Surveillance & Society

User Perception of Smart Home Surveillance: An Integrative Review

Jessica Percy-Campbell, Jacob Buchan, Charlene H. Chu, Andria Bianchi, Jesse Hoey et Shehroz S. Khan

Volume 22, numéro 3, 2024

Open Issue

URI : https://id.erudit.org/iderudit/1113685ar
DOI : https://doi.org/10.24908/ss.v22i3.16084

Aller au sommaire du numéro

Éditeur(s)

Surveillance Studies Network

ISSN

1477-7487 (numérique)

Découvrir la revue

Citer cet article

Percy-Campbell, J., Buchan, J., Chu, C., Bianchi, A., Hoey, J. & Khan, S. (2024). User Perception of Smart Home Surveillance: An Integrative Review. *Surveillance & Society*, *22*(3), 304–324. https://doi.org/10.24908/ss.v22i3.16084

Résumé de l'article

Smart Home Technologies (SHTs) have recently become popular for a variety of purposes, including healthcare, entertainment, and convenience, among others. While SHT manufacturers promise to provide a range of services relating to home security, health and wellness, automated domestic tasks, entertainment, and beyond, user perceptions vary widely in terms of benefits and drawbacks. Moreover, surveillance studies researchers have warned against normalizing technologies that may exacerbate uneven power dynamics between users and household members, marketing companies, insurance brokers, law enforcement, and others. Through an analysis of the interdisciplinary literature stemming from computer science and engineering, gerontology, the social sciences, and related fields, we explore the extent to which these potential risks and related concerns are reflected upon by smart home users. This scoping review aims to explore SHT user perceptions of privacy attitudes, the purposes of smart home surveillance, risks and benefits, and impacts on home safety. Through our review of sixty-eight relevant studies, we found that many smart home users reported satisfaction over perceived benefits such as an increased sense of safety and home security. Many others displayed limited understandings of data collection practices or expressed privacy concerns. Nonetheless, SHT usage prevailed among these users. Others report a perceived trade-off between privacy and other factors, such as convenience, and some may have resorted to privacy cynicism, a coping mechanism for dealing with ubiquitous surveillance. In order to better understand SHT adoption trends despite concerns, exploring the conflict between user perceptions of privacy, understanding of SHT data collection purposes, risks and benefits, and home safety, is essential.

Surveillance & Society

Article

User Perception of Smart Home Surveillance: An Integrative Review

Jessica Percy-Campbell
University of Victoria, Canada
jpercycampbell@uvic.ca

Jacob Buchan
University of Toronto, Canada
jacob.buchan@mail.utoronto.ca

Charlene H. Chu
University of Toronto, Canada
charlene.chu@utoronto.ca

Andria Bianchi
University Health Network, Canada
andria.bianchi@uhn.ca

Jesse Hoey
University of Waterloo, Canada
jesse.hoey@uwaterloo.ca

Shehroz S. Khan
University of Toronto, Canada
shehroz.khan@utoronto.ca

Abstract

Smart Home Technologies (SHTs) have recently become popular for a variety of purposes, including healthcare, entertainment, and convenience, among others. While SHT manufacturers promise to provide a range of services relating to home security, health and wellness, automated domestic tasks, entertainment, and beyond, user perceptions vary widely in terms of benefits and drawbacks. Moreover, surveillance studies researchers have warned against normalizing technologies that may exacerbate uneven power dynamics between users and household members, marketing companies, insurance brokers, law enforcement, and others. Through an analysis of the interdisciplinary literature stemming from computer science and engineering, gerontology, the social sciences, and related fields, we explore the extent to which these potential risks and related concerns are reflected upon by smart home users. This scoping review aims to explore SHT user perceptions of privacy attitudes, the purposes of smart home surveillance, risks and benefits, and impacts on home safety. Through our review of sixty-eight relevant studies, we found that many smart home users reported satisfaction over perceived benefits such as an increased sense of safety and home security. Many others displayed limited understandings of data collection practices or expressed privacy concerns. Nonetheless, SHT usage prevailed among these users. Others report a perceived trade-off between privacy and other factors, such as convenience, and some may have resorted to privacy cynicism, a coping mechanism for dealing with ubiquitous surveillance. In order to better understand SHT adoption trends despite concerns, exploring the conflict between user perceptions of privacy, understanding of SHT data collection purposes, risks and benefits, and home safety, is essential.

Introduction: The Rise of the Smart Home

Over the last two decades, innovative features and decreased prices have made smart home technologies (SHTs) more accessible to many. Improvements made to Internet of Things (IoT) capabilities, internet access in general, and faster WIFI connections have resulted in upward trends in SHT adoption (Lasquety-

Percy-Campbell, Jessica, Jacob Buchan, Charlene H. Chu, Andria Bianchi, Jesse Hoey, and Shehroz S. Khan. 2024. User Perception of Smart Home Surveillance: An Integrative Review. *Surveillance & Society* 22 (3): 304-324.
https://ojs.library.queensu.ca/index.php/surveillance-and-society/index | ISSN: 1477-7487

