12-10-2024

Navigating Resistance: The Role of Data Governance in Smart Health Monitoring Systems

Jingjing Zhang
Auckland University of Technology (AUT), jingjing.zhang@autuni.ac.nz

Farkhondeh Hassandoust
University of Auckland, farkhondeh.hassandoust@auckland.ac.nz

Allen C. Johnston
University of Alabama, acjohnston5@ua.edu

Navigating Resistance: The Role of Data Governance in Smart Health Monitoring Systems

Full research paper

Jingjing Zhang
Department of Management, Technology, and Organization
Auckland Univeristy of Technology
Auckland, New Zealand
Email: jingjing.zhang@autuni.ac.nz

Farkhondeh Hassandoust
Department of Information Systems and Operation Management
University of Auckland
Auckland, New Zealand
Email: farkhondeh.hassandoust@auckland.ac.nz

Allen C. Johnston
Culverhouse College of Business
University of Alabama
Tuscaloosa, USA
Email: acjohnston5@ua.edu

Abstract

Smart health monitoring systems (SHMSs) have encountered resistance and limited adoption from various stakeholders, including consumers and healthcare professionals, primarily due to psychological and functional barriers to SHMSs. Drawing on innovation resistance theory and data governance mechanisms, this mixed-methods study aims to investigate the impact of data governance on the associated concerns and barriers, thereby shedding light on the resistance to SHMSs. The findings reveal that procedural data governance mechanisms are more influential than structural and relational mechanisms in reducing user resistance to SHMSs. Cultural and religious differences within procedural data governance significantly influence both privacy concerns and functional barriers to SHMSs. Gender differences also play a crucial role in how data governance mechanisms are perceived, with certain aspects showing significant effects on male users.

Keywords innovation resistance theory, data governance, privacy, functional barriers, smart health monitoring

1 Introduction

Smart health monitoring systems (SHMSs) epitomize innovative personal healthcare systems, integrating real-time surveillance technologies and sensor-based smart applications to monitor users' daily health status and vital signs remotely (Almujally et al. 2023; Shen et al. 2020). The substantial growth of SHMSs in recent years can be attributed to the anticipated benefits stemming from the innovation of surveillance technologies. These benefits include facilitating communication between patients and healthcare providers, streamlining diagnostic and treatment processes, reducing costs associated with professional visits, and improving the quality of personal care (Akmandor and Jha 2018; Salehi-Amiri et al. 2022). These surveillance technologies encompass devices like blood glucose wearables and electrocardiogram (ECG) monitors, which are crucial for the functionality of SHMSs (Stavropoulos et al. 2020). The global SHMS market, valued at USD 190 billion in 2024, is projected to surge to USD 474 billion by 2032 (GlobeNewswire 2023). However, despite their significant advantages and ambitious investments, SHMSs have encountered resistance and limited diffusion from multiple stakeholders, including consumers and health professionals, due to various barriers such as resistance to change, concerns about trustworthiness, lack of ability to operate smart devices, and transition costs (Iyanna et al. 2022; Kamal et al. 2020; Talwar et al. 2023).

Among the cited barriers, the negative impact of privacy issues caused by surveillance technologies stands out as a prominent obstacle. Multiple global reports (e.g., Accenture.com 2020; Capterra.com 2021; Fortune.com 2023) emphasize privacy concerns of consumers related to the surveillance technologies integrated into SHMSs as the primary factor causing customers' resistance to their adoption and reluctance to share health data with healthcare professionals. Such innovative technologies often raise confusion or uncertainty among SHMS consumers regarding the assurance of its proper protection and usage within the surveillance system. Additionally, there is ambiguity surrounding data regulation policies, which define responsibility in the event of health data loss (Duckert and Barkhuus 2022; Princi and Krämer 2020). All these underscore the importance of robust data governance practices since these practices are essential to diffuse the tensions surrounding privacy and data sharing, mitigate risks, and balance interests within the multidisciplinary contexts of health data sharing (Knoppers and Thorogood 2017). Data governance refers to allocating authority and control over data, and the exercise of such authority through decision-making in data-related matters (DAMA International 2009; Janssen et al. 2020; Plotkin 2020). Crucially, data governance functions as the vehicle for identifying, resolving, and managing several different types of data-related issues, including data privacy, confidentiality, and security issues (DAMA International 2009). Its role extends beyond individual organizations, as effective data governance both within and across organizations is pivotal in facilitating digital innovation and striking a balance between social, economic, and technical benefits and risks for individuals, organizations, and societies at large (Davidson et al. 2023). Given that SHMSs heavily rely on personal and sensitive data, with multiple stakeholders operating across organizations, concerns surrounding privacy emerge as paramount barriers behind resistance to SHMS (Lee 2020).

Alongside privacy concerns, other potential barriers behind resistance to innovative technologies have been gradually explored, such as complicated environments of SHMSs, security issues, complexity of innovation, and lack of perceived value (Chouk and Mani 2019; Prakash and Das 2022). To dissect these barriers in SHMSs, we need to understand their origins and impacts to be able to mitigate them through effective data governance and other means. However, there is a lack of literature regarding the specific impact of data governance on mitigating privacy concerns and other barriers deriving the resistance to SHMSs (Chibuike et al. 2024; Davidson et al. 2023; Yaqoob et al. 2022). Effective data governance is essential for addressing privacy concerns and lowering resistance to technology adoption (Abraham et al. 2019). Drawing on innovation resistance theory (Ram and Sheth 1989) and data governance mechanisms, this study aims to explore the role of data governance toward concerns and barriers in relation to resistance to SHMS adoption to provide actionable insights for healthcare providers, technology developers, and policymakers. The research questions (RQs) are: (RQ1) *What are the contributing factors of resistance to SHMS?* And (RQ2) *How and in what ways do data governance mechanisms influence individuals' concerns and barriers to SHMS resistance*?

This study enriches SHMS-based privacy research by proposing a framework that considers relationships between data governance-related factors and perceived concerns and barriers in relation to SHMSs' resistance. It provides valuable insights that assist both service providers and policymakers in addressing privacy, complexity, and value barriers of personal health information in healthcare surveillance environments like SHMSs. The remaining sections are organized as follows: a theoretical background that informs our current understanding of concerns and barriers, data governance

mechanisms, and innovation resistance theory; the mixed-methods research design and results that inform our discussion. Limitations, conclusions, and future directions follow.

2 Background

This section focuses on the concerns and barriers causing users' resistance to SHMSs, the role of data governance mechanisms in mitigating privacy concerns in the innovative technology-centered context. It also discusses innovation resistance theory, enabling an exploration of the concerns and barriers and their impact on users' resistance to SHMSs.

2.1 Concerns and Barriers Related to SHMSs

Privacy has become one of the perpetual social issues associated with the development of innovative information technologies that enable pervasive surveillance, massive databases, and rapid distribution of information throughout the world (Nissenbaum 2010; Timan and Albrechtslund 2018). Privacy concerns are people's perceptions of what happens with the data they provide to or share with others (Bélanger and Crossler 2011; Dinev and Hart 2006). These concerns have been seen as psychological barriers against undesirable instruction in the context of surveillance activities (Burgoon 1982; Solove 2006). Due to the ability to capture detailed contextual information of individuals, the use of surveillance or monitoring applications without appropriate privacy protection mechanisms is likely to increase privacy concerns and, therefore, yield resistance to smart health applications by users (Pirzada et al. 2021; Prati et al. 2019). Privacy and surveillance are closely connected but distinct concepts: surveillance implies an entity (or entities) that accesses personal data through a discovery means like SHMSs, while privacy is a fundamental human right protecting individuals from unwanted intrusion by others (Solove 2002). It is imperative to study the issues contributing to the resistance of SHMSs, including individuals' privacy concerns and barriers associated with surveillance innovation technologies (Dinev et al. 2008). For instance, the complexity of the barriers to usage of a new mobile payment solution may pose potential challenges for users with low technical skills or poor experience in using such innovation, contradicting conventional cash-based payment methods (Kaur et al. 2020). Moreover, users may reject this innovative payment solution because of value barriers, perceiving that the costs associated with using it outweigh the benefits it offers (Kaur et al. 2020). Aligning with these insights, several studies have explored privacy concerns and other barriers in terms of surveillance technology toward customers' resistance to SHMSs environments (e.g., Chouk and Mani 2019; Prakash and Das 2022; Talwar et al. 2023).

