (2023). AI-powered blockchain technology for public health: A contemporary review, open challenges, and future research directions. *Healthcare, 11*(1), 81.

Kwiecień, I., Kowalczyk-Rolczynska, P., & Popielas, M. (2020). Are the generations ready to accept the new technologies in life insurance underwriting? Questionnaire study in Poland. *IBIMA Business Review, 2020*(2020), 539912.

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues, 33*(3), 22–42.

LeBaron, V., Bennett, R., Alam, R., Blackhall, L., Gordon, K., Hayes, J., Homdee, N., Jones, R., Martinez, Y., Ogunjirin, E., Thomas, T., & Lach, J. (2020). Understanding the experience of cancer pain from the perspective of patients and family caregivers to inform design of an in-home smart health system: Multimethod approach. *JMIR Formative Research, 4*(8).

Li, J., Silvera-Tawil, D., Varnfield, M., Hussain, M. S., & Math, V. (2021). Users' perceptions toward mHealth technologies for health and well-being monitoring in pregnancy care: Qualitative interview study. *JMIR Formative Research, 5*(12).

Li, Y. (2011). Empirical studies on online information privacy concerns: Literature review and an integrative framework. *Communications of the Association for Information Systems, 28*(28), 453–496.

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

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

Liu, K., & Tao, D. (2022). The roles of trust, personalization, loss of privacy, and anthropomorphism in public acceptance of smart healthcare services. *Computers in Human Behavior, 127*.

Lu, L., Zhang, J., Xie, Y., Gao, F., Xu, S., Wu, X., & Ye, Z. (2020). Wearable health devices in health care: Narrative systematic review. *JMIR Mhealth and Uhealth, 8*(11).

Lu, X., Hao, J., Shan, B., & Gu, A. (2021). Determinants of the intention to use smart healthcare devices: A framework and public policy implications. *Journal of Healthcare Engineering, 2021*.

Lyles, C. R., Adler-Milstein, J., Thao, C., Lisker, S., Nouri, S., & Sarkar, U. (2021). Alignment of key stakeholders' priorities for patient-facing tools in digital health: Mixed methods study. *Journal of Medical Internet Research, 23*(8), e24890.

Lyon, D. (2003). *Surveillance as social sorting: Privacy, risk and digital discrimination*. Routledge.

Lyon, D. (2007). *Surveillance studies: An overview*. Polity Press.

Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., & Hung Byers, A. (2011). *Big data: The next frontier for innovation, competition, and productivity*. McKinsey Global Institute.

Market.Us. (2023). *Global smart medical devices market*. Retrieved from https://market.us/report/smart-medical-devices-market/

Markus, M. L., & Robey, D. (1988). Information technology and organizational change: Causal structure in theory and research. *Management Science, 34*(5), 583–598.

Matt, C., Becker, M., Kolbeck, A., & Hess, T. (2019). Continuously healthy, continuously used?–A thematic analysis of user perceptions on consumer health wearables. *Pacific Asia Journal of the Association for Information Systems, 11*(1), 108–132.

May, C. R., Mair, F., Finch, T., MacFarlane, A., Dowrick, C., Treweek, S., Rapley, T., Ballini, L., Ong, B. N., & Rogers, A. (2009). Development of a theory of implementation and integration: Normalization Process Theory. *Implementation Science, 4*(1), 1–9.

Meier, C. A., Fitzgerald, M. C., & Smith, J. M. (2013). eHealth: Extending, enhancing, and evolving health care. *Annual Review of Biomedical Engineering, 15*, 359–382.

Mettler, T., & Wulf, J. (2020). Health promotion with physiolytics: What is driving people to subscribe in a data-driven health plan. *PLoS One, 15*(4), e0231705.

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

Miyachi, K., & Mackey, T. K. (2021). hOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design. *Information Processing and Management, 58*(3), 102535.

Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G., & Group, P. (2009). Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *PLoS Medicine, 6*(7), e1000097.

Mordor Intelligence. (2024). *Video surveillance market - Growth, trends, COVID-19 impact, and forecasts (2024–2029)*. Retrieved from https://www.mordorintelligence.com/industry-reports/video-surveillance-market

Mueller, B., & Urbach, N. (2017). Understanding the why, what, and how of theories in IS research. *Communications of the Association for Information Systems, 41*, 349–388.

Mujirishvili, T., Maidhof, C., Florez-Revuelta, F., Ziefle, M., Richart-Martinez, M., & Cabrero-García, J. (2023). Acceptance and privacy perceptions toward video-based active and assisted living technologies: Scoping review. *Journal of Medical Internet Research, 25*, e45297.

Mulligan, D. K., Koopman, C., & Doty, N. (2016). Privacy is an essentially contested concept: A multi-dimensional analytic for mapping privacy. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 374*(2083), 20160118.

Nelson, E. C., Verhagen, T., & Noordzij, M. L. (2016). Health empowerment through activity trackers: An empirical smart wristband study. *Computers in Human Behavior, 62*, 364–374.

New Zealand IoT Alliance. (2017). *An analysis of the impact of the Internet of Things on the New Zealand economy*. Retrieved from https://iotalliance.org.nz/wp-content/uploads/sites/4/2018/09/Accelerating-a-Connected-New-Zealand-eBOOK.pdf

Newell, P. B. (1995). Perspectives on privacy. *Journal of Environmental Psychology, 15*(2), 87–104.

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

Nissenbaum, H. (2018). Respecting context to protect privacy: Why meaning matters. *Science and Engineering Ethics, 24*(3), 831–852.

OECD. (2015). *Introducing high-value, privacy-protective health information systems*. Retrieved from https://www.oecd.org/content/dam/oecd/en/publications/reports/2015/10/health-data-governance_g1g5a9e9/9789264244566-en.pdf

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

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., McGuinness, L. A., Stewart, L. A., Thomas, J., Tricco, A. C., Welch, V. A., Whiting, P., & Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *British Medical Journal, 372*(n71), 1–9.

Pan, J., Ding, S., Wu, D., Yang, S., & Yang, J. (2019). Exploring behavioural intentions toward smart healthcare services among medical practitioners: A technology transfer perspective. *International Journal of Production Research, 57*(18), 5801–5820.

Pang, P. C.-I., McKay, D., Chang, S., Chen, Q., Zhang, X., & Cui, L. (2020). Privacy concerns of the Australian My Health Record: Implications for other large-scale opt-out personal health records. *Information Processing & Management, 57*(6), 102364.

Papa, A., Mital, M., Pisano, P., & Del Giudice, M. (2020). E-health and wellbeing monitoring using smart healthcare devices: An empirical investigation. *Technological Forecasting and Social Change, 153*, 119226.

Paré, G., Tate, M., Johnstone, D., & Kitsiou, S. (2016). Contextualizing the twin concepts of systematicity and transparency in information systems literature reviews. *European Journal of Information Systems, 25*(6), 493–508.