Reyes 2022). For example, 47% of Canadians reported using a smart home device in 2022, compared to 42% in 2020 (Statistics Canada 2022). Likewise, smart home device ownership in the United States rose from 33% of households in 2019 to 43% in 2021 (Thormundsson 2023). While SHTs differ substantially, they generally include some combination of IoT devices (e.g., voice activated smart speakers, locks, security cameras, lights) and related WIFI or sensor connected appliances controlled by smartphone apps (Zeng, Mare, and Roesner 2017; Zheng et al. 2018). Their key features are meant to enhance user convenience by way of easy access controls and custom automated processes, sometimes through Artificial Intelligence (AI), such as voice assistants (VAs) embedded into smart speakers (Park et al. 2022). While commercial SHTs are often used for entertainment purposes, home appliance control, home security, or managing energy consumption (Sadowski 2020), they can also include wearable devices and environmental sensors for healthcare and rehabilitation purposes (Chan et al. 2009; Demiris and Hensel 2008; Marikyan, Papagiannidis, and Alamanos 2019; Pirzada et al. 2022).

Conversely, throughout surveillance studies and related literature, SHTs have raised numerous ethical, privacy, and security concerns due to their invasive capabilities. Surveillance can be understood beyond passive monitoring as "the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction" (Lyon 2007: 14). In some ways, SHTs add an element of surveillance of the home but may have not yet fully "solidified their purpose," adding to user confusion over data collection practices (Pridmore and Mols 2020: 3). IoT devices, including SHTs, can collect and share behavioral user data with manufacturers and third parties for various reasons. User data can be used to train AI platforms (Eliot and Murakami Wood 2022) or to commodify user interactions through targeted advertising (Maalsen and Sadowski 2019; Zuboff 2019). Collecting VA interactions or transcripts for targeted advertisements can sometimes take place without user awareness or meaningful consent (Malkin et al. 2019), which is in part due to a lack of transparency in privacy policies and End User Agreements (EUAs) (Iqbal et al. 2022; Neville 2020). EUAs are often illegible to ordinary users (Neville 2021), which is a well-documented problem with online platforms in general (Obar and Oeldorf-Hirsch 2020). Further, SHT concerns span from the risk of unauthorized data access from unknown attackers (Abomhara and Køien 2014; Zhang et al. 2018) to the facilitation of domestic surveillance from potentially abusive partners (Parkin et al. 2019) to unwarranted law enforcement access to private spaces (Murakami Wood and Steeves 2021) and personalized insurance pricing (Carver and Mackinnon 2020; Sadowski 2020). This review draws on SHT user perception literature from various disciplines and analyses findings through a critical surveillance studies lens. The tendency for surveillance to lead to uneven power dynamics makes user perception of SHTs an important topic of inquiry.

In light of the above-mentioned concerns, the purpose of this integrative literature review is to explore users' privacy attitudes, their understanding of the purposes of smart home surveillance, as well as the risks and benefits and home safety perceptions. Further, we explore the extent to which users are informed about data collection practices, engage in perceived trade-offs between privacy and other factors, or display attitudes of privacy cynicism: "uncertainty, powerlessness and mistrust" or resignation in data handling (Lutz, Hoffmann, and Ranzini 2020: 1174). The overall aim is to shed light on the perceived benefits and drawbacks of SHTs from a user perspective, demonstrating that the growing popularity of SHTs does not necessarily imply that users are unconcerned about privacy or security risks. Ideally, a nuanced understanding of their attitudes can lead to user centric policy or design choices that preserve the most beneficial features of SHTs, such as safety or convenience, while limiting excessive surveillance capabilities or non-consensual data access and usage.

Our research questions were designed to explore a wide range of smart home user perception literature. The questions are as follows:

(1) Privacy: What are SHT users' privacy attitudes?

(2) Purpose: What are SHT users' understandings of data collection purposes?

(3) Risks/Benefits: How do users perceive the potential risks and benefits of SHTs?

(4) Safety: How do users perceive home safety in the context of SHTs?

Background: Surveillance Implications

Today, most public behavior, consumer transactions, and online activities are subject to some form of surveillance (Lyon 2018). Through SHTs, this trend has paved the way for large tech companies to further seep into the realm of domestic spaces. Although privacy, or control over information that pertains to oneself (Westin 1967), may be the first ethical implication that comes to mind, it ought to be further considered with related issues such as autonomy, dignity, informed consent, and differential treatment (Wright and Raab 2012). The negative consequences of automated and under regulated surveillance are perpetuated and even amplified by algorithms and AI systems to profile users, contributing to discrimination that further disadvantages oppressed or marginalized groups while rewarding others (Costanza-Chock 2020; Noble 2018; O'Neil 2016). Surveillance generally warrants skepticism towards its socio-political implications, as well as the potential for surveillance creep, where devices and data may be used beyond their original intent in the future (Bennett et al. 2014; Solove 2008). Although the full ethical implications of SHTs are yet to be seen, manufacturers and third parties have been criticized for relying on surveillance capitalism to commodify the user experience in an attempt to predict, modify, or control behavior (Neville 2020; Zuboff 2019. Further, marketing techniques make surveillance seem enjoyable or culturally acceptable (see Guo and Ohlheiser 2022), a phenomenon referred to as seductive surveillance (Troullinou 2017; see also Draper and Turow 2019; Neville 2020).