2.2 Data Governance for SHMSs

Data governance pertains to the allocation of decision-making authority concerning data assets within an organization (Khatri and Brown 2010; Lis and Otto 2021). It helps manage the conflicts between privacy and data sharing, mitigate risks, and balance interests within multidisciplinary contexts at multiple levels of data sharing (Jain et al. 2016; Knoppers and Thorogood 2017). As an essential part of the data governance approach, data governance mechanisms refer to control mechanisms and procedures for data issues, including privacy, from the management perspective of collaborative stakeholders (Abraham et al. 2019; DAMA International 2009). These mechanisms ensure responsible data sharing by enabling access when required but blocking it when not (Janssen et al. 2020). Data governance mechanisms can be distinguished between s*tructural, procedural,* and *relational* mechanisms (Abraham et al. 2019; Borgman et al. 2016; Tallon et al. 2013). Structural mechanisms focus on the identification of key decision-makers and their roles and responsibilities regarding data ownership, cost management, and value analysis, among others (Tallon 2013). Procedural mechanisms aim to ensure that data is recorded reliably and accurately, used ethically and effectively, held securely and confidentially, and shared appropriately and lawfully (Borgman et al. 2016). Relational governance mechanisms facilitate collaboration between stakeholders, covering themes of communication, training, the coordination of decision-making, and so on (Abraham et al. 2019).

In sum, privacy concerns and surveillance usage are deeply intertwined and tightly associated with the effectiveness of data governance mechanisms implemented by various stakeholders in personal data monitoring contexts (Janssen et al. 2020; Plotkin 2020; Rosenbaum 2010). In healthcare, data governance is the process by which the responsibilities of data stewardship are conceptualized and excised through approaches and policies enabling stewardship (Rosenbaum 2010). Given the importance of exploring antecedents or determination factors across multiple levels in order to address privacy issues leading to customers' resistance, numerous scholars have delved into multi-level antecedents in their studies focusing on resistance in SHMSs. For instance, Iyanna et al. (2022) and Xu (2019) assessed organizational factors contributing to resistance in the adoption and effective use of

diverse e-health innovations. Park et al. (2022b) investigated technological issues such as technological complexity and ease of use that may negatively affect invasions of privacy that lead to resistance outcomes. Park et al. (2022a) studied perceived controllability as a critical individual-level factor that moderates the relationship between surveillance anxiety and the rejection of continuous monitoring of patient's health. However, there is insufficient information on how these contributing factors can be mitigated through mechanisms such as data governance among collaborative stakeholders, underscoring the need for data governance-based solutions (Chibuike et al. 2024; Davidson et al. 2023).

2.3 Innovation Resistance Theory

Innovation resistance theory was developed by Ram and Sheth (1989) that explains the reasons behind customers' resistance to adopt innovations despite their perceived desirability and necessity. It assumes that individuals resist adopting modern technologies either because these technologies require customers to potentially change from a satisfactory existing state or because they contradict customers' belief structure (Park et al. 2022a; Ram and Sheth 1989). According to the theory, main reasons to innovation resistance are categorized as psychological and functional barriers (Ram and Sheth 1989). Psychological barriers such as privacy concerns, surveillance discomfort, and dependence (Lee 2020; Mani and Chouk 2017; Prakash and Das 2022; Talwar et al. 2023), emerge when the innovation conflicts with individuals' existing beliefs derived from various sources (Park et al. 2022a; Ram and Sheth 1989).

Functional barriers emerge when individuals perceive substantial changes resulting from adopting an innovation (Park et al. 2022a; Ram and Sheth 1989). Functional barriers include *value barriers*, *complexity barriers* of usage, and *risk barriers* (e.g., lack of endorsements and testimonials), among others. *Value barriers* refer to how customers perceive the performance of an innovation in relation to its cost, compared to other available options (Iyanna et al. 2022; Ram and Sheth 1989). Unless an innovation provides a compelling performance-to-price ratio compared to existing alternatives, there is little motivation for customers to adopt it (Ram and Sheth 1989). *Complexity barriers* refer to when users perceive the innovation as difficult to understand due to the complexity of the idea or challenging to use because of its complex execution (Friedman and Ormiston 2022; Prakash and Das 2022). Users may encounter complexity barriers when an innovative technology requires a significant change that conflicts with existing usage patterns and daily routines (Kaur et al. 2020; Ram and Sheth 1989). Such change includes the cognitive time and effort devoted to learning, impacting the usability of the innovation (Borraz-Mora et al. 2017; Orbaiz and Arce-Urriza 2024). *Risk barriers* involve uncertainty and unforeseen side effects associated with the timing of innovation adoption (Ram and Sheth 1989). Customers, mindful of these risks, may delay adopting the innovation until they are able to learn more about it (Ram and Sheth 1989). In other words, while risk barriers can influence when people adopt a product, it may not necessarily prevent adoption altogether. For example, customers might delay their purchases until a better product with a lower price tag will soon be on the market (Ram and Sheth 1989).

Numerous scholars have applied innovation resistance theory to examine both psychological and functional barriers in SHMSs as a typical surveillance-based innovative application (e.g., Iyanna et al. 2022; Mani and Chouk 2017; Park et al. 2022a; Prakash and Das 2022). For instance, Mani and Chouk (2017) developed a model drawn on the theory, exploring the factors that influence consumer resistance to smart products. The factors entail consumer characteristics (e.g., privacy concerns) from psychological barriers and innovation characteristics (e.g., perceived uselessness) from functional barriers. Therefore, this study explores the factors of data governance addressing the key barriers, including privacy concerns, value barriers, and complexity barriers in relation to resistance to SHMSs.

3 Mixed-method Research Design and Results

This study follows a post-positivist research paradigm (Creswell and Poth 2018). It uses a sequential two-stage mixed-methods design comprising both qualitative and quantitative analyses (Creswell and Plano Clark 2018). This specific methodology is selected for its three key methodological advantages. Firstly, a sequential mixed-methods design enables addressing exploratory questions in the same research inquiry (Venkatesh et al. 2013). Secondly, it facilitates a comprehensive understanding and synthesis of insights derived from qualitative and quantitative dimensions, thereby balancing depth and breadth (Venkatesh et al. 2013). Thirdly, a mixed-methods design is particularly beneficial for investigating new contexts where issues are challenging to elucidate or describe using existing perspectives (Ågerfalk 2013). Our mixed-methods approach is structured around a developmental purpose with two study phases (Study 1 and Study 2). Study 1 aims to use the findings of a qualitative study to develop a suitable set of constructs, establish relationships among these constructs in the form of a model, and propose a corresponding set of hypotheses. In Study 2, these hypotheses are tested using a quantitative method (Venkatesh et al. 2016).

3.1 Study 1: Qualitative Study Design

Study 1 follows an explorative research approach (Creswell and Poth 2018). It uses a purposive random sampling strategy to target participants with knowledge and experience in specific SHMSs. The study includes 15 qualitative interviews with individuals from diverse stakeholder groups (individual users, healthcare providers, smart technology providers, and government health authorities). Interviews covered various SHMS scenarios, from clinical trials to surveillance-based monitoring products available in the local market, e.g., glucose monitors. Data collection ceased after 15 interviews as theoretical saturation was reached, ensuring that no new insights were emerging from additional interviews. The purpose of these interviews is to discuss and identify key contextual factors or theoretical considerations in terms of data governance mechanisms and innovation resistance theory and then use those insights to develop a research model and associated set of hypotheses. Guided by Taylor et al. (2016), the interviews were semi-structured, covering demographic information and exploring factors contributing to key barriers in relation to users' resistance to SHMS technology. All interviews were audio-recorded and transcribed in full. The first author coded and analyzed the interview transcripts using NVivo v12 software, and the second author checked the coding and analysis work. Then, the authors used thematic analysis to study the interview transcripts and find important themes and patterns in relation to data governance mechanisms that mitigate users' concerns in relation to resistance to SHMS. Thematic analysis is a common method for analyzing and reporting patterns or themes in qualitative data (Braun and Clarke 2006).