Pavlou, P. A. (2011). State of the information privacy literature: Where are we now and where should we go? *MIS Quarterly, 35*(4), 977–988.

Peek, S. T. M., Wouters, E. J., Luijkx, K. G., & Vrijhoef, H. J. (2016). What it takes to successfully implement technology for aging in place: Focus groups with stakeholders. *Journal of Medical Internet Research, 18*(5), e98.

Plangger, K., & Montecchi, M. (2020). Thinking beyond privacy calculus: Investigating reactions to customer surveillance. *Journal of Interactive Marketing, 50*, 32–44.

Polyviou, A., Pouloudi, N., Pramatari, K., & Silva, L. O. (2024). A DNA helix analogy for interdependent mixed methods research: Enabling cross-fertilizations and interim meta-inferences. *Journal of the Association for Information Systems, 25*(6), 1585–1627.

Pool, J., Akhlaghpour, S., Fatehi, F., & Burton-Jones, A. (2024). A systematic analysis of failures in protecting personal health data: A scoping review. *International Journal of Information Management, 74*, 102719.

Princi, E., & Krämer, N. C. (2020). Out of control – Privacy calculus and the effect of perceived control and moral considerations on the usage of IoT healthcare devices. *Frontiers in Psychology, 11*, 1–15.

Rahman, M. J., Morshed, B. I., Harmon, B., & Rahman, M. (2022). A pilot study towards a smart-health framework to collect and analyze biomarkers with low-cost and flexible wearables. *Smart Health, 23*.

Ramaswamy, V., & Ozcan, K. (2014). *The co-creation paradigm*. Stanford University Press.

Rashidi, P., & Mihailidis, A. (2013). A survey on ambient-assisted living tools for older adults. *IEEE Journal of Biomedical and Health Informatics, 17*(3), 579–590.

Ratta, P., Kaur, A., Sharma, S., Shabaz, M., & Dhiman, G. (2021). Application of blockchain and Internet of Things in healthcare and medical sector: Applications, challenges, and future perspectives. *Journal of Food Quality*, 1–20.

Ravishankar, V. K., Burleson, W., & Mahoney, D. (2015). Smart home strategies for user-centered functional assessment of older adults. *International Journal of Automation and Smart Technology, 5*(4), 233–242.

Renukappa, S., Mudiyi, P., Suresh, S., Abdalla, W., & Subbarao, C. (2022). Evaluation of challenges for adoption of smart healthcare strategies. *Smart Health, 26*, 100330.

Renwick, R., & Gleasure, R. (2021). Those who control the code control the rules: How different perspectives of privacy are being written into the code of blockchain systems. *Journal of Information Technology, 36*(1), 16–38.

Rissel, C. (1994). Empowerment: The holy grail of health promotion? *Health Promotion International, 9*(1), 39–47.

Rogers, E. M. (2003). *Diffusion of innovations* (5th ed.). Free Press.

Rouidi, M., Elouadi, A. E., Hamdoune, A., Choujtani, K., & Chati, A. (2022). TAM-UTAUT and the acceptance of remote healthcare technologies by healthcare professionals: A systematic review. *Informatics in Medicine Unlocked, 32*, 101008.

Ruhlandt, R. W. S. (2018). The governance of smart cities: A systematic literature review. *Cities, 81*, 1–23.

Runkle, J., Sugg, M., Boase, D., Galvin, S. L., & Coulson, C. (2019). Use of wearable sensors for pregnancy health and environmental monitoring: Descriptive findings from the perspective of patients and providers. *Digital Health, 5*, 1–14.

Sahin, I. (2006). Detailed review of Rogers' diffusion of innovations theory and educational technology-related studies based on Rogers' theory. *Turkish Online Journal of Educational Technology, 5*(2), 14–23.

Sayibu, M., Chu, J., Akintunde, T. Y., Rufai, O. H., Amosun, T. S., & George-Ufot, G. (2022). Environmental conditions, mobile digital culture, mobile usability, knowledge of app in COVID-19 risk mitigation: A structural equation model analysis. *Smart Health, 2022*(Sep. 25), 100286.

Schiavone, F., Mancini, D., Leone, D., & Lavorato, D. (2021). Digital business models and ridesharing for value co-creation in healthcare: A multi-stakeholder ecosystem analysis. *Technological Forecasting and Social Change, 166*, 120647.

Schlackl, F., Link, N., & Hoehle, H. (2022). Antecedents and consequences of data breaches: A systematic review. *Information & Management*, *59*(4),103638.

Schoeman, F. (1984). Privacy: Philosophical dimensions. *American Philosophical Quarterly, 21*(3), 199–213.

Seberger, J. S., & Patil, S. (2021). Post-COVID public health surveillance and privacy expectations in the United States: Scenario-based interview study. *JMIR Mhealth Uhealth, 9*(10), e30871.

Seiferth, A., & Schaarschmidt, M. (2020). Sharing personal health and fitness data with health insurance providers: An empirical study considering trust and risk. In *Proceedings of the 53rd Hawaii International Conference on System Sciences*.

Shachak, A., Kuziemsky, C., & Petersen, C. (2019). Beyond TAM and UTAUT: Future directions for HIT implementation research. *Journal of Biomedical Informatics, 100*, 103315.

Shah, R., & Ward, P. T. (2003). Lean manufacturing: Context, practice bundles, and performance. *Journal of Operations Management, 21*(2), 129–149.

Shalley, C. E., Zhou, J., & Oldham, G. R. (2004). The effects of personal and contextual characteristics on creativity: Where should we go from here? *Journal of Management, 30*(6), 933–958.

Shen, N., Bernier, T., Sequeira, L., Strauss, J., Silver, M. P., Carter-Langford, A., & Wiljer, D. (2019). Understanding the patient privacy perspective on health information exchange: A systematic review. *International Journal of Medical Informatics, 125*, 1–12.

Shimizu, Y., Ishizuna, A., Osaki, S., Hashimoto, T., Tai, M., Tanibe, T., & Karasawa, K. (2022). The social acceptance of smart health services in Japan. *International Journal of Environmental Research and Public Health, 19*(3), 1298.

Shimizu, Y., Osaki, S., Hashimoto, T., & Karasawa, K. (2021). How do people view various kinds of smart city services? Focus on the acquisition of personal information. *Sustainability, 13*(19).

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

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

Solove, D. J. (2002). Conceptualizing privacy. *California Law Review, 90*(4), 1087–1155.

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review, 154*(3), 477–564.

Solove, D. J. (2007). I've got nothing to hide and other misunderstandings of privacy. *San Diego Law Review, 44*, 745–772.

Someh, I., Davern, M., Breidbach, C. F., & Shanks, G. (2019). Ethical issues in big data analytics: A stakeholder perspective. *Communications of the Association for Information Systems, 44*, 718–747.