SHTs introduce the ability for unprecedented digital surveillance inside the home. As argued by Maalsen and Sadowski (2019: 120), "Watching people in their homes has always been, first and foremost, a way of exercising power." Surveillance often signals a power dynamic that favors the watcher (Gilliom and Monahan 2012; Sadowski 2020), which can be especially problematic in intimate settings (e.g., the home). Due to this fundamental relationship between power and surveillance, it is important to question the impact on SHT user privacy, autonomy, and dignity, not only with commercial smart home devices but also within healthcare or eldercare settings where such technologies are used (Mortenson, Sixsmith and Woolrych 2015). Although there may be major differences between commercial for-profit SHT companies and healthcare oriented SHT, an ethical tension related to privacy and autonomy remains (see Mortenson, Sixsmith and Woolrych 2015; Zhu et al. 2021).

Related Privacy Literature

In a number of settings, there tends to be a disconnect between privacy concerns (e.g., Auxier et al. 2019) and actual behaviour, such as engaging with intrusive customer loyalty programs (Draper and Turow 2019) or social media platforms (Hargittai and Marwick 2016). This is known as the privacy paradox (Draper and Turow 2019; Nissenbaum 2009), which has led to various attempts to theorize user behaviour. Some have argued the privacy paradox may result from a lack of user awareness over direct marketing practices or low levels of digital literacy (Dommeyer and Gross 2003; Park 2013). Others have noted that consumers are often asked to make trade-offs between privacy and access to personalized services or convenience (Draper 2017; Hoofnagle and Urban 2014; Westin 2003). The privacy calculus theory has been used to explain IoT users' trade-off decisions in giving up their personal information (Kim et al. 2019). For example, outside of healthcare settings, the ability to personalize services is often considered a salient factor in whether to give up personal information, more so than privacy risk (Kim et al. 2019). Even as concerned users might be expected to refrain from privacy invasive behaviour online, perceived benefits are often a key motivator for

self-disclosing personal information (Hoffmann, Lutz and Ranzini 2016). Nonetheless, the privacy calculus theory has been critiqued for its limited ability to fully explain the privacy paradox (Lutz, Hoffmann, and Ranzini 2020).

Draper and Turow (2019) have offered digital resignation as an alternative explanation for seemingly contradictory consumer behaviour, where feelings of powerlessness over a loss of privacy are a logical reaction to overwhelming environments of digital mass surveillance. Even though some digitally resigned individuals engage in privacy protecting behaviour, they often do not feel confident that such efforts will be fruitful (Draper and Turow 2019). Following Lutz, Hoffmann, and Ranzini (2020), alongside powerlessness, uncertainty, and mistrust, resignation is a component of the broader concept of privacy cynicism, where individual attempts at online privacy protection are viewed as limited or futile. Others have employed concepts of privacy helplessness (Cho 2022), surveillance realism (Dencik and Cable 2017), privacy fatigue (Choi, Park, and Jung 2018), or privacy apathy (Hargittai and Marwick 2016). Taken together, these concepts can be understood as coping strategies for engaging in privacy-invasive environments where surveillance is considered "inevitable or uncontrollable" (Cho 2022:165; Lutz, Hoffmann, and Ranzini 2020) and can be seen as pragmatic rather than paradoxical responses to surveillance intensive online environments (Hargittai and Marwick 2016). With the exception of a few studies (e.g., Kim et al. 2019; Lutz and Newlands 2021), such research often pertains to online environments such as social media platforms but not smart home or IoT users specifically. This work is an effort to begin to bridge that gap. We do so by exploring user privacy attitudes alongside other perceived risks and benefits and flagging patterns of uninformed users, perceived trade-offs, or privacy cynicism throughout.

Previous Research on Smart Home Surveillance

SHT user perception can be contextual and dynamic due to various factors. Researchers have often focused on barriers to SHT adoption, which can include perceptions of privacy, security, and risk (Chan et al. 2009; Marikyan, Papagiannidis, and Alamanos 2019; Paetz et al. 2011; Yang, Lee, and Zo 2017; Zheng et al. 2018). In further exploring the reasoning behind the acceptance and rejection of SHTs, cost, reliability, useability, and knowledge gaps about device functionality have been identified as key factors (Marikyan, Papagiannidis, and Alamanos 2019). Conflicted attitudes are often present, as SHT surveillance systems may make users feel more secure from outside intruders while simultaneously concerned about non-consensual data monitoring (Mäkinen 2016).

Smart speaker users often lack awareness in terms of the collection, use, and storage of voice recordings (Lau, Zimmerman, and Schaub 2018; Malkin et al. 2019). Users who expressed the need to trade privacy for convenience also vary in levels of awareness over data collection practices and may appear resigned (Lau, Zimmerman, and Schaub 2018). However, even among informed individuals, continued usage of SHTs does not necessarily imply full acceptance of their surveillance capabilities. For example, users find ways to negotiate privacy boundaries with their voice-activated devices, such as by avoiding sensitive topics in their vicinity or keeping them out of certain areas of the home (Pridmore and Mols 2020).