3.2 Developing and Hypothesizing SHMSs' Users' Resistance Model

From the literature on innovation resistance theory and interview results, we identified six key factors (antecedents) across three aspects of data governance mechanisms: *responsibility* (structural aspect); *legislative protection*, *cultural and religious differences*, and *traceability* (procedural aspect); *transparency* and *trust* (relational aspect). These factors address RQ1 and inform the development of the quantitative model to answer RQ2. *Responsibility* is the overall relationship of the system with all its stakeholders, which involves being accountable for actions and fulfilling obligations or commitments (Dahlsrud 2008; Ebrahim and Buheji 2020). It has crucial implications for addressing data-related concerns such as ethical dilemmas, fear, dependence, and trust in emerging technologies in healthcare (Someh et al. 2019). With respect to the responsibility factor of structural mechanisms, one participant (p#4: individual user) indicated, "*the existence of accountability [responsibility] is necessary, but for us as ordinary users, at first we may not feel it, or even know it exists*." However, most non-individual user participants emphasized the importance of the responsibilities and roles from a management perspective in a SHMS context. For example, a participant (p#11: technology provider) stated that they complied with relevant laws and regulations (such as the General Data Protection Regulation) by assigning a data protection officer to oversee and supervise data-related issues within their organizations. Another participant (p#2, government health authority) stated, "*We have mechanisms for responsibility in charge of privacy violations in a digital innovation context*". He explained that if an individual user had a concern, they should be able to make a complaint and direct that concern to an officer who should use the authority to resolve the concern. He added, "*from the view of stakeholders' collaboration, responsibility-based mechanisms help increase the entire quality of the service and simplify complicated processes among various stakeholders*". Thus, we posit the following hypotheses:

H1a-c: *Increased responsibility within structural data governance mechanisms is likely to decrease users' (a) privacy concerns, (b) complexity barriers, and (c) value barriers in relation to SHMSs.*

Three factors were identified in the procedural aspect: *legislative protection*, *cultural and religious differences*, and *traceability*. *Legislative protection* strives for the right to information, restrictions on the use of data governance mechanisms, IT security legislation, and supports for the implementation (Weber 2010). Legislative protection mechanisms play a crucial role in addressing privacy concerns, preserving personal autonomy, and mitigating skepticism toward technical innovations. Robust legislative safeguards enhance trust in new technologies and bolster their perceived value (Gasser et al. 2020; Nguyen et al. 2022; Princi and Krämer 2020). All the interviewees show a consensus on the importance of legislative protection for effective data management within SHMSs. Moreover, most participants from non-individual users have all presented their strong confidence in their familiarity with the local Privacy Acts and relevant codes (e.g., Privacy Act 2020 and Health Information Privacy Code 2003, and Good Medical Practice) or their capability to access the acts for more legal information to address the potential issues and concerns about personal data and the SHMS technologies. A participant (p#5: healthcare provider) expressed, "*I am very familiar with the existing privacy acts and codes …[because] we were repeatedly mentioned all those acts when we have nursing courses*." She (p#5) added, "*effective legislative protection mechanisms can influence how users look at the value of*

the smart service…it is because robust health data protection mechanisms are critical for the overall value derived from data… and it is very helpful to simply the process of our data protection activities when complying with the GDPR framework." However, a participant (p#2: government health authority) noted, "*otential users may find it complex and time consuming in understanding complicated legislative terms…it's quite often to be asked to give more consents…it could deter them from recognizing the potential value of a smart device.*" An individual user (p#3) suggested that "*a pipeline between privacy protection and access to data for a positive outcome should be established.*" Thus, we posit the following hypotheses:

H2a: *Increased legislative protection from procedural data governance mechanisms is likely to decrease users' privacy concerns in relation to SHMS.*
H2b-c: *Increased legislative protection from procedural data governance mechanisms is likely to increase users' (b) complexity barriers, and (c) value barriers in relation to SHMS.*

Different cultural and religious backgrounds lead to different interpretations and viewpoints on privacy-related issues (Smith et al. 2011; Zhu et al. 2021). Nearly all interviewees highlighted the significance of cultural and religious factors in relation to associated concerns regarding SHMSs. One interviewee (p#10: healthcare provider), an SHMS project manager from the healthcare industry, stated, "*We would get feedback from one of our cultural advisory groups before we go into these projects. We are just making sure that we're not completely missing the issue [since] the device could be linked with some ethical considerations*." Different cultural and religious backgrounds are connected to how people value and understand a health network (Alashoor et al. 2015; Schwartz 2012). An interviewee (p#8: technology provider) who was a technical manager pointed out, "*New Zealand has to respect to Māori culture, we need to obey to Māori data protection rights…also, different culture and religious background in our country should always be considered as it may link to citizen's perceived value and difficulty when they use such innovative service*." Thus, we posit the following hypotheses:

H3a-c: *Cultural and religious differences from procedural data governance mechanisms are associated with users' (a) privacy concerns, (b) complexity barriers, and (c) value barriers in relation to SHMS.*

Traceability allows for identifying the interconnectedness and enhancing analysis between SHMS devices and their data owners within SHMSs (Lomotey et al. 2017). However, improper use of traceability has limitations in health data management. This can lead to consumer concerns and anxiety when they realize they are being traced, as various service providers can access their sensitive health data (Chouk and Mani 2019; Ismail et al. 2020). Our interview findings showed that *traceability* has emerged as a critical topic that potentially influences individuals' concerns and barriers during data protection practices among stakeholders. A participant (p#10: healthcare provider) stressed, *"To be able to use that device within New Zealand, we have to switch off the voice recognition part, but there were questions such as can I be listened or can I be tracked*." On the other hand, it is noteworthy to learn that traceability can contribute to the enhancement of health data protection practices and increase the service value of smart monitoring. One participant (p#4: individual user) thought, "*They [traceability] will be able to monitor improper data transfer processes… this [traceability] can avoid or detect unauthorized behaviors and increases data protection ability of the system* [SHMS]*…in this sense, the tracing ability simplifies management and collaboration process among service providers and reduce a feeling that the service is too complex to understand*." Thus, we posit the following hypotheses:

H4a-c: *Increased traceability from procedural data governance mechanisms is likely to increase users' (a) privacy concerns, (b) complexity barriers, and (c) value barriers in relation to SHMS.*

The interview findings also revealed *transparency* and *trust* as two critical factors in terms of relational data governance mechanisms that could mitigate concerns regarding personal data and barriers of using the SHMSs. *Transparency* involves making everything visible, indicating openness or open communication to establish trustworthiness (Kim et al. 2014). Transparency is closely associated with various issues in relation to users' resistance to SHMS usage, including mistrust, control, perceived privacy and security concerns, and cultural considerations (Talal et al. 2019; Van Zoonen 2016). One interviewee (p#2: government health authority) supported the importance of transparency and indicated, *"You should also be very clear in your privacy-related materials about what the information will be used for you can provide what we call a layered privacy statement…if you want more information go to this 3 pages, 5 pages, 10 pages, whatever it is that gives you the full explanation of the system. We wrote a probably 60 or 70-page privacy impact assessment associated with COVID tracer…so people who really wanted to know what's going on go and read the full document…but for the relatively small number of people that could read that code and understand it, they could go there and confirm that."* Moreover, one participant (p#5: healthcare provider) mentioned, "*when we collect*

personal data from customers, we need to clearly explain our aim, behaviors…why we have to use it. By making the whole data sharing process open and transparent…customers can better understand the benefit or value from using it [device] and reduce reluctance to cooperate with us." Thus, the hypotheses are as follows:

H5a-c: *Increased transparency from relational data governance mechanisms is likely to decrease users' (a) privacy concerns (b) complexity barriers, and (c) value barriers in relation to SHMS.*

Trust management in data governance focuses on handling security policies, credentials, and trust relationships. It has emerged as a promising technology to enable collaboration among entities in digital contexts where traditional security methods cannot be enforced due to decentralized control and incomplete knowledge of the context (Yan et al. 2011). Thus, trusting beliefs have been seen as a predictor that influence the forming of psychological obstacles, such as fear of technological complexity and discomfort when being monitored by service providers (Elahi et al. 2019; Puntoni et al. 2021). One interviewee (p#7: healthcare provider) remarked, "*Overall, trust is an extremely important thing. It can even have a direct impact on the health index of the elderly…*" Another interviewee (p#4: individual user) stated, *"trust can boost users' confidence in its potential value of the service and minimize perceived risks or difficulties, thereby encouraging users to give it a try*." Another participant (p#1: government health authority) stressed from the community perspective, "*Trust is often regarded as a relational basis that can influence the entire population health development*." We posit two hypotheses:

H6a-c: *Increased trust from relational data governance mechanisms is likely to decrease users' (a) privacy concerns, (b) complexity barriers, and (c) value barriers in relation to SHMS.*

Privacy concerns regarding personal data are the important psychological barriers that have contributed to users' resistance to new information technologies (e.g., Hew et al. 2019; Zhu et al. 2022). Our interviews' data underscored a potentially positive association between individuals' privacy concerns and their resistance to adopting SHMSs. A typical quote (p#3: individual user) was that *"There can be no movement along the journey…unless they [we] feel confident that their [our] data is going to be protected and respected…they [we] can be confident their [our] data is not going to be used for any reason*." Moreover, consistent with prior research showing value and complexity are functional barriers positively affecting resistance of innovative technologies (e.g., Mani and Chouk 2017; Prakash and Das 2022), the interview results suggested that these two barriers are critical factors toward customers' resistance to SHMSs. For example, one participant (p#12: healthcare provider) noted, "*some patients found it challenging to remember to charge or set up a smart device…which could deter them from wearing it.*" Another participant (p#4: individual user) indicated, "*I find the appearance of the app looks a bit cluttered… I think it should have a simpler design…it is complicated for me to manage my health data properly, for example, uploading the records in the correct location and removing them after a period for my privacy purpose.*" Thus, we posit the following hypotheses:

H7: *Privacy concerns are positively associated with users' resistance to SHMSs*.
H8: *Usage barriers are positively associated with users' resistance to SHMS.*
H9: *Complexity barriers are positively associated with users' resistance to SHMS*.