Spreitzer, G. M. (1995). Psychological empowerment in the workplace: Dimensions, measurement, and validation. *Academy of Management Journal, 38*(5), 1442–1465.

Stavropoulos, T. G., Papastergiou, A., Mpaltadoros, L., Nikolopoulos, S., & Kompatsiaris, I. (2020). IoT wearable sensors and devices in elderly care: A literature review. *Sensors, 20*(10), 2826.

Stewart, K., & Segars, A. (2002). An empirical examination of the concern for information privacy instrument. *Information Systems Research, 13*, 36–49.

Suddaby, R. (2006). From the editors: What grounded theory is not. *Academy of Management Journal, 49*(4), 633–642.

Suman, A. B. (2017). In search for the value of connectivity: Accountable citizens fostering accountable governance via connectivity: The case of environmental health policies. In *2017 IEEE International Conference on Cloud Engineering (IC2E)*.

Sutton, R. I., & Staw, B. M. (1995). What theory is not. *Administrative Science Quarterly*, 40(3), 371–384.

Swinkels, I. C. S., Huygens, M. W. J., Schoenmakers, T. M., Nijeweme-D'Hollosy, W. O., Van Velsen, L., Vermeulen, J., Schoone-Harmsen, M., Jansen, Y. J., Van Schayck, O. C., & Friele, R. (2018). Lessons learned from a living lab on the broad adoption of eHealth in primary health care. *Journal of Medical Internet Research, 20*(3), e83.

Talal, M., Zaidan, A., Zaidan, B., Albahri, A. S., Alamoodi, A., Albahri, O. S., Alsalem, M., Lim, C. K., Tan, K. L., Shir, W., & Mohammed, K. I. (2019). Smart home-based IoT for real-time and secure remote health monitoring of triage and priority system using body sensors: Multi-driven systematic review. *Journal of Medical Systems, 43*(3).

Tallon, P. P. (2013). Corporate governance of big data: Perspectives on value, risk, and cost. *Computer, 46*(6), 32–38.

Thelancet.com. (2023). *Wearable health data privacy*. Retrieved from https://www.thelancet.com/journals/landig/article/PIIS2589-7500(23)00055-9/fulltext

Thiebes, S., Gao, F., Briggs, R. O., Schmidt-Kraepelin, M., & Sunyaev, A. (2023). Design concerns for multiorganizational, multistakeholder collaboration: A study in the healthcare industry. *Journal of Management Information Systems, 40*(1), 239–270.

Tran, C. D., & Nguyen, T. T. (2021). Health vs. privacy? The risk-risk tradeoff in using COVID-19 contact-tracing apps. *Technology in Society, 67*, 101755.

Ullah, F., Qayyum, S., Thaheem, M. J., Al-Turjman, F., & Sepasgozar, S. M. (2021). Risk management in sustainable smart cities governance: A TOE framework. *Technological Forecasting and Social Change, 167*.

Valle-Cruz, D. (2019). Public value of e-government services through emerging technologies. *International Journal of Public Sector Management, 32*(5), 530–545.

Venkatesh, V., Brown, S. A., & Bala, H. (2013). Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. *MIS Quarterly, 37*(1), 21–54.

Venkatesh, V., Brown, S. A., & Sullivan, Y. W. (2016). Guidelines for conducting mixed-methods research: An extension and illustration. *Journal of the Association for Information Systems, 17*(7), 435–495.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly, 27*(3), 425–478.

Venkatesh, V., Thong, J. Y., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly, 36*(1), 157–178.

Wagner, G., Prester, J., Roche, M. P., Schryen, G., Benlian, A., Paré, G., & Templier, M. (2021). Which factors affect the scientific impact of review papers in IS research? A scientometric study. *Information & Management, 58*(3), 103427.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, 4*(5), 193–220.

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly, 26*(2), xiii–xxiii.

Weiss, L., & Johar, G. V. (2013). Egocentric categorization and product judgment: Seeing your traits in what you own (and their opposite in what you don't). *Journal of Consumer Research, 40*(1), 185–201.

Wiegard, R.-B., & Breitner, M. H. (2019). Smart services in healthcare: A risk-benefit-analysis of pay-as-you-live services from customer perspective in Germany. *Electronic Markets, 29*(1), 107–123.

Windasari, N. A., Lin, F., & Kato-Lin, Y. (2021). Continued use of wearable fitness technology: A value co-creation perspective. *International Journal of Information Management, 57*, 102292.

Winter, J. S., & Davidson, E. (2019). Big data governance of personal health information and challenges to contextual integrity. *The Information Society, 35*(1), 36–51.

Winter, J. S., & Davidson, E. (2022). Harmonizing regulatory regimes for the governance of patient-generated health data. *Telecommunications Policy, 46*(5), 102285.

Xing, F., Peng, G., Zhang, B., Li, S., & Liang, X. (2021). Socio-technical barriers affecting large-scale deployment of AI-enabled wearable medical devices among the ageing population in China. *Technological Forecasting and Social Change, 166*, 120609.

Xu, H., & Bélanger, F. (2013). Information systems journal special issue on: Reframing privacy in a networked world. *Information Systems Journal, 23*(4), 371–375.

Xu, H., & Zhang, N. (2022). From contextualizing to context theorizing: Assessing context effects in privacy research. *Management Science, 68*(10), 7383–7401.

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems, 12*(12), 798–824.

Xu, Z. (2019). An empirical study of patients' privacy concerns for health informatics as a service. *Technological Forecasting and Social Change, 143*, 297–306.

Yang, C. (2022). Digital contact tracing in the pandemic cities: Problematizing the regime of traceability in South Korea. *Big Data and Society, 9*(1).

Zaman, U., Mehmood, F., Iqbal, N., Kim, J., & Ibrahim, M. (2022). Towards secure and intelligent Internet of Health Things: A survey of enabling technologies and applications. *Electronics (Switzerland), 11*(12), 1–43.

Zhang, F., Pan, Z., & Lu, Y. (2023). AIoT-enabled smart surveillance for personal data digitalization: Contextual personalization-privacy paradox in smart home. *Information & Management, 60*(2), 103736.

Zhang, J., Li, H., Luo, X., & Warkentin, M. (2017). Exploring the effects of the privacy-handling management styles of social networking sites on user satisfaction: A conflict management perspective. *Decision Sciences, 48*(5), 956–989.

Zhang, N. A., Wang, C. A., Karahanna, E., & Xu, Y. (2022). Peer privacy concern: Conceptualization and measurement. *MIS Quarterly, 46*(1), 491–530.

Zhang, Y., Liu, C., Luo, S., Xie, Y., Liu, F., Li, X., & Zhou, Z. (2019). Factors influencing patients' intentions to use diabetes management apps based on an extended Unified Theory of Acceptance and Use of Technology model: Web-based survey. *Journal of Medical Internet Research, 21*(8), e15023.