Certain SHT surveillance capabilities, such as video or audio recording, are most often related to feelings of privacy intrusion (Marikyan, Papagiannidis, and Alamanos 2019). However, SHTs that do not rely on capturing images, video footage, or voice recordings can still be used to make sensitive inferences about users in less obvious ways (Kröger 2018; Zheng et al. 2018). For instance, malicious actors may access data from smart thermostats to detect whether users are at home (Copos et al. 2016). Smart energy meters can also be used to infer various types of user behavior inside the home, including sleep cycles or bathroom activity (Kröger 2018). Smart light bulbs or thermostats may be used to make inferences about user sleep patterns or home occupancy rates (Zheng et al. 2018). Often, users trust SHT manufacturers to secure their private data without verifying security claims, resulting in the absence of informed privacy choices (Zheng et al. 2018).

Previous literature reviews have often focused on SHTs in healthcare, rehabilitation, or independent aging (e.g., Choukou et al. 2021; Read et al. 2022; Zhu et al. 2021). In the case of older adults, user perceptions of SHTs may depend on their trust toward caregivers with access to device data (Lie, Lindsay, and Brittain 2016), who sometimes lack technological literacy themselves (Parzen et al. 2021). User trust is essential, as dignity and self-esteem are connected to one's ability to control their privacy preferences (Berridge and Wetle 2020). Older adults may generally prefer certain types of SHTs, such as motion sensors, over cameras or microphones (Fritz and Dermody 2019). Further, even as SHTs may represent potential health and safety benefits for older adults, there are many cases in which trading privacy for safety or convenience may not be seen as an acceptable choice by users, especially when sensitive data are involved (Carver and Mackinnon 2020). Overall, there are numerous potential explanations as to why many individuals would accept SHTs into their private spaces, even if they do not fully accept their surveillance capabilities. To better understand this phenomenon, we summarize and examine user attitudes from sixty-eight studies on SHTs.

Methods

To gain a deeper understanding of smart home user attitudes and behaviour, we utilized an integrative review framework. This is an established and rigorous method of generating a comprehensive review of the literature. Integrative reviews are useful for amassing a broad range of research articles from various theoretical backgrounds and empirical methods to further understand a certain phenomenon (Whittemore and Knafl 2005). This framework was most suitable for our task of reviewing papers from various academic backgrounds under the lens of privacy and surveillance literature.

Data Synthesis

The selected studies' data were imported to record the publication date, country, number of participants, demographic information (e.g., age, gender), research method, research question, type of technology, a summary of key findings, and for examples of uninformed users, trade-offs, or privacy cynicism. Following our research questions, we classified each study under the non-mutually exclusive themes of privacy, the purpose of data collection, and risks/benefits or safety. The data extraction (see Appendix 1) shows the total number of studies in each classified theme with their citations.

Search Strategy

A health information specialist helped to identify and refine the list of keywords[1] for the search strategy as shown alongside Figure 1. The keywords were selected by our research team based on relevance to our research questions about privacy, the purpose of data collection, the perceived risks and benefits, and the perceived home safety regarding various SHTs. The search for peer reviewed English studies was conducted in the following databases, which were selected and refined by the health information specialist: Ovid MEDLINE; Ovid Embase; Cochrane Database of Systematic Reviews (Ovid); Cochrane Central Register of Controlled Trials (Ovid); Scopus; Web of Science Core Collection; and IEEE Xplore / IET Electronic Library (IEL). Publication dates of our accepted studies ranged from 2011 to October 2021. The final results of all collected studies were imported into Covidence to manage the screening process.

[1] List of search keywords: (smart home*) OR (intelligent home*) OR (smart house*) OR (home automation) OR domotic OR smarthome OR homeseer OR homekit OR mihome OR homeOS OR "Google home" OR "Amazon home" OR (smart environment) OR "ubiquitous home*" OR (smart apartment) OR (home intelligence) OR (home network) OR (remote control home) OR (smart appliance) OR (ambient sensor) OR (Ambient assistive living) OR (Smart speaker) OR (Voice assistant) OR Agetech OR Gerontechnolog*) AND (surveill* OR security OR privacy OR (data collection) OR (data access) OR (data own) OR risk* OR benefit OR safety OR safe OR monitoring) AND (focus group or qualitative or ethnographic or ethnography or fieldwork or "field work" or "key informant" OR interview OR interviews OR questionnaire OR questionnaires OR survey OR surveys OR themes OR phenomenology OR Delphi OR narration).

Inclusion and Exclusion Criteria

To meet selection criteria, included peer-reviewed studies primarily focused on smart home user perception of privacy, data collection purposes, attitudes towards physical safety, and perceived risks or social benefits with SHTs. These four themes were selected to highlight both the perceived SHT pitfalls and benefits from the user perspective. The privacy theme was selected to tease out user attitudes surrounding data collection and sharing with various entities such as household members, manufacturers and advertisers, healthcare providers, and government or law enforcement. Next, the purpose theme was chosen to expose user understanding levels of what data are collected and why. Although there is some overlap within the risks and benefits category and the previous categories, this theme highlights user perceptions of risk that span beyond privacy into the realms of security issues such as the potential for hacking, technological dependence or loss of autonomy, and the cost of SHTs, among others. It also measures perceived benefits such as convenience, entertainment, healthcare, or home security, which are sometimes balanced against perceived risks through trade-offs. Finally, the safety theme explores user understanding of how SHTs can impact feelings of physical safety and security at home, such as through emergency contact features or fall detection services. Studies with participants from all age groups were included as long as users were community dwelling as opposed to living in care homes (e.g., nursing homes), assisted living facilities, or hospitals. The complexities of these clinical settings surrounding SHTs (e.g., legal requirements, staff and patient consent) were beyond the scope of this review. Qualitative, quantitative, or mixed methods empirical studies that measured user perception of smart home surveillance through questionnaires, surveys, interviews, or focus groups were included.