Based on the extant literature and qualitative results, and the posited hypotheses, we propose a concern mitigation data governance model in relation to SHMS users' resistance, as shown in Figure 1.

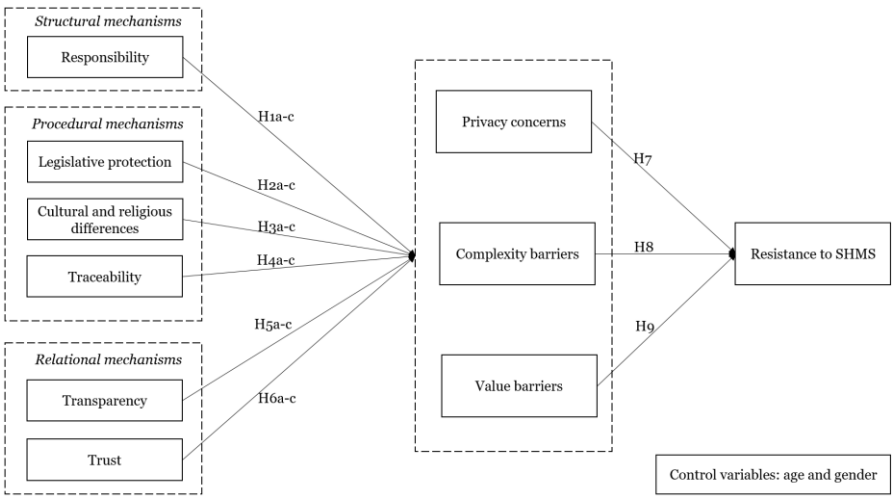

Figure 1: Concern Mitigation Data Governance Model against Resistance to SHMS

3.3 Study 2: Quantitative Study Design

Following the mixed-methods design, Study 2 aims to empirically test the proposed model among individuals familiar with an SHMS or currently using an SHMS technology. An online questionnaire survey webpage was developed using the Qualtrics platform. We launched the webpage link and handled participant recruitment using a professional agency–Prolific. Based on a statistical power analysis with G Power v3.1 software, a sample size of 208 is suitable for the complete model (Faul et al., 2007). Overall, 277 valid responses were collected from October to November 2024 after filtering out incomplete and unqualified responses. The hypothesis-related measurement items were developed from sources examined in previous research. In detail, 5 items for *responsibility* adapted from Son and Kim (2008), 3 items for *legislative protection* from Lwin et al. (2007), 4 items for *cultural and religious differences* from Karadag et al. (2019), 3 items for *traceability* from Wu et al. (2021), 3 items for transparency from Xu (2019), 4 items for *trust* from Chang and Fang (2013), 4 items for *privacy concerns* from Trkman et al. (2023), 3 items for *complexity barriers* from Prakash and Das (2022), 4 items for *value barriers* from Khanra et al. (2021), Laukkanen et al. (2007), and Prakash and Das (2022), and *resistance to SHMS* from Park et al. (2022a). These constructs of the model were measured via a five-point Likert scale spanning from 1 (strongly disagree) to 5 (strongly agree). All the constructs are first-order reflective constructs. The measurement and structural models were tested using Partial Least Squares-Structural Equation Modelling (PLS-SEM) SmartPLS v4 software. PLS-SEM is ideal for complex modelling because it has fewer constraints (e.g., the non-normal data distribution and sample sizes), making it advantageous when the data do not meet the strict assumptions required by CB-SEM (Hair et al. 2019).

3.4 Quantitative Results

3.4.1 Measurement Model Assessment

We evaluated the reliability and validity of the measurement in the model through several criteria, including internal consistency, indicator reliability, convergent validity, and discriminant validity of the instrument items (Chin 2009). Indicator reliability (loadings > 0.7), internal consistency reliability (α > 0.7, CR > 0.7), and convergent validity (AVE > 0.5) were all confirmed to be satisfactory, except for REPS2, CURE3, TRUS1, and TRUS2, which were removed from the model. Discriminant validity was evaluated using the HeteroTrait-MonoTrait (HTMT) criteria (Hair et al. 2023). When HTMT values exceed 0.9, it suggests a lack of discriminant validity between constructs that are conceptually similar. According to the assessment, all HTMT values between the constructs were below 0.9 and in line with the requirement.

3.4.2 Structural Model Assessment

A structural model assessment was assessed after evaluating the adequacy of the measurement model. This assessment aims to examine collinearity among the exogenous constructs (Hair et al. 2019). The Variance Inflation Factor (VIF) test was conducted to verify collinearity among the constructs. Most of the values were satisfactory, except for the PRIV3 item value in the construct of privacy concerns, which was then removed. We ran bootstrapping with 5000 subsamples at a 5% significance value to test the path coefficients' statistical significance (Hair et al. 2019). The results of this assessment are shown in Figure 2.

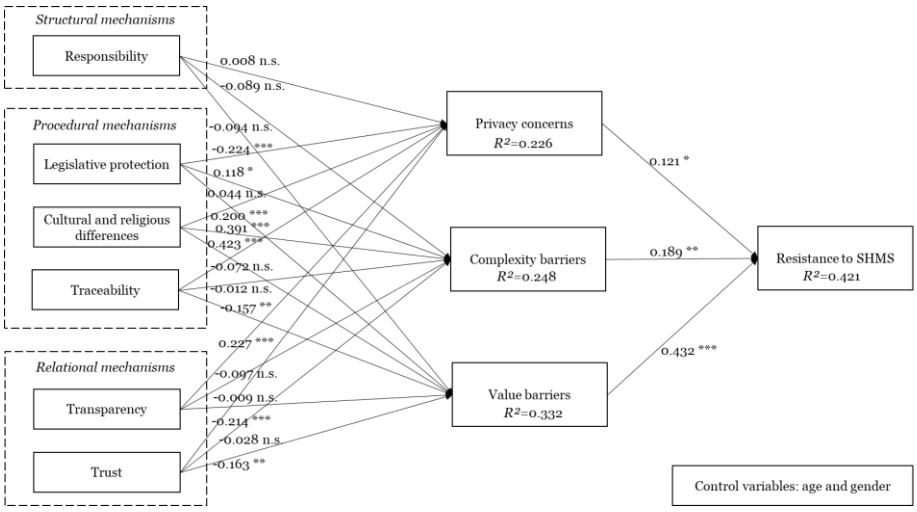

*Figure 2: Structural Model Results (*p < 0.05, **p < 0.01 and ***p < 0.001)*

In respect to tests of hypotheses H1a-c, the results do not support all of H1a (β =0.008, p = 0.902), H1b (β =0.089, p = 0.217), and H1c (β =-0.094, p = 0.104) showing that responsibility is not a significant factor regarding structural data governance mechanisms to affect privacy concerns and functional barriers in SHMS contexts. Despite not supporting the hypotheses, these test results are in line with our interview findings indicating responsibility was not a significant factor from the view of consumer participants. For Hypotheses H2a-c, the results support H2a (β =-0.224, p = 0.000) showing that legislative protection regarding procedural data governance mechanisms is a significant factor that negatively affects privacy concerns in SHMSs. This result is in line with many studies that suggest a negative influence of legislative protection on customers' privacy concerns in various health informatics environments (e.g., Nguyen et al. 2022; Xu 2019). The results also support H2b (β = 0.118, p = 0.048) showing that legislative protection positively affects complexity barriers in SHMSs, aligning with our interview findings. However, the results do not confirm H2c (β = 0.044, p = 0.425) meaning that legislative protection is not a significant factor to affect value barriers in SHMSs. The results support all H3a (β =0.200, p = 0.000), H3b (β =0.391, p = 0.000), and H3c (β =0.423, p = 0.000), showing that cultural and religious differences are significant factors positively affecting privacy concerns, complexity barriers, and value barriers. These findings align with prior literature. For instance, Kulyk et al. (2020) confirmed the effect of cultural differences on privacy and security risk perceptions in smart health environments across three countries. Perry-Hazan et al. (2021) examined that different religious backgrounds affect the worldview and complexity of how people behave in the disparities. von Humboldt et al. (2020) explored the relationship between the value of smart technology and faith and belonging (religion). Regarding Hypotheses H4a-c, the results only support H4c (β = -0.157, p = 0.007), showing that traceability negatively affects value barriers in SHMS. The results do not confirm H4a (β = -0.072, p = 0.209) or H4b (β = -0.012, p = 0.844), showing that traceability is not a significant factor affecting neither privacy concerns nor complexity barriers.