Zhu, Y., Lu, Y., Gupta, S., Wang, J., & Hu, P. (2022). Promoting smart wearable devices in the health-AI market: The role of health consciousness and privacy protection. *Journal of Research in Interactive Marketing, 17*(2), 257–272.

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology, 30*(1), 75–89.

Zuboff, S. (2019). 'We make them dance': Surveillance capitalism, the rise of instrumentarian power, and the threat to human rights. In *Human rights in the age of platforms* (pp. 3–51). MIT Press.

# Appendix A: Previous Review Studies on Privacy in the Health Information Technology Domain

**Table A1. Previous Review Studies on Privacy in the Health Information Technology Domain**

| Article | Study context | Review type | Search strategy | | | | | Included studies | Contextual definition | Highlight of contextual matters | | Theoretical model | Method | Research agenda |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Keywords | Database | Coverage date | Inclusion / exclusion | Process of screening and selection | | | Antecedent | Outcome | | | |
| Al-rawashdeh et al. (2022) | IoT adoption and smart healthcare | Systematic review | ✓ | ✓ | 2015 - 2021 | ✓ ✓ | ✓ | 22 | N/A | N/A | ✓ | N/A | ✓ | N/A |
| Al-Shaqi et al. (2016) | Ambient assisted living systems (AALS) | Comprehensive and critical review | ✓ | ✓ | 2001 - 2016 | ✓ | Not clear | 133 | N/A | N/A | N/A | N/A | N/A | N/A |
| Carver and Mackinnon (2020) | Wearables and smart home or ambient assistive living (AAL) devices | Scoping review | ✓ | ✓ | 2007 - 2018 | ✓ | ✓ | 20 | N/A | Surveillance | N/A | N/A | N/A | N/A |
| Hassan et al. (2023) | AI-driven smart city healthcare monitoring | Systematic review | ✓ | ✓ | N/A | Not clear | ✓ | 70 | N/A | N/A | Not clear | N/A | N/A | N/A |
| Ismail et al. (2020) | eHealth | Scoping Review | N/A | ✓ | 1793 - 2020 | ✓ | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A |
| Keshta (2022) | AI-driven IoT for smart health care | Systematic review | ✓ | ✓ | N/A | ✓ | ✓ | 50 | N/A | N/A | N/A | N/A | N/A | Not clear |
| Kumar et al. (2023) | AI-powered blockchain for public | Contemporary review, Systematic | | ✓ | 2012 - 2022 | ✓ ✓ | ✓ | 120 | N/A | N/A | N/A | N/A | N/A | Not clear |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Health, smart health applications | review | | | | | | | | | | | | |
| Lu et al. (2020) | Wearable health devices in health care | Narrative systematic review | ✓ | ✓ | 2015-2019 | ✓<br>✓ | ✓ | 82 | N/A | N/A | N/A | N/A | N/A | Not clear |
| Mujirishvili et al. (2023) | Active and assisted living (AAL) technologies | Scoping review | ✓ | ✓ | Up to 2021 | ✓<br>✓ | ✓ | 22 | N/A | Not clear | ✓ | N/A | ✓ | N/A |
| Ratta et al. (2021) | IoT and blockchain in healthcare systems | Not specify | Not clear | ✓ | 2008-2020 | ✓<br>✓ | Not clear | 22 | N/A | Not clear | N/A | N/A | N/A | Not clear |
| Shen et al. (2019) | Health information exchange (HIE), health information technology (HIT) | Systematic review | ✓ | ✓ | 2004-2017 | ✓ | ✓ | 59 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Talal et al. (2019) | IoT-based smart home | Systematic review | ✓ | ✓ | 2007-2017 | ✓<br>✓ | ✓ | 9 | N/A | Not clear | N/A | N/A | N/A | ✓ |
| Zaman et al. (2022) | Internet of Health Things | Systematic review | ✓ | ✓ | 2016-2022 | ✓<br>✓ | Not clear | 384 | Not clear | ✓ | N/A | N/A | N/A | ✓ |

# Appendix B: The PRISMA 27-Item Checklist

**Table B1. The PRISMA 27-Item Checklist**

| Section and Topic | Item # | Checklist item | Location where item is reported |
|---|---|---|---|
| TITLE | | | |
| Title | 1 | Identify the report as a systematic review. | P.1 (Title page) |
| ABSTRACT | | | |
| Abstract | 2 | See the PRISMA 2020 for Abstracts checklist. | P.1 (Title page) |
| INTRODUCTION | | | |
| Rationale | 3 | Describe the rationale for the review in the context of existing knowledge. | P.4 - 8 |
| Objectives | 4 | Provide an explicit statement of the objective(s) or question(s) the review addresses. | P.5 |
| METHODS | | | |
| Eligibility criteria | 5 | Specify the inclusion and exclusion criteria for the review and how studies were grouped for the syntheses. | P.9 - 11 |
| Information sources | 6 | Specify all databases, registers, websites, organisations, reference lists and other sources searched or consulted to identify studies. Specify the date when each source was last searched or consulted. | P.9 – 10, P.15 |
| Search strategy | 7 | Present the full search strategies for all databases, registers and websites, including any filters and limits used. | P.9 - 13 |
| Selection process | 8 | Specify the methods used to decide whether a study met the inclusion criteria of the review, including how many reviewers screened each record and each report retrieved, whether they worked independently, and if applicable, details of automation tools used in the process. | P.9 - 11 |
| Data collection process | 9 | Specify the methods used to collect data from reports, including how many reviewers collected data from each report, whether they worked independently, any processes for obtaining or confirming data from study investigators, and if applicable, details of automation tools used in the process. | P.11 - 12 |
| Data items | 10a | List and define all outcomes for which data were sought. Specify whether all results that were compatible with each outcome domain in each study were sought (e.g. for all measures, time points, analyses), and if not, the methods used to decide which results to collect. | P.12 - 15 |
| | 10b | List and define all other variables for which data were sought (e.g. participant and intervention characteristics, funding sources). Describe any assumptions made about any missing or unclear information. | P.12 - 15 |
| Study risk of bias assessment | 11 | Specify the methods used to assess risk of bias in the included studies, including details of the tool(s) used, how many reviewers assessed each study and whether they worked independently, and if applicable, details of automation tools used in the process. | P.11 |
| Effect measures | 12 | Specify for each outcome the effect measure(s) (e.g. risk ratio, mean difference) used in the synthesis or presentation of results. | |
| Synthesis methods | 13a | Describe the processes used to decide which studies were eligible for each synthesis (e.g. tabulating the study intervention characteristics and comparing against the planned groups for each synthesis (item #5)). | P.9 - 12 |
| | 13b | Describe any methods required to prepare the data for presentation or synthesis, such as handling of missing summary statistics, or data conversions. | P.9 - 12 |
| | 13c | Describe any methods used to tabulate or visually display results of individual studies and syntheses. | P.12 -13 |
| | 13d | Describe any methods used to synthesize results and provide a rationale for the choice(s). If meta-analysis was performed, describe the model(s), method(s) to identify the presence and extent of statistical heterogeneity, and software package(s) used. | P.11 |
| | 13e | Describe any methods used to explore possible causes of | |