Exclusion criteria were as follows: (1) studies focused solely on wearables or smart phones (due to their use outside of the home); (2) energy grid studies that related to cost or sustainability; (3) studies that were solely technical (e.g., algorithm or system development) or theoretical; (4) system feasibility studies, as they did not reflect user perception; (5) other review papers; (6) usability or acceptability studies that were unrelated to our research questions on privacy, data collection purpose, safety, or risk. To ensure reliability and limit subjective biases, the selection of articles in each phase required the acceptance of two team members who worked independently of each other. In the final phase, each paper that passed the abstract review phase was assigned to be read in full and evaluated by at least two team members. The two team members then independently accepted or rejected in the Covidence review management software. In the rare event of disagreement where one team member accepted a paper and the other rejected it, the consensus was achieved through weekly team discussions among the team of four researchers. In these meetings, each team member would explain their reasoning for exclusion or inclusion followed by a team vote to finalize the decision. Finally, accepted papers were divided up to be summarized, categorized into relevant themes based on relevance to research questions, and entered into a shared spreadsheet for data extraction that was then further reviewed and finalized for consistency across categories.

Search Results

Our search yielded 2,398 titles and abstracts that were screened. The PRISMA flow diagram in Figure 1 outlines the screening process. We selected 146 full-text articles for full-text review. Of these, sixty-eight articles were included in this review paper based on the abovementioned inclusion criteria. After two team members read each of the full text articles, seventy-eight were excluded for the following reasons: they centered on the wrong population, such as non-users or consumers in general (forty-three studies); the focus was not substantially related to research questions (seventeen studies); the research was conducted in the wrong setting outside of the home (seven studies); the research examined the wrong technology (five studies); the researchers implemented the wrong study design (four studies); or the studies were not written in English (two studies).

Most included studies focused on participants from the US and UK, but SHT user perspectives spanned over twenty-five countries with a range of user demographics (see Table 1). Further, while the majority of

studies focused on users of all ages, fifteen studies focused exclusively on adults aged over fifty (see Appendix 1), the results of which we explore in depth elsewhere.