For the tests of hypotheses H5-H6 based on the factors from relational data governance mechanisms, the results provide support for H5a (β = -0.157, p = 0.007), indicating that transparency management in terms of data governance mechanisms is negatively associated with privacy concerns in relation to SHMS. This result aligns with previous research, which has explored and substantiated similar hypotheses from various angles. For example, Xu (2019) examined that organizational-level information transparency positively correlates with patients' information privacy concerns in the context of health informatics services. However, the findings do not confirm H5b (β = -0.097, p = 0.149) and H5c (β = -0.009, p = 0.879), suggesting that both value and complexity barriers are not significantly influenced by traceability-related data governance mechanisms. Finally, the results confirm H6a (β = -0.214, p = 0.000) and H6c (β = -0.163, p = 0.005) that trust negatively affects privacy concerns and value barriers in SHMSs. However, H6b (β = -0.028, p = 0.662) is not confirmed, presenting that trust is not a significant factor in affecting complexity barriers.

In terms of tests of hypotheses concerning the impact of psychological barriers on resistance to SHMSs, the results endorse H7 (β = 0.121, p = 0.017), indicating that privacy concerns exhibit a positive relationship with SHMS users' resistance. This outcome is consistent with a great number of previous studies (e.g., Lee 2020; Xu 2019), which have demonstrated that privacy concerns have a positive impact on individuals' rejection of various innovative technologies. For hypotheses concerning functional barriers, the results support H8 (β = 0.432, p = 0.000) and H9 (β = 0.189, p = 0.003), suggesting that both value barriers and complexity barriers positively affect users' resistance to SHMSs. The findings are consistent with existing studies on a wide range of new technologies. For example, Prakash and Das (2022) has confirmed that value and complexity barriers are positively related to citizens' resistance to using digital contact tracing apps.

4 Discussion

Drawing on innovation resistance theory and data governance mechanisms, the study employed a developmental mixed-methods research approach. The qualitative findings from Study 1 suggest five salient factors of data governance mechanisms partially influencing users' privacy concerns, complexity barrier, and value barriers: legislative protection, cultural and religious differences, traceability, transparency, and trust. The findings also support the relationships of resistance to SHMSs with privacy concerns, complexity barriers, and value barriers. Then, a quantitative study was conducted in Study 2. Guided by Venkatesh and his colleagues (2013; 2016), three main findings were extracted and discussed.

4.1 Theoretical Implications

One of the main findings of this study is that procedural data governance mechanisms are found to be more influential than structural and relational mechanisms in reducing user resistance to SHMSs. While

improving users' engagement, including control over data and transparency, procedural mechanisms provide users with the most immediate and tangible evidence to address their resistance. For example, clear information on how to opt out of data sharing or details about what data is collected and why it is necessary (legislative protection) can directly influence a user's decision to adopt or reject an SHMS. These mechanisms are actionable and allow users to control their interaction with the system, hence playing a critical role in reducing resistance. Moreover, different cultural and religious groups may have distinct views on privacy, which are shaped by their unique values, norms, and historical contexts (Martin and Nissenbaum 2016; Miltgen and Peyrat-Guillard 2014). While structural mechanisms like responsibility and accountability are crucial for establishing the framework within which data governance is executed, their impact on user resistance may be less direct than procedural mechanisms. Structural mechanisms often operate at an organizational or system level and may not be as visible to end-users or consumers, as their primary roles are focused on reporting data-related issues and specifying requirements (Abraham et al. 2019). Although they underpin the overall governance of the system by defining roles and responsibilities, users might not directly perceive their impact on their day-to-day interaction with SHMS. As a result, these mechanisms might not be as effective in immediately alleviating user concerns about privacy and barriers regarding SHMS technology. Moreover, relational mechanisms such as trust and transparency are essential for building long-term user engagement and confidence (Borgman et al. 2016; DAMA International 2009). Trust is fostered by consistently demonstrating transparency in actions and decision-making processes related to data use (DAMA International 2009). However, building confidence is a gradual process and might not have an immediate effect on reducing initial resistance to SHMS. Users might appreciate transparency and may be more willing to trust the system over time, but these mechanisms might not quickly overcome initial barriers posed by privacy concerns or skepticism towards new technologies.

The findings highlight that cultural and religious differences within procedural data governance significantly influence both psychological and functional barriers in relation to SHMSs, suggesting the importance of integrating cultural sensitivity into governance frameworks. Different cultural and religious groups have diverse norms and expectations concerning privacy (Martin and Nissenbaum 2016; Miltgen and Peyrat-Guillard 2014). For instance, in some cultures, there may be a greater expectation of communal sharing and less emphasis on individual privacy, which could influence how privacy is perceived and what privacy protections are expected in SHMS (Banville 2020; Chu et al. 2019). Certain religious practices might dictate specific privacy or data handling requirements that standard SHMS protocols could violate. Moreover, SHMS often involve complex interfaces that require a basic understanding of digital interactions, which can vary widely across different cultural backgrounds (Esmaeilzadeh 2023; Hatuka and Zur 2020). Users with limited exposure to technology, possibly due to educational or socioeconomic factors more prevalent in certain cultures, might find SHMS particularly daunting (Beaudin et al. 2006; Choi and Kim 2024). Regarding value barriers, cultures with a strong focus on holistic and preventive healthcare might see more value in SHMS that monitor long-term health trends and promote wellness, as opposed to systems primarily designed for reactive medical intervention. Considering the critical role of cultural and religious differences, procedural data governance must involve consent processes that are both legally sound and culturally appropriate (Khanna and Srivastava 2020). This includes providing consent forms and privacy notices in multiple languages and formats that are easily understandable, respecting literacy levels and linguistic norms. In addition, incorporating regular feedback mechanisms into the SHMS governance framework allows for continual assessment and adaptation of the system to meet evolving cultural needs. This dynamic approach can help maintain the relevance and efficacy of the system across diverse user bases (Khanna and Srivastava 2020; Zimmerman 2000).

The findings suggest that gender differences play a crucial role in how data governance mechanisms are perceived, with certain aspects showing significant effects on male users, pointing to the need for gender-specific considerations in SHMS governance strategies. The findings reveal that different aspects of data governance have varying impacts on male and female users, highlighting the importance of incorporating gender-specific considerations into SHMS governance strategies. Transparency and trust are significantly associated with reducing privacy concerns among male participants. These suggest that men may value clear and explicit information regarding how their data is used and protected. Men may perceive transparency as an indicator of system integrity and legitimacy, which helps them to trust the system and directly address their privacy concerns. Men may require visible proof of reliability and credibility within the SHMS, such as certifications or endorsements, to feel comfortable with the privacy aspects of the technology (Alsyouf et al. 2021; Pirzada et al. 2021). The finding also shows that legislative protection is significantly associated with reducing complexity barriers for male users. Men may perceive legal safeguards as simplifying the technology's trustworthiness. Knowing that stringent laws govern data use and protection may help men better understand and navigate SHMSs (Zimmerman

2000), reducing the perceived complexity of using the system. Instead, women may focus more on the operational aspects or require different forms of support to overcome complexity barriers (Pirzada et al. 2021).

4.2 Implications for Research and Practice

This study serves as a valuable resource for both further research and practical applications. It builds upon the existing framework on innovation resistance by integrating data governance, demonstrating how theoretical models can be tailored to address diverse needs within the HIT domain. From the findings, cultural and religious differences have been identified as significant precursors in prior research and in this study, contributing to privacy apprehensions and obstacles causing SHMS users' resistance. Recognizing and incorporating these cultural nuances into the design and governance of SHMSs can help alleviate privacy concerns by aligning system operations with user expectations and comfort levels. Understanding these differences (e.g., digital literacy among different groups/cultures) can guide the development of user interfaces and support systems that are culturally and linguistically adapted to meet the specific needs of diverse user groups, thus reducing perceived complexity. Cultural and religious considerations should be integrated into the procedural aspects of data governance. For instance, healthcare providers can implement customized consent forms and privacy notices aligning with cultural norms about information sharing, to enhance trust and transparency. It shows respect for the user's cultural background, which can be crucial for systems like SHMS that handle sensitive personal health data. This level of customization not only mitigates privacy concerns but also addresses potential resistance due to cultural mismatches. Moreover, healthcare providers and technology providers can leverage insights from this study to collaboratively develop gender-sensitive communication strategies that address the different privacy concerns of male and female users. When developing data governance policies, the policymakers from government authorities can consider the differential impacts on male and female users. Policies should not only be equitable but also sufficiently flexible to address these varied impacts effectively. The findings also imply that factors deemed critical by non-user stakeholders (e.g., technology providers and government health authorities), including responsibility, may not resonate as strongly from the users' perspective. This discrepancy underscores the importance of incorporating diverse stakeholder inputs in the design and development of data governance mechanisms. Such an inclusive and user-centered approach ensures that the systems are tailored to address the specific needs and concerns of all parties and involved, thereby enhancing the likelihood of user adoption of SHMSs.