**Table B1. The PRISMA 27-Item Checklist**

| Section and Topic | Item # | Checklist item | Location where item is reported |
|---|---|---|---|
| | | heterogeneity among study results (e.g. subgroup analysis, meta-regression). | |
| | 13f | Describe any sensitivity analyses conducted to assess robustness of the synthesized results. | |
| Reporting bias assessment | 14 | Describe any methods used to assess risk of bias due to missing results in a synthesis (arising from reporting biases). | P.11 |
| Certainty assessment | 15 | Describe any methods used to assess certainty (or confidence) in the body of evidence for an outcome. | P.11 |
| RESULTS | | | |
| Study selection | 16a | Describe the results of the search and selection process, from the number of records identified in the search to the number of studies included in the review, ideally using a flow diagram. | P.15 - 16 |
| | 16b | Cite studies that might appear to meet the inclusion criteria, but which were excluded, and explain why they were excluded. | P.10 |
| Study characteristics | 17 | Cite each included study and present its characteristics. | P.15 |
| Risk of bias in studies | 18 | Present assessments of risk of bias for each included study. | |
| Results of individual studies | 19 | For all outcomes, present, for each study: (a) summary statistics for each group (where appropriate) and (b) an effect estimate and its precision (e.g. confidence/credible interval), ideally using structured tables or plots. | P.15 - 24 |
| Results of syntheses | 20a | For each synthesis, briefly summarise the characteristics and risk of bias among contributing studies. | |
| | 20b | Present results of all statistical syntheses conducted. If meta-analysis was done, present for each the summary estimate and its precision (e.g. confidence/credible interval) and measures of statistical heterogeneity. If comparing groups, describe the direction of the effect. | |
| | 20c | Present results of all investigations of possible causes of heterogeneity among study results. | |
| | 20d | Present results of all sensitivity analyses conducted to assess the robustness of the synthesized results. | |
| Reporting biases | 21 | Present assessments of risk of bias due to missing results (arising from reporting biases) for each synthesis assessed. | |
| Certainty of evidence | 22 | Present assessments of certainty (or confidence) in the body of evidence for each outcome assessed. | |
| DISCUSSION | | | |
| Discussion | 23a | Provide a general interpretation of the results in the context of other evidence. | P.24 - 25 |
| | 23b | Discuss any limitations of the evidence included in the review. | P.36 - 37 |
| | 23c | Discuss any limitations of the review processes used. | P.36 - 37 |
| | 23d | Discuss implications of the results for practice, policy, and future research. | P.29 - 36 |
| OTHER INFORMATION | | | |
| Registration and protocol | 24a | Provide registration information for the review, including register name and registration number, or state that the review was not registered. | |
| | 24b | Indicate where the review protocol can be accessed, or state that a protocol was not prepared. | |
| | 24c | Describe and explain any amendments to information provided at registration or in the protocol. | |
| Support | 25 | Describe sources of financial or non-financial support for the review, and the role of the funders or sponsors in the review. | |
| Competing interests | 26 | Declare any competing interests of review authors. | |
| Availability of data, | 27 | Report which of the following are publicly available and where they can be found: template data collection forms; data extracted from | |

**Table B1. The PRISMA 27-Item Checklist**

| Section and Topic | Item # | Checklist item | Location where item is reported |
|---|---|---|---|
| code and other materials | | included studies; data used for all analyses; analytic code; any other materials used in the review. | |

*Note.* From Page MJ, McKenzie JE, Bossuyt PM, Boutron I, Hoffmann TC, Mulrow CD, et al. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. BMJ 2021;372:n71. doi: 10.1136/bmj.n71

# Appendix C: Coding Results

**Table C1. Theories Used to Explain the Antecedents**

| Category | Antecedents | Privacy proxy | Theory |
|---|---|---|---|
| Individual | Perceived health information sensitivity | Perceived privacy risk | PCT (Wiegard & Breitner, 2019) |
| | Surveillance concerns | N/A | Theory of communicative action (Chadborn et al., 2019) |
| | Mobile users' information privacy concerns | Perceived privacy risk | MUIPC (Wiegard & Breitner, 2019) |
| Stakeholder | Stakeholders' experience of using mHealth | Perceived risk (including privacy risk) | Categorization theory (Pan et al., 2019) |
| | Implementation of data mechanisms | N/A | CI theory, Notions of borders (Burrows et al., 2018) |

For the individual antecedents, PCT was the most commonly used theory in privacy research. In the smart health domain, PCT was used as the extended risk-benefit analysis framework to predict the impact of perceived health information sensitivity on perceived privacy risk (Wiegard & Breitner, 2019). The MUIPC model was considered an important predictor of individuals' perception of privacy risk in a smart monitoring service (Wiegard & Breitner, 2019). In addition, the theory of communicative action was used to interpret the divergence between the experience and views of participants regarding their privacy concerns when using smart home monitoring devices (or services) (Chadborn et al., 2019).

In terms of organizational antecedents, categorization theory (or principles) was used to explain the interplay between individuals and products, proposing that customers classify the products they own as integral to their personal selves (Weiss & Johar, 2013). In the healthcare area, categorization theory was employed to interpret medical practitioners' initial impression and acceptance of smart healthcare. In this theory, customers' acceptance of a new product may be based on similarity with earlier products rather than on the technology itself (Pan et al., 2019). CI theory highlights a desirable state in which individuals strive to keep perceived private information private in accordance with the context (Nissenbaum, 2010). In the privacy and smart health monitoring literature, the notion of borders and CI theory were jointly used to explain the stakeholder antecedent, with the argument that data management mechanisms of smart homes should meet the criteria of robustness and plasticity inherent to boundary objects because they are associated with the privacy expectations of other household members in smart homes (Burrows et al., 2018).