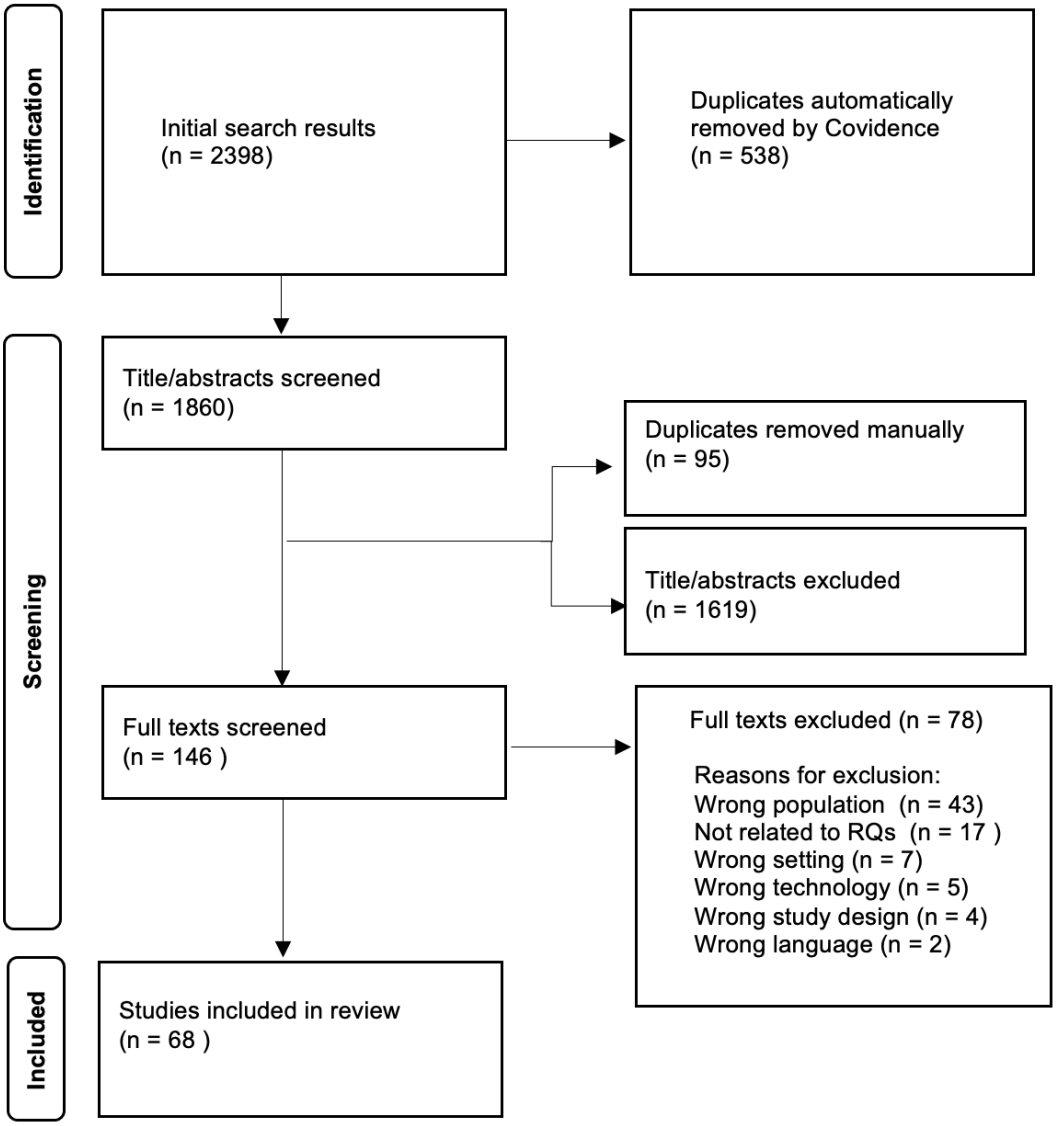

Figure 1: *PRISMA flow chart.*

Overall, we found perceptions of privacy, purpose, safety, and risk to be diverse. Our research questions resulted in a variety of SHT user concerns and perceived benefits related to privacy (sixty studies), purpose (twenty-two studies), risks and benefits (forty-three studies), and safety (twenty-five studies). A wide range of SHTs were evaluated by the extracted studies, with some focusing on more than one type of device. The most common SHTs analyzed throughout the selected studies were voice assistants (VAs) or smart speakers, environmental sensors, home automation tools, and other SHTs in general (smart thermostats, security cameras, or a mix of other SHTs) (see Appendix 1; see Figure 2 for the number of publications by year and Figure 3 for the number of studies by methodology).