5 Limitations, Conclusions, and Future Directions

Drawing on innovation resistance theory and data governance mechanisms, the present study followed a mixed-method approach and explored the role of data governance to mitigate users' privacy concerns, complexity barriers, and value barriers in relation to resistance to SHMS. We proposed a concern mitigation data governance model for SHMS users' resistance and offered actionable insights for healthcare providers, technology providers, and policymakers. This study has a few limitations. For example, our survey findings may be affected by sample selection bias. People who participated in this survey were individuals from New Zealand and Australia at the time of the survey, which might limit the generalizability of this study. This limitation arises from the importance of geographical, regulatory, and cultural (localization) aspects in attitudes and behaviors responding to psychological and functional barriers. Another limitation is that we are focusing on the perspectives of potential SHMS users rather than the experiences of real users. The findings that challenge prevailing notions of concerns and barriers pave the way for new directions in future research. For example, while transparency emerges as a significant factor in addressing privacy concerns, its insignificance in functional barriers warrants further exploration from a dual perspective.

6 References

Abraham, R., Schneider, J., and Vom Brocke, J. 2019. "Data Governance: A Conceptual Framework, Structured Review, and Research Agenda," *International Journal of Information Management* (49), pp. 424-438 (doi: 10.1016/j.ijinfomgt.2019.07.008).

Accenture.com. 2020. "How Can Leaders Make Recent Digital Health Gains Last?," (available at https://www.accenture.com/us-en/insights/health/leaders-make-recent-digital-health-gains-last, retrieved April 26, 2024).

Ågerfalk, P. J. 2013. "Embracing Diversity through Mixed Methods Research," *European Journal of Information Systems* (22:3), pp. 251-256 (doi: 10.1057/ejis.2013.6).

Akmandor, A. O., and Jha, N. K. 2018. "Smart Health Care: An Edge-Side Computing Perspective," *IEEE Consumer Electronics Magazine* (7:1), pp. 29-37 (doi: 10.1109/MCE.2017.2746096).

Alashoor, T., Keil, M., Liu, L., and Smith, J. 2015. "How Values Shape Concerns About Privacy for Self and Others," in: *2015 International Conference on Information Systems: Exploring the Information Frontier*. Fort Worth, Texas: Association for Information Systems. AIS Electronic Library (AISeL).

Almujally, N. A., Aljrees, T., Saidani, O., Umer, M., Faheem, Z. B., Abuzinadah, N., Alnowaiser, K., and Ashraf, I. 2023. "Monitoring Acute Heart Failure Patients Using Internet-of-Things-Based Smart Monitoring System," *Sensors* (23:10) (doi: 10.3390/s23104580).

Alsyouf, A., Masa'deh, R. e., Albugami, M., Al-Bsheish, M., Lutfi, A., and Alsubahi, N. 2021. "Risk of Fear and Anxiety in Utilising Health App Surveillance Due to Covid-19: Gender Differences Analysis," *Risks* (9:179) (doi: 10.3390/risks9100179).

Banville, M. C. 2020. "Resisting Surveillance: Responding to Wearable Device Privacy Policies," *Proceedings of the 38th ACM International Conference on Design of Communication*, pp. 1-8 (doi: 10.1145/3380851.3416764).

Beaudin, J. S., Intille, S. S., and 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), pp. 1-29 (doi: 10.2196/jmir.8.4.e29).

Bélanger, F., and Crossler, R. E. 2011. "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems," *MIS Quarterly* (35:4), pp. 1017-1041 (doi: 10.2307/41409971).

Borgman, H., Heier, H., Bahli, B., and Boekamp, T. 2016. "Dotting the I and Crossing (out) the T in It Governance: New Challenges for Information Governance," *2016 49th Hawaii International Conference on System Sciences (HICSS)*: IEEE, pp. 4901-4909 (doi: 10.1109/HICSS.2016.608).

Borraz-Mora, J., Bordonaba-Juste, V., and Polo-Redondo, Y. 2017. "Functional Barriers to the Adoption of Electronic Banking: The Moderating Effect of Gender," *Revista de Economía Aplicada* (25:75), pp. 87-107 (doi:

Braun, V., and Clarke, V. 2006. "Using Thematic Analysis in Psychology," *Qualitative Research in Psychology* (3:2), pp. 77-101 (doi: 10.1191/1478088706qp0630a).

Burgoon, J. K. 1982. "Privacy and Communication," *Annals of the International Communication Association* (6:1), pp. 206-249 (doi: 10.1080/23808985.1982.11678499).

Capterra.com. 2021. "New Technologies for Telehealth in Canada: 61% of Canadians Want to Implement Ai," (available at https://www.capterra.ca/blog/2039/telehealth-in-canada-technology-ai, retrieved 24 May, 2023).

Chang, Y., and Fang, S. 2013. "Antecedents and Distinctions between Online Trust and Distrust: Predicting High-and Low-Risk Internet Behaviors," *Journal of Electronic Commerce Research* (14:2), pp. 149-166 (doi:

Chibuike, M. C., Sara, G. S., and Adele, B. 2024. "Overcoming Challenges for Improved Patient-Centric Care: A Scoping Review of Platform Ecosystems in Healthcare," *IEEE Access*) (doi:

Chin, W. W. 2009. "How to Write up and Report Pls Analyses," in *Handbook of Partial Least Squares: Concepts, Methods and Applications*. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 655-690.

Choi, J. R., and Kim, S. 2024. "Predicting Individuals' Privacy Protection and Self-Tracking Behaviors in the Context of Smart Health," *Telematics and Informatics* (86), p. 102069 (doi: 10.1016/j.tele.2023.102069).

Chouk, I., and Mani, Z. 2019. "Factors for and against Resistance to Smart Services: Role of Consumer Lifestyle and Ecosystem Related Variables," *Journal of Services Marketing* (33:4), pp. 449-462 (doi: 10.1108/JSM-01-2018-0046).

Chu, X., Luo, X., and Chen, Y. 2019. "A Systematic Review on Cross-Cultural Information Systems Research: Evidence from the Last Decade," *Information & Management* (56:3), pp. 403-417 (doi: 10.1016/j.im.2018.08.001).

Creswell, J. W., and Plano Clark, V. L. 2018. *Designing and Conducting Mixed Methods Research*, (Third ed.). Los Angeles: Sage.

Creswell, J. W., and Poth, C. N. 2018. *Qualitative Inquiry and Research Design: Choosing among Five Approaches*, (4th ed.). Sage.

Dahlsrud, A. 2008. "How Corporate Social Responsibility Is Defined: An Analysis of 37 Definitions," *Corporate Social Responsibility and Environmental Management* (15:1), pp. 1-13 (doi: 10.1002/csr.132).

DAMA International. 2009. *The Dama Guide to the Data Management Body of Knowledge*. New Jersey: Technics Publications, LLC.

Davidson, E., Wessel, L., Winter, J. S., and Winter, S. 2023. "Future Directions for Scholarship on Data Governance, Digital Innovation, and Grand Challenges," *Information and Organization* (33:1) (doi: 10.1016/j.infoandorg.2023.100454).

Dinev, T., and Hart, P. 2006. "An Extended Privacy Calculus Model for E-Commerce Transactions," *Information Systems Research* (17:1), pp. 61-80 (doi: 10.1287/isre.1060.0080).

Dinev, T., Hart, P., and Mullen, M. R. 2008. "Internet Privacy Concerns and Beliefs About Government Surveillance – an Empirical Investigation," *The Journal of Strategic Information Systems* (17:3), pp. 214-233 (doi: 10.1016/j.jsis.2007.09.002).

Duckert, M., and 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), pp. 1-22 (doi: 10.1145/3492830).

Ebrahim, A. H., and Buheji, M. 2020. "A Pursuit for a 'Holistic Social Responsibility Strategic Framework'addressing Covid-19 Pandemic Needs," *American Journal of Economics* (10:5), pp. 293-304 (doi: 10.5923/j.economics.20201005.04).

Elahi, H., Wang, G., Peng, T., and Chen, J. 2019. "On Transparency and Accountability of Smart Assistants in Smart Cities," *Applied Sciences* (9:24) (doi: 10.3390/app9245344).

Esmaeilzadeh, P. 2023. "Older Adults' Perceptions About Using Intelligent Toilet Seats Beyond Traditional Care: Web-Based Interview Survey," *JMIR mHealth and uHealth* (11:1) (doi: 10.2196/46430).

Fortune.com. 2023. "The Best Technology to Prevent Falls, Monitor Safety, and Help Older Adults Age in Place Longer," (available at https://fortune.com/well/2023/02/03/technology-can-help-older-adults-age-in-place-longer/, retrieved April 26, 2024).

Friedman, N., and Ormiston, J. 2022. "Blockchain as a Sustainability-Oriented Innovation?: Opportunities for and Resistance to Blockchain Technology as a Driver of Sustainability in Global Food Supply Chains," *Technological Forecasting and Social Change* (175) (doi: 10.1016/j.techfore.2021.121403).