**Table C2. Theories Used to Explain the Outcomes**

| Category | Outcomes | Privacy proxy | Theory |
|---|---|---|---|
| Individual | Adoption/use/participation | Perceived privacy risk | The concept of risk-risk tradeoff, PCT (Tran & Nguyen, 2021) |
| | | Privacy concerns | Unique theoretical framework of 'surveillance culture' (Choi & Kim, 2024) |
| | | N/A | IDT, Person-centered care (Fritz et al., 2016) |
| | | N/A | Balance theory (Hassandoust et al., 2021) |
| | Continuous use | N/A | UTAUT 2, HITAM, HIPC (Matt et al., 2019) |
| | Intention to adoption/use | N/A | UTAUT (Arar et al., 2021; Dadhich et al., 2022) |
| | | Privacy concerns | UTAUT (Zhu et al., 2022) |
| | | Perceived privacy risk | UTAUT (Zhang et al., 2019) |
| | | Privacy concerns | PCT, TPB (Princi & Krämer, 2020) |
| | | Perceived privacy risk | TAM, IDT, PMT, PCT (Karahoca et al., 2018) |
| | | Loss of privacy | TAM (Liu & Tao, 2022) |
| | Attitude toward adoption | Loss of privacy | TAM (Papa et al., 2020) |
| | Trust in technology/services | Loss of privacy | TAM (Liu & Tao, 2022) |
| | | N/A | TAM, TRA, TPB, UTAUT2 (Bhatt |

| | | | |
|---|---|---|---|
| | | | & Chakraborty, 2020) |
| | Perceived value | Perceived privacy risk | The concept of risk-risk tradeoff, PCT (Tran & Nguyen, 2021) |
| | | Perceived privacy risk | PCT, TPB, TRA (Wiegard & Breitner, 2019) |
| | Feelings of health empowerment | Privacy protection | Self-regulation theory (Nelson et al., 2016) |
| | Perceived usefulness | Loss of privacy | TAM (Papa et al., 2020) |
| | | N/A | UTAUT (Sayibu et al., 2022) |
| | Perceived ease of use | Loss of privacy | TAM (Papa et al., 2020) |
| Organizational | Medical practitioners' attitude to adopting smart healthcare services | N/A | Valence framework (Pan et al., 2019) |
| Stakeholder | Smart home development | N/A | Foucault's theory (governmentality and bio-power) (Suman, 2017) |
| | Implementation of smart health services | N/A | Normalization process theory (NPT) (Peek et al., 2016) |

In terms of the individual outcome aspect, theories of TAM, UTAUT, and/or UTAUT2 were commonly used to test individual-related outcomes affected by privacy. Based on the individual's perceived usefulness (PU) and perceived ease of use (EOU) of that information technology (Davis, 1989), TAM in smart health studies was extended with other characteristics, e.g., some AI-specific factors, to examine the impact of the loss of privacy on users' trust in smart technology and their adoption intention (Liu & Tao, 2022). UTAUT was formulated with four core determinants (i.e., experience, voluntariness, age, and gender) aiming to explain users' intentions to use information technology (Venkatesh et al., 2003). For instance, it was applied to test the relationship between privacy issues and individuals' intention to adopt certain smart health monitoring services (Dadhich et al., 2022). Extending UTAUT with three additional constructs of habit, price value, and hedonic motivation (El-Masri & Tarhini, 2017; Venkatesh et al., 2012), researchers combined UTAUT2 with other theories to explain the privacy impact on individuals' continuous use (e.g., Matt et al., 2019) and their trust in the new smart healthcare devices (or services) (e.g., Bhatt & Chakraborty, 2020). Moreover, PCT was often employed to investigate the tradeoff between benefits and privacy-related risks (e.g., Tran & Nguyen, 2021; Wiegard & Breitner, 2019). In the reviewed literature, PCT was used to test the impact of privacy issues on individuals' perception of an application's value and individuals' intention to use the application following integration with other theories, such as the concept of risk-risk tradeoff (Tran & Nguyen, 2021), IDT (Karahoca et al., 2018), PMT (Karahoca et al., 2018), TPB, and TRA (Princi & Krämer, 2020; Wiegard & Breitner, 2019). Other theories, including the balance theory (Hassandoust et al., 2021), the health information technology acceptance model (HITAM), the health information privacy concerns model (HIPC) (Matt et al., 2019), and the unique theoretical framework of 'surveillance culture' (Choi & Kim, 2024), were applied in the literature to explore individuals' use or their continuous use of smart healthcare services in health monitoring contexts. Moreover, self-regulation theory was used to examine the feelings of health empowerment as an outcome at the individual level (Nelson et al., 2016).

With regard to the organizational outcomes, researchers used the valence framework to evaluate the privacy-related impact of smart healthcare services on medical practitioners' attitudes toward adopting these services from an integrated economics and psychology perspective (Pan et al., 2019). In terms of stakeholder-related outcomes, Foucault's theory integrating governmentality and bio-power was applied to explore the relationship between privacy and overall smart home development from a collective perspective of key stakeholders (Suman, 2017). This theory is related to oppressive practices enabled by authoritarian relations of power and knowledge (Banville, 2020). Moreover, normalization process theory (NPT) was adopted to investigate the overall implementation effectiveness of smart health services affected by privacy issues (Peek et al., 2016), proposing the necessary factors for successfully implementing and integrating interventions into routine tasks (May et al., 2009).

**Table C3. Methods Used in the Published Articles**

| Method | Frequency | Articles |
|---|---|---|
| Quantitative | | |
| Survey | 21 | Aljedaani et al. (2023); Bhatt and Chakraborty (2020); Choi and Kim (2024); Dadhich et al. (2022); del Río-Lanza et al. (2020); Deng et al. (2018); Etemad-Sajadi and Dos Santos (2019); Karahoca et al. (2018); Kwiecień et al. (2020); Liu and Tao (2022); Lu et al. (2021); Mettler and Wulf (2020); Nelson et al. (2016); Pan et al. (2019); Papa et al. (2020); Runkle et al. (2019); Sayibu et al. (2022); Shimizu et al. (2021); Tran and Nguyen (2021); Zhang et al. (2019); Zhu et al. (2022) |
| Experiment | 2 | Princi and Krämer (2020); Seiferth and Schaarschmidt (2020) |
| Qualitative | | |
| Interview | 10 | Alzahrani et al. (2021); Beaudin et al. (2006); Burrows et al. (2018); (Esmaeilzadeh, 2023); Fritz et al. (2016); Hassandoust et al. (2021); Kennedy et al. (2021); LeBaron et al. (2020); Li et al. (2021); Matt et al. (2019) |
| Focus group | 4 | Ghorayeb et al. (2021); Hunter et al. (2020); Peek et al. (2016); Xing et al. (2021) |
| Case study | 3 | Ravishankar et al. (2015); Shimizu et al. (2022); Suman (2017) |
| Longitudinal study | 1 | Chen et al. (2021) |
| Workshop | 1 | Kim et al. (2018) |
| Jury session | 1 | Chadborn et al. (2019) |
| Qualitative survey | 1 | Kulyk et al. (2020) |
| Mixed-methods | | |
| Developmental | 2 | Cristiano et al. (2022); Wiegard and Breitner (2019) |
| Diversity | 2 | Arar et al. (2021); Balta-Ozkan et al. (2013) |
| Completeness | 1 | Choi et al. (2020) |