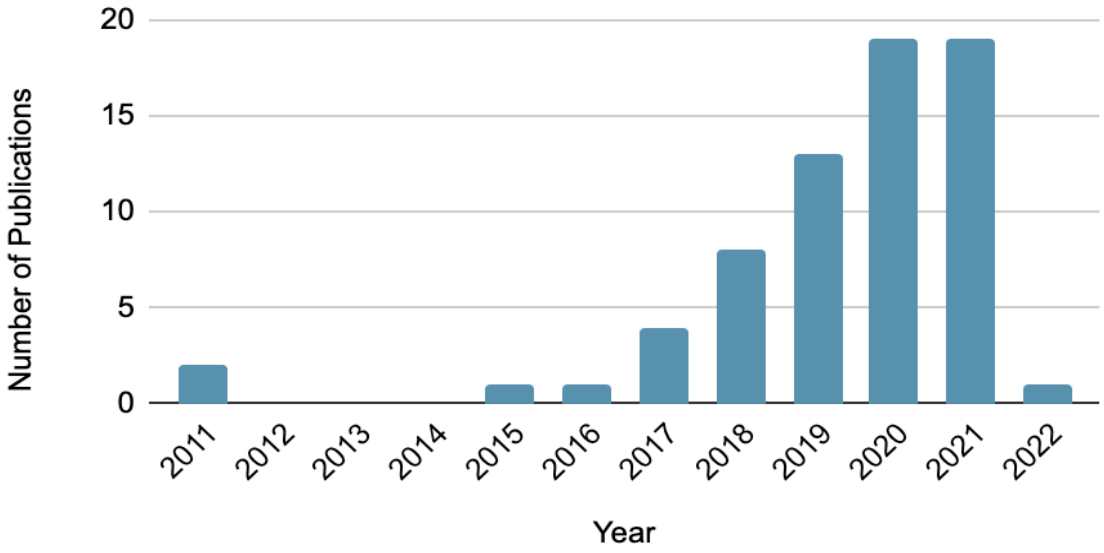

Figure 2: *Number of publications by year.*

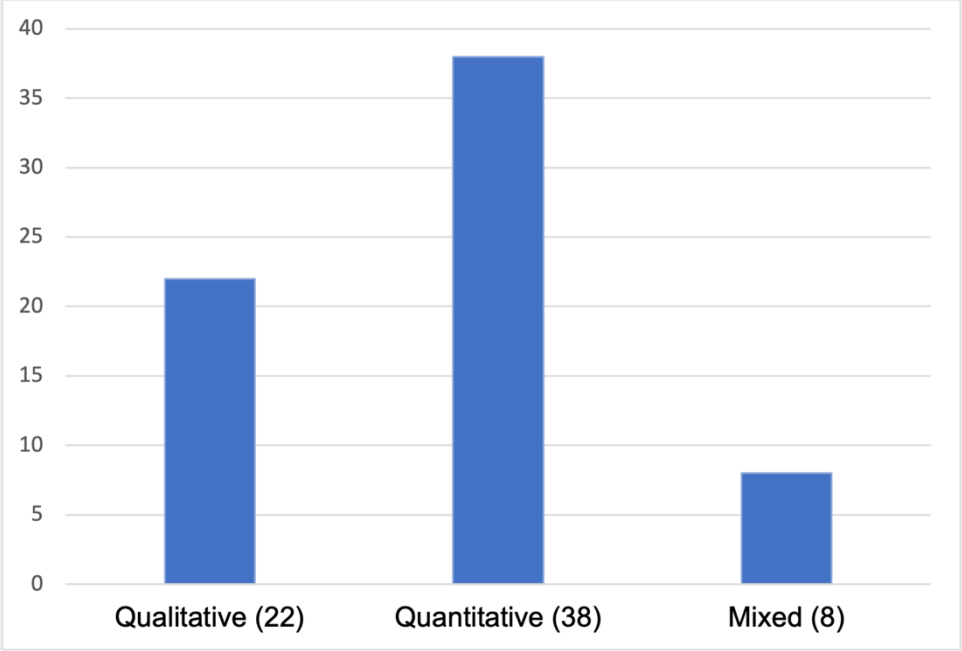

Figure 3: *Number of studies by methodology.*

Results

The following four sections are separated by theme: privacy, the purpose of data collection, risks and benefits, and safety. The findings in each section correspond to research questions linked to each theme. Each section begins with a summary of findings, which are then grouped into like categories and explained in further detail.

Theme 1: Privacy

Throughout our first theme, privacy, users' attitudes as well as interpretations of privacy itself were diverse. One interview study from the UK on telecare and smart home energy systems reported that participants thought privacy was essential, and "for some it meant that only they would have full access and control over what happened with the data" while others had more flexible interpretations (Burrows, Coyle, and Gooberman-Hill 2018: 116). Varied attitudes may stem from several factors. Studies that compared more than one geographic location tended to find culturally relevant variations in privacy attitudes (Pridmore et al. 2019; Tu et al. 2021). Age also appeared to be a relevant factor in privacy attitudes and levels of awareness, although the results were mixed. Some studies indicated that younger people were more privacy concerned than older people in terms of SHT or wearable data collection (Abaquita et al. 2020) and sensor based IoT devices (Psychoula et al. 2018). Others found that that privacy and security awareness declined slightly with age (Abrokwa et al. 2021). Conversely, some older people were least likely to trust in SHTs and had higher levels of concern over the impact of privacy breaches (Cannizzaro et al. 2019; Cannizzaro et al. 2020).

The following explores a few common topics that emerged under this theme, where study participants have often expressed concern or lack thereof. First, one common discussion relates to the difficulty in protecting SHT data from household members or visitors, potentially impacting household power dynamics (Furszyfer Del Rio, Sovacool, and Martiskainen 2021; Geeng and Roesner 2019; Huang, Obada-Obieh, and Beznosov 2020; Sovacool, Martiskainen, and Furszyfer Del Rio 2021). Other commonly explored topics included attitudes surrounding top-down surveillance from state actors (Furszyfer Del Rio, Sovacool, and Martiskainen 2021; Pridmore et al. 2019) and SHT manufacturers or third parties (Ammari et al. 2019; Furszyfer Del Rio, Sovacool, and Martiskainen 2021; Huang, Obada-Obieh, and Beznosov 2020), each of which is further explained below.

Household Power Dynamics

SHTs are often shared household devices that can involve data sharing between multiple users. Attitudes about shared SHT devices and their ability to influence household power dynamics differed among users to varying degrees. Semi-structured interviews with twenty-five American smart speaker users showed that shared devices resulted in behavioral self-management, such as avoiding sharing sensitive information to limit access from household members or visitors (Huang, Obada-Obieh, and Beznosov 2020). Interestingly, primary users—the main person who manages settings—and secondary users—such as a guest or housemate with limited account access—shared similar privacy concerns and mitigation strategies (Huang, Obada-Obieh, and Beznosov 2020). Another survey (n=214) found that privacy invasive tendencies of smart speakers, such as accidental voice recording, sometimes led to interpersonal conflict in the home (Benlian, Klumpe, and Hinz 2020). A national UK survey (n=1032) analyzed user perception of SHTs such as burglar alarms, energy meters, and smart speakers, among others. Here, women were more likely than men to report that the main purpose of SHTs was to "control family members" (Furszyfer Del Rio, Sovacool, and Martiskainen 2021: 7). In another study using the same dataset, one participant mentioned that couples may use such devices to "to spy on each other" (Sovacool, Martiskainen, and Furszyfer Del Rio 2021: 6).

In some cases, participants were unconcerned about data sharing between household members. Lutz and Newlands (2021) surveyed 367 participants in the UK where smart speaker users were least worried about household members accessing their data, as opposed to contractors or third-party app developers (Lutz and Newlands 2021). Semi structured interviews (n=18) in the US and Australia asked about concerns of sharing general SHTs with household members—such as smart thermostats, lights, outlets, locks, motion sensors, speakers, and cameras (Geeng and Roesner 2019). Couples were generally unperturbed regarding potential power imbalances between the household members who had installed SHTs and secondary users. The authors hypothesize that this lack of concern could be due to interview participants self-identifying as being in "stable, generally trusting relationships," or that they may have had "incorrect or incomplete mental

models" about what types of information can be inferred or made visible by SHT data (Geeng and Roesner 2019: 9). The potential for SHT data sharing with organizations, such as state or corporate data recipients, was further explored in several studies.