Gasser, U., Ienca, M., Scheibner, J., Sleigh, J., and Vayena, E. 2020. "Digital Tools against Covid-19: Taxonomy, Ethical Challenges, and Navigation Aid," *The Lancet Digital Health* (2:8), pp. e425-e434 (doi: 10.1016/S2589-7500(20)30137-0).

GlobeNewswire. 2023. "Smart Medical Devices Market Expecting to Hit Usd 474 Billion by 2032, with a Cagr of 12.3 %," (available at 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, retrieved April 26, 2024).

Hair, J., Hair Jr, J. F., Sarstedt, M., Ringle, C. M., and Gudergan, S. P. 2023. *Advanced Issues in Partial Least Squares Structural Equation Modeling*. Sage.

Hair, J. F., Risher, J. J., Sarstedt, M., and Ringle, C. M. 2019. "When to Use and How to Report the Results of Pls-Sem," *European Business Review* (31:1), pp. 2-24 (doi: 10.1108/EBR-11-2018-0203).

Hatuka, T., and Zur, H. 2020. "Who Is the 'Smart'resident in the Digital Age? The Varied Profiles of Users and Non-Users in the Contemporary City," *Urban Studies* (57:6), pp. 1260-1283 (doi: 10.1177/0042098019835690).

Hew, J.-J., Leong, L.-Y., Tan, G. W.-H., Ooi, K.-B., and Lee, V.-H. 2019. "The Age of Mobile Social Commerce: An Artificial Neural Network Analysis on Its Resistances," *Technological Forecasting and Social Change* (144), pp. 311-324 (doi: 10.1016/j.techfore.2017.10.007).

Ismail, L., Materwala, H., Karduck, A. P., and Adem, A. 2020. "Requirements of Health Data Management Systems for Biomedical Care and Research: Scoping Review," *Journal of Medical Internet Research* (22:7) (doi: 10.2196/17508).

Iyanna, S., Kaur, P., Ractham, P., Talwar, S., and Najmul Islam, A. K. M. 2022. "Digital Transformation of Healthcare Sector. What Is Impeding Adoption and Continued Usage of Technology-Driven Innovations by End-Users?," *Journal of Business Research* (153), pp. 150-161 (doi: 10.1016/j.jbusres.2022.08.007).

Jain, P., Gyanchandani, M., and Khare, N. 2016. "Big Data Privacy: A Technological Perspective and Review," *Journal of Big Data* (3:1), p. 25 (doi: 10.1186/s40537-016-0059-y).

Janssen, M., Brous, P., Estevez, E., Barbosa, L. S., and Janowski, T. 2020. "Data Governance: Organizing Data for Trustworthy Artificial Intelligence," *Government Information Quarterly* (37:3), p. 101493 (doi: 10.1016/j.giq.2020.101493).

Kamal, S. A., Shafiq, M., and Kakria, P. 2020. "Investigating Acceptance of Telemedicine Services through an Extended Technology Acceptance Model (Tam)," *Technology in Society* (60), p. 101212 (doi: 10.1016/j.techsoc.2019.101212).

Karadag, E., Parlar Kilic, S., Ugur, O., and Akyol, M. A. 2019. "Attitudes of Nurses in Turkey toward Care of Dying Individual and the Associated Religious and Cultural Factors," *Journal of Religion and Health* (58), pp. 303-316 (doi: 10.1007/s10943-018-0657-4).

Kaur, P., Dhir, A., Singh, N., Sahu, G., and Almotairi, M. 2020. "An Innovation Resistance Theory Perspective on Mobile Payment Solutions," *Journal of Retailing and Consumer Services* (55) (doi: 10.1016/j.jretconser.2020.102059).

Khanna, S., and Srivastava, S. 2020. "Patient-Centric Ethical Frameworks for Privacy, Transparency, and Bias Awareness in Deep Learning-Based Medical Systems," *Applied Research in Artificial Intelligence and Cloud Computing* (3:1), pp. 16-35 (doi:

Khanra, S., Dhir, A., Kaur, P., and Joseph, R. P. 2021. "Factors Influencing the Adoption Postponement of Mobile Payment Services in the Hospitality Sector During a Pandemic," *Journal of Hospitality and Tourism Management* (46), pp. 26-39 (doi: 10.1016/j.jhtm.2020.11.004).

Khatri, V., and Brown, C. V. 2010. "Designing Data Governance," *Communications of the ACM* (53:1), pp. 148-152 (doi: 10.1145/1629175.1629210).

Kim, B., Hong, S., and Cameron, G. T. 2014. "What Corporations Say Matters More Than What They Say They Do? A Test of a Truth Claim and Transparency in Press Releases on Corporate Websites and Facebook Pages," *Journalism & Mass Communication Quarterly* (91:4), pp. 811-829 (doi: 10.1177/1077699014550087).

Knoppers, B. M., and Thorogood, A. M. 2017. "Ethics and Big Data in Health," *Current Opinion in Systems Biology* (4), pp. 53-57 (doi: 10.1016/j.coisb.2017.07.001).

Kulyk, O., Reinheimer, B., Aldag, L., Mayer, P., Gerber, N., and Volkamer, M. 2020. "Security and Privacy Awareness in Smart Environments–a Cross-Country Investigation," *Proceedings of AsiaUSEC 2020, Financial Cryptography and Data Security*: Springer, pp. 84-101 (doi: 10.1007/978-3-030-54455-3_7).

Laukkanen, T., Sinkkonen, S., Kivijärvi, M., and Laukkanen, P. 2007. "Innovation Resistance among Mature Consumers," *Journal of Consumer Marketing* (24:7), pp. 419-427 (doi: 10.1108/07363760710834834).

Lee, H. 2020. "Home Iot Resistance: Extended Privacy and Vulnerability Perspective," *Telematics and Informatics* (49) (doi: 10.1016/j.tele.2020.101377).

Lis, D., and Otto, B. 2021. "Towards a Taxonomy of Ecosystem Data Governance," *Proceedings of the 54th Hawaii International Conference on System Sciences 2021*, pp. 6067-6076 (doi:

Lomotey, R. K., Pry, J., and Sriramoju, S. 2017. "Wearable Iot Data Stream Traceability in a Distributed Health Information System," *Pervasive and Mobile Computing* (40), pp. 692-707 (doi: 10.1016/j.pmcj.2017.06.020).

Lwin, M., Wirtz, J., and Williams, J. D. 2007. "Consumer Online Privacy Concerns and Responses: A Power–Responsibility Equilibrium Perspective," *Journal of the Academy of Marketing Science* (35:4), pp. 572-585 (doi: 10.1007/s11747-006-0003-3).

Mani, Z., and Chouk, I. 2017. "Drivers of Consumers' Resistance to Smart Products," *Journal of Marketing Management* (33:1/2), pp. 76-97 (doi: 10.1080/0267257X.2016.1245212).

Martin, K., and Nissenbaum, H. 2016. "Measuring Privacy: An Empirical Test Using Context to Expose Confounding Variables," *Columbia Science and Technology Law Review* (18:1), pp. 176-218 (doi: 10.2139/ssrn.2709584).

Miltgen, C. L., and 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), pp. 103-125 (doi: 10.1057/ejis.2013.17).

Nguyen, T. T., Tran Hoang, M. T., and Phung, M. T. 2022. "“To Our Health!” Perceived Benefits Offset Privacy Concerns in Using National Contact-Tracing Apps," *Library Hi Tech* (41:1), pp. 174-191 (doi: 10.1108/LHT-12-2021-0461).

Nissenbaum, H. 2010. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, California: Stanford University Press.

Orbaiz, M. L. V., and Arce-Urriza, M. 2024. "The Role of Active and Passive Resistance in New Technology Adoption by Final Consumers: The Case of 3d Printing," *Technology in Society* (77), p. 102500 (doi: 10.1016/j.techsoc.2024.102500).

Park, E. H., Werder, K., Cao, L., and Ramesh, B. 2022a. "Why Do Family Members Reject Ai in Health Care? Competing Effects of Emotions," *Journal of Management Information Systems* (39:3), pp. 765-792 (doi: 10.1080/07421222.2022.2096550).

Park, I., Kim, D., Moon, J., Kim, S., Kang, Y., and Bae, S. 2022b. "Searching for New Technology Acceptance Model under Social Context: Analyzing the Determinants of Acceptance of Intelligent Information Technology in Digital Transformation and Implications for the Requisites of Digital Sustainability," *Sustainability* (14:1), p. 579 (doi: 10.3390/su14010579).

Perry-Hazan, L., Finefter-Rosenbluh, I., and Muzikovskaya, E. 2021. "Secular Teachers in Jewish Religious Schools: Passing, Resistance, and Freedom of Religion," *Oxford Review of Education* (47:4), pp. 495-512 (doi: 10.1080/03054985.2020.1862780).