**Table C4. Coding of Privacy Definitions/Descriptions**

| Definitions and causal explanations | Perspectives | | | | | Articles |
|---|---|---|---|---|---|---|
| | Right | Commodity | Control | State | N/A | |
| ***Privacy definitions*** | | | | | | |
| "The concept of privacy has therefore evolved in the digital age to include contextual integrity… which advocates the flow of personal information should be contextually appropriate". (p. 113) | | | X | | | Burrows et al. (2018) |
| Perceived privacy is "other people can see my data without (letting) me knowing; …other people will release my data against my will; …difficult to maintain the data totally protected; …difficult to ensure that good use is made of the data". (p. 142) | | | X | | | del Río-Lanza et al. (2020) |
| "Four views on privacy emerged: 'privacy as modesty', 'private by nature', 'privacy normed', and 'privacy as American'".<br>"'Privacy as modesty' was portrayed as the idea of being watched while not fully clothed."<br>"'Private by nature' was seen as a form of privacy that involved a general way of life in which one maintains a significant part of personal life that is considered private."<br>"'Privacy normed' referred to the idea that a group view (societal or cultural) exists regarding what individuals do, or not do, in private."<br>"'Privacy as American' was associated with the language of the historical values of United States' citizens such as rights to life and liberty, which included the right to | X | | X | X | | Fritz et al. (2016) |

| | | | | | | |
|---|---|---|---|---|---|---|
| privacy." (p. 150) | | | | | | |
| "A fundamental aspect of privacy is the control over personal data". (p. 4)<br>"…individuals evaluate anticipated benefits and perceived risks in order to make a rational decision regarding the disclosure of their personal data…people will rather not use IoT in healthcare when they perceive privacy risks". | | X | X | | | Princi and Krämer (2020) |
| "…information privacy refers to individuals' control over the collection, unauthorized access and improper use of their personal information". (p. 3) | | X | X | | | Tran and Nguyen (2021) |
| ***Privacy (or privacy proxies) with causal explanations/descriptions*** | | | | | | |
| Perceived privacy captures users' attitudes toward personal health information disclosure. Privacy threats were attributable to the subthemes of perceived relativity, severity, and control. | | X | X | | | Matt et al. (2019) |
| Privacy risk refers to the possibility of information abuse, such as information theft and leakage due to using mHealth services. | | | | X | | Deng et al. (2018) |
| Individuals' privacy concerns are related to their sensitive health data sharing and their ability to control their lifestyles. | | | X | | | Hassandoust et al. (2021) |
| Perceived risks mostly refer to the "potential for loss associated with releasing personal information". | | X | | X | | Karahoca et al. (2018) |
| Different people rate privacy's importance differently for a myriad of reasons across different circumstances. | | | | | X | Kennedy et al. (2021) |
| Concerns were expressed regarding privacy and data sharing, e.g., what exactly is being collected and where the data is going, and when. | | | X | | | LeBaron et al. (2020) |
| Loss of privacy refers to how an individual perceives that using smart healthcare services infringes on their privacy. Perceived loss of privacy negatively influenced consumers' acceptance of m-health services. | | X | | X | | Liu and Tao (2022) |
| Perceived privacy protection is the perception of the likelihood that a smart wristband provider will protect consumers' confidential information collected during electronic transfer from unauthorized use or disclosure. | | | X | | | Nelson et al. (2016) |
| There is a loss of privacy as smart wearable healthcare records personal information. | | | | X | | Papa et al. (2020) |
| Privacy concerns of mobile users are modeled using three dimensions: errors, perceived intrusion, and secondary use of personal information. Individuals compare perceived privacy risks (PPR) with anticipated benefits. | | X | X | | | Wiegard and Breitner (2019) |
| Perceived privacy risk is defined as patients' feeling of a lack of control over their personal information after adopting mobile apps, and it is not consistent with a real privacy risk. | | | X | | | Zhang et al. (2019) |
| Privacy concerns reflect an individual's sense of boundary, self-protection, and | | | X | X | | Zhu et al. (2022) |

| | | | | | | |
|---|---|---|---|---|---|---|
| control. Users' concerns about the violation of their ability to control their personal information have also become increasingly severe. | | | | | | |

*Note.* 'N/A' = 'not applicable'. Kennedy et al. (2021) was labeled with 'N/A', as it suggests that different people rate the importance of privacy differently for a myriad of reasons across a number of circumstances. Therefore, it was difficult to classify this study into any existing conceptual perspectives.

**Table C5. Coding of Privacy Proxies**

| Privacy proxy | Frequency | Percentage | Articles |
|---|---|---|---|
| Not using a proxy | 23 | 47% | Alzahrani et al. (2021); Arar et al. (2021); Balta-Ozkan et al. (2013); Beaudin et al. (2006); Bhatt and Chakraborty (2020); Burrows et al. (2018); Chadborn et al. (2019); Dadhich et al. (2022); Etemad-Sajadi and Dos Santos (2019); Fritz et al. (2016); Hassandoust et al. (2021); Hunter et al. (2020); Kennedy et al. (2021); Kulyk et al. (2020); Kwiecień et al. (2020); LeBaron et al. (2020); Li et al. (2021); Peek et al. (2016); Ravishankar et al. (2015); Sayibu et al. (2022); Shimizu et al. (2021); Suman (2017); Xing et al. (2021) |
| Privacy concerns (or perceived) | 9 | 18% | Choi and Kim (2024); Choi et al. (2020); Cristiano et al. (2022); Ghorayeb et al. (2021); Kim et al. (2018); Mettler and Wulf (2020); Princi and Krämer (2020); Runkle et al. (2019); Zhu et al. (2022) |
| Privacy risk (or perceived) | 7 | 14% | Deng et al. (2018); Esmaeilzadeh (2023); Karahoca et al. (2018); Lu et al. (2021); Tran and Nguyen (2021); Wiegard and Breitner (2019); Zhang et al. (2019) |
| Privacy protection | 3 | 6% | Chen et al. (2021); Nelson et al. (2016); Shimizu et al. (2022) |
| Perceived risk (including privacy risk) | 3 | 6% | del Río-Lanza et al. (2020); Pan et al. (2019); Seiferth and Schaarschmidt (2020) |
| Loss of privacy | 2 | 4% | Liu and Tao (2022); Papa et al. (2020) |
| Perceived privacy | 1 | 2% | Matt et al. (2019) |
| Privacy policy | 1 | 2% | Aljedaani et al. (2023) |

**Table C6. Surveillance Focused as a Matter of Context**

| Category | Keywords | Articles |
|---|---|---|
| Highlight | Monitoring, tracking | Alzahrani et al. (2021) |
| | Monitoring | Aljedaani et al. (2023) |
| | Monitoring sensors | Burrows et al. (2018) |
| | Sensors, video camera | Arar et al. (2021); Balta-Ozkan et al. (2013) |
| | Personal tracking | Beaudin et al. (2006) |
| | Safety monitoring | Chadborn et al. (2019) |
| | Sensor, passive monitoring | Choi et al. (2020); Hunter et al. (2020) |
| | Remote monitoring | Cristiano et al. (2022) |
| | Intrusiveness | Etemad-Sajadi and Dos Santos (2019) |
| | Intervention | Fritz et al. (2016) |
| | Interventions, surveillance | Shimizu et al. (2022) |
| | Ethical, monitoring | Kennedy et al. (2021) |
| | Spying, surveillance, monitoring, eavesdropping | Kulyk et al. (2020) |
| | Continuous tracking | Matt et al. (2019) |
| | Constantly tracking | Mettler and Wulf (2020) |
| | Constant monitoring (Regular check-ups, ongoing screening, continuing surveillance of health status, monitoring symptoms, constant observation of signs, being controlled) | Esmaeilzadeh (2023) |
| | Sensors | Ravishankar et al. (2015) |
| | Surveillance, anxieties | Shimizu et al. (2021) |
| | Surveillance culture, surveillance imaginary, surveillance practices, watched | Choi and Kim (2024) |

| | | |
|---|---|---|
| | Acceptance of monitoring | Kwiecień et al. (2020) |
| | Watching, recording | LeBaron et al. (2020) |
| | Track, nonintrusive, passive | Li et al. (2021) |
| | Monitoring, negative beliefs | Nelson et al. (2016) |
| | Duration of monitoring, behavioral modification | Runkle et al. (2019) |
| | Social surveillance | Tran and Nguyen (2021) |
| | Technology surveillance | Sayibu et al. (2022) |
| Mention | Monitoring technology | Ghorayeb et al. (2021) |
| | Surveillance | Kim et al. (2018) |
| | Extensive collection | Princi and Krämer (2020) |
| | Tracking, behavioral profiles | Wiegard and Breitner (2019) |
| | Track | Xing et al. (2021) |
| | Feeling of being followed or watched | Papa et al. (2020) |
| | Feeling under surveillance | Zhu et al. (2022) |
| Not mention | | Bhatt and Chakraborty (2020); Chen et al. (2021); Dadhich et al. (2022); del Río-Lanza et al. (2020); Deng et al. (2018); Hassandoust et al. (2021); Karahoca et al. (2018); Liu and Tao (2022); Lu et al. (2021); Pan et al. (2019); Papa et al. (2020); Seiferth and Schaarschmidt (2020); Suman (2017); Zhang et al. (2019) |

**Table C7. Stakeholder Focused as a Matter of Context**

| Category | Stakeholders | Articles | Frequency | Percentage |
|---|---|---|---|---|
| Single stakeholder | Individuals | Aljedaani et al. (2023); Arar et al. (2021); Bhatt and Chakraborty (2020); Burrows et al. (2018); Chadborn et al. (2019); Chen et al. (2021); Choi and Kim (2024); Choi et al. (2020); Dadhich et al. (2022); del Río-Lanza et al. (2020); Esmaeilzadeh (2023); Etemad-Sajadi and Dos Santos (2019); Fritz et al. (2016); Ghorayeb et al. (2021); Hassandoust et al. (2021); Hunter et al. (2020); Karahoca et al. (2018); Kennedy et al. (2021); Kulyk et al. (2020); Kwiecień et al. (2020); Liu and Tao (2022); Lu et al. (2021); Matt et al. (2019); Mettler and Wulf (2020); Nelson et al. (2016); Pan et al. (2019); Papa et al. (2020); Princi and Krämer (2020); Ravishankar et al. (2015); Sayibu et al. (2022); Seiferth and Schaarschmidt (2020); Shimizu et al. (2022); (Shimizu et al., 2021); Suman (2017); Tran and Nguyen (2021); Zhang et al. (2019); Zhu et al. (2022) | 35 | 71% |
| | Healthcare professionals | Hunter et al. (2020); Pan et al. (2019) | 2 | 4% |
| Multiple stakeholders | Healthcare providers and individuals | Beaudin et al. (2006); Cristiano et al. (2022); Deng et al. (2018); LeBaron et al. (2020); Li et al. (2021); Runkle et al. (2019) | 6 | 12% |
| | Insurance companies and individuals | Wiegard and Breitner (2019) | 1 | 2% |
| | Experts (Industrial) and individuals | Balta-Ozkan et al. (2013) | 1 | 2% |
| | Service providers, technology developers, and | Alzahrani et al. (2021) | 1 | 2% |

| | | | | |
|---|---|---|---|---|
| | individuals | | | |
| | Individuals, device providers, and healthcare providers | Xing et al. (2021) | 1 | 2% |
| | Healthcare experts, IT experts, and law professionals | Kim et al. (2018) | 1 | 2% |
| | Individuals, healthcare providers, technology designers and suppliers, and policymakers | Peek et al. (2016) | 1 | 2% |

## About the Authors

**Jingjing Zhang** recently completed her PhD at Auckland University of Technology (AUT), New Zealand. Her research focuses on surveillance and privacy-protective data governance in smart health contexts, supported by the AUT Doctoral Scholarship. Jingjing's research can be found in the *Pacific Asia Journal of the Association for Information Systems* and *Australasian Conference on Information Systems 2024*. She is currently working as a Teaching Assistant and Research Assistant in the Department of Management, Technology, and Organization (MTO) at AUT.

**Farkhondeh Hassandoust** is Senior Lecturer in Information Systems at the University of Auckland. Dr Hassandoust's research interests are centered around the behavioral and organizational aspects of information security and privacy, as well as the impact of emerging technologies (e.g., AI) in healthcare across diverse communities. Her work has been published in *Information Systems Journal*, *Information & Management*, *Journal of the American Medical Informatics Association*, *Behaviour & IT*, *IS Frontiers* among others. Her research has been supported by grants from Health Research Council (HRC), Auckland University of Technology Vice-Chancellor's Scholarship and Internet New Zealand.

**Allen C. Johnston** is the Hewson Professor of Cybersecurity and a Professor of Management Information Systems (MIS) in the Culverhouse College of Business at the University of Alabama. The primary focus of his research is in the areas of behavioral information security, privacy, data loss prevention, collective security and innovation. His research can be found in such outlets as *MIS Quarterly*, *Journal of Information Technology*, *the Journal of the Association for Information Systems*, *European Journal of Information Systems*, *Information Systems Journal*, *Decision Sciences*, *Decision Support Systems* and *Communications of the ACM*, among others. He currently serves as an Associate Editor for *MIS Quarterly* and Senior Editor for *European Journal of Information Systems*, as well as serving on the Editorial Review Board for *the Journal of the Association for Information Systems*. He is a founding member and current Chair of the IFIP Working Group on Information Systems Security Research (WG8.11/11.13). Dr. Johnston has also served as a consultant, visiting professor or invited speaker at several universities, workshops, panels and companies in the United States and abroad.