Pirzada, P., Wilde, A., Doherty, G. H., and Harris-Birtill, D. 2021. "Ethics and Acceptance of Smart Homes for Older Adults," *Informatics for Health and Social Care* (47:1), pp. 10-37 (doi: 10.1080/17538157.2021.1923500).

Plotkin, D. 2020. *Data Stewardship : An Actionable Guide to Effective Data Management and Data Governance*. San Diego, US: Elsevier Science & Technology.

Prakash, A. V., and Das, S. 2022. "Explaining Citizens' Resistance to Use Digital Contact Tracing Apps: A Mixed-Methods Study," *International Journal of Information Management* (63) (doi: 10.1016/j.ijinfomgt.2021.102468).

Prati, A., Shan, C., and Wang, K. I.-K. 2019. "Sensors, Vision and Networks: From Video Surveillance to Activity Recognition and Health Monitoring," *Journal of Ambient Intelligence and Smart Environments* (11:1), pp. 5-22 (doi: 10.3233/AIS-180510).

Princi, E., and 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), pp. 1-15 (doi: 10.3389/fpsyg.2020.582054).

Puntoni, S., Reczek, R. W., Giesler, M., and Botti, S. 2021. "Consumers and Artificial Intelligence: An Experiential Perspective," *Journal of Marketing* (85:1), pp. 131-151 (doi: 10.1177/0022242920953847).

Ram, S., and Sheth, J. N. 1989. "Consumer Resistance to Innovations: The Marketing Problem and Its Solutions," *Journal of Consumer Marketing* (6:2), pp. 5-14 (doi: 10.1108/EUM0000000002542).

Rosenbaum, S. 2010. "Data Governance and Stewardship: Designing Data Stewardship Entities and Advancing Data Access," *Health Services Research* (45:5p2), pp. 1442-1455 (doi: 10.1111/j.1475-6773.2010.01140.x).

Salehi-Amiri, A., Jabbarzadeh, A., Hajiaghaei-Keshteli, M., and Chaabane, A. 2022. "Utilizing the Internet of Things (Iot) to Address Uncertain Home Health Care Supply Chain Network," *Expert Systems with Applications* (208), p. 118239 (doi: 10.1016/j.eswa.2022.118239).

Schwartz, S. H. 2012. "An Overview of the Schwartz Theory of Basic Values," *Online Readings in Psychology and Culture* (2:1), pp. 1-20 (doi: 10.9707/2307-0919.1116).

Shen, Y.-C., Wang, M.-Y., and Yang, Y.-C. 2020. "Discovering the Potential Opportunities of Scientific Advancement and Technological Innovation: A Case Study of Smart Health Monitoring Technology," *Technological Forecasting and Social Change* (160), p. 120225 (doi: 10.1016/j.techfore.2020.120225).

Smith, H. J., Dinev, T., and Xu, H. 2011. "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly* (35:4), pp. 989-1015 (doi: 10.2307/41409970).

Solove, D. J. 2002. "Conceptualizing Privacy," *California Law Review* (90:4), pp. 1087-1155 (doi: 10.2307/3481326).

Solove, D. J. 2006. "A Taxonomy of Privacy," *University of Pennsylvania Law Review* (154:3), pp. 477-564 (doi: 10.2307/40041279).

Someh, I., Davern, M., Breidbach, C. F., and Shanks, G. 2019. "Ethical Issues in Big Data Analytics: A Stakeholder Perspective," *Communications of the Association for Information Systems* (44), pp. 718-747 (doi: 10.17705/1CAIS.04434).

Son, J.-Y., and Kim, S. S. 2008. "Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model," *MIS Quarterly*), pp. 503-529 (doi: 10.2307/25148854).

Stavropoulos, T. G., Papastergiou, A., Mpaltadoros, L., Nikolopoulos, S., and Kompatsiaris, I. 2020. "Iot Wearable Sensors and Devices in Elderly Care: A Literature Review," *Sensors* (20:10), p. 2826 (doi: 10.3390/s20102826).

Talal, M., Zaidan, A., Zaidan, B., Albahri, A. S., Alamoodi, A., Albahri, O. S., Alsalem, M., Lim, C. K., Tan, K. L., Shir, W., and 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) (doi: 10.1007/s10916-019-1158-z).

Tallon, P. P. 2013. "Corporate Governance of Big Data: Perspectives on Value, Risk, and Cost," *Computer* (46:6), pp. 32-38 (doi: 10.1109/MC.2013.155).

Tallon, P. P., Ramirez, R. V., and Short, J. E. 2013. "The Information Artifact in It Governance: Toward a Theory of Information Governance," *Journal of Management Information Systems* (30:3), pp. 141-178 (doi: 10.2753/MIS0742-1222300306).

Talwar, S., Dhir, A., Islam, N., Kaur, P., and Almusharraf, A. 2023. "Resistance of Multiple Stakeholders to E-Health Innovations: Integration of Fundamental Insights and Guiding Research Paths," *Journal of Business Research* (166) (doi: 10.1016/j.jbusres.2023.114135).

Taylor, S. J., Bogdan, R., and DeVault, M. 2016. *Introduction to Qualitative Research Methods: A Guidebook and Resource*, (4th ed.). Hoboken, United States: John Wiley & Sons, Incorporated.

Timan, T., and Albrechtslund, A. 2018. "Surveillance, Self and Smartphones: Tracking Practices in the Nightlife," *Science and Engineering Ethics* (24:3), pp. 853-870 (doi: 10.1007/s11948-015-9691-8).

Trkman, M., Popovič, A., and Trkman, P. 2023. "The Roles of Privacy Concerns and Trust in Voluntary Use of Governmental Proximity Tracing Applications," *Government Information Quarterly* (40:1) (doi: 10.1016/j.giq.2022.101787).

Van Zoonen, L. 2016. "Privacy Concerns in Smart Cities," *Government Information Quarterly* (33:3), pp. 472-480 (doi: 10.1016/j.giq.2016.06.004).

Venkatesh, V., Brown, S. A., and Bala, H. 2013. "Bridging the Qualitative-Quantitative Divide: Guidelines for Conducting Mixed Methods Research in Information Systems," *MIS Quarterly* (37:1), pp. 21-54 (doi: 10.25300/MISQ/2013/37.1.02).

Venkatesh, V., Brown, S. A., and Sullivan, Y. W. 2016. "Guidelines for Conducting Mixed-Methods Research: An Extension and Illustration," *Journal of the Association for Information Systems* (17:7), pp. 435-495 (doi: 10.17705/1jais.00433).

von Humboldt, S., Mendoza-Ruvalcaba, N. M., Arias-Merino, E. D., Costa, A., Cabras, E., Low, G., and Leal, I. 2020. "Smart Technology and the Meaning in Life of Older Adults During the Covid-19 Public Health Emergency Period: A Cross-Cultural Qualitative Study," *International Review of Psychiatry* (32:7-8), pp. 713-722 (doi: 10.1080/09540261.2020.1810643).

Weber, R. H. 2010. "Internet of Things–New Security and Privacy Challenges," *Computer Law & Security Review* (26:1), pp. 23-30 (doi: 10.1016/j.clsr.2009.11.008).

Wu, X., Xiong, J., Yan, J., and Wang, Y. 2021. "Perceived Quality of Traceability Information and Its Effect on Purchase Intention Towards Organic Food," *Journal of Marketing Management* (37:13-14), pp. 1267-1286 (doi: 10.1080/0267257X.2021.1910328).

Xu, Z. 2019. "An Empirical Study of Patients' Privacy Concerns for Health Informatics as a Service," *Technological Forecasting and Social Change* (143), pp. 297-306 (doi: 10.1016/j.techfore.2019.01.018).

Yan, Z., Kantola, R., and Zhang, P. 2011. "A Research Model for Human-Computer Trust Interaction," in: *2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications*. Changsha, China: IEEE, pp. 274-281.

Yaqoob, I., Salah, K., Jayaraman, R., and Al-Hammadi, Y. 2022. "Blockchain for Healthcare Data Management: Opportunities, Challenges, and Future Recommendations," *Neural Computing and Applications*), pp. 1-16 (doi: 10.1007/s00521-020-05519-w).

Zhu, M., Wu, C., Huang, S., Zheng, K., Young, S. D., Yan, X., and Yuan, Q. 2021. "Privacy Paradox in Mhealth Applications: An Integrated Elaboration Likelihood Model Incorporating Privacy Calculus and Privacy Fatigue," *Telematics and Informatics* (61) (doi: 10.1016/j.tele.2021.101601).

Zhu, Y., Lu, Y., Gupta, S., Wang, J., and 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), pp. 257-272 (doi: 10.1108/JRIM-10-2021-0246).

Zimmerman, M. A. 2000. "Empowerment Theory," in *Handbook of Community Psychology,* J. Rappaport and E. Seidman (eds.). Boston, MA: Springer, pp. 43-63.

Copyright