State Surveillance

In addition to the concerns about household or peer-to-peer surveillance noted above, top-down or institutional surveillance was also explored in examples of privacy concerns over the potential for state surveillance. In a study of American (n=65) and Dutch (n=36) smart speaker users, participants in the US focus groups sometimes expressed concerns over the threat of state surveillance. However, they were less concerned about data privacy than their Dutch counterparts (Pridmore et al. 2019). Other American smart speaker users showed some concerns over "external entities" accessing their data, such as state actors or device manufacturers (Huang, Obada-Obieh, and Beznosov 2020). In the UK, some users reported fears of devices listening to conversations, some mentioning the dangers of "Big Brother" spying on their behavior through Amazon Echo (Furszyfer Del Rio, Sovacool, and Martiskainen 2021).

Corporate Surveillance

Corporate surveillance and third-party data sharing are other frequently explored topics within the literature. Levels of user trust in SHT companies is an important factor due to the high levels of uncertainty surrounding data collection, use, and storage (Furszyfer Del Rio, Sovacool, and Martiskainen 2021; Vimalkumar et al. 2021). As one UK participant mentioned: "To date, it is not possible to know where the data is transmitted. Manufacturer's claims cannot be guaranteed" (qtd. in Furszyfer Del Rio, Sovacool, and Martiskainen 2021: 10). Regarding third-party data sharing, many users expressed discontent: "I do not like [my data] being sold, because you would wonder about how much personal information they have," said one respondent (qtd. in Huang, Obada-Obieh, and Beznosov 2020: 6). Manufacturers were seen as untrustworthy and non-transparent about data sharing (Huang, Obada-Obieh, and Beznosov 2020). Interestingly, six participants resorted to feelings of learned helplessness. As stated by one participant: "It (Google) has everything that [is] digitally mine. There is nothing I can do about it" (qtd. in Huang Obada-Obieh and Beznosov 2020: 8). Similar to findings from Richards (2019), where SHT users expressed a decline in privacy concerns over time, some eventually succumbed to the idea that "nothing" could be done to preserve their data (Huang, Obada-Obieh, and Beznosov 2020: 8). Although voice assistant users expressed privacy concerns over contractors and third-party data access, Lutz and Newlands (2021) found that such attitudes had limited influence over privacy-protecting behaviours among users.

Relatedly, US families (n=19 adults; n=24 children) rationalized the continued use of Amazon Echo despite privacy concerns, with some expressing that maintaining privacy was no longer feasible in present times (Belanger et al. 2021). In a study of 419 voice assistant users, convenience and personalized services were considered more important than privacy. This study also found that users did not mind receiving personalized shopping recommendations based on their data (Pal and Arpnikanondt 2021). Vimalkumar et al. (2021) demonstrated that tech-savvy university students in India (n=252) engaged in privacy calculus decisions, adopting voice assistant technology even when privacy concerns were present. However, those who considered these SHTs to be the most useful were also the least concerned with privacy. As meaningful decision-making and consent requires a certain level of privacy literacy, we now turn to explore the extent to which users understand the purposes of data collection.

Theme 2: Purpose of Data Collection

Users expressed a range of perspectives on why and how their data are collected. Overall, many users were often unaware of what data were being collected or why (Abdi, Ramokapane, and Such 2019; Al-Turkistani and AlSa'awi 2020). Conversely, others understood the basic purposes of data collection such as marketing (Abdi, Ramokapane, and Such 2019; Pridmore et al. 2019), product improvement and personalization in the case of commercial SHTs (Abaquita et al. 2020; Tabassum, Kosinski, and Lipford 2019), or health

monitoring in the case of environmental sensors for older adults (Jo, Ma, and Cha 2021). Even in such cohorts, users often felt SHTs (including speakers, lights, plugs, doorbells, thermostats, sensors, and others) were collecting more data than they should (Tabassum, Kosinski, and Lipford 2019).

Confusion over SHT Data Collection Practices

Why and how smart speakers collect data through voice assistants was difficult for users to understand, as they were often unaware that their voice interactions are recorded (Ammari et al. 2019; Javed, Sethi, and Jadoun 2019); where data were stored (Abdi, Ramokapane, and Such 2019; Al-Turkistani and AlSa'awi 2020; Javed, Sethi, and Jadoun 2019); or where to access privacy settings (Lin and Parkin 2020). A survey of American Amazon Alexa users (n=113) showed that only 36.28% knew their voice data interactions were recorded and stored. Only a small minority (16.8%) knew they could delete their recordings, some of which were accidentally recorded and sensitive in nature (Javed, Sethi, and Jadoun 2019). Overall, voice assistant users expressed the need for higher levels of transparency and consent over data collection, sharing, and storage (Lopatovska et al. 2019).

Other types of SHT users were often confused over the hidden surveillance capabilities of their devices. For example, users knew that their smart doorbells were recording video but were unaware that the associated smartphone apps were also tracking their location (Tabassum, Kosinski, and Lipford 2019). A UK study with six older adult participants found that users were forgetting why non-medical sensors had been installed in their homes (Ghorayeb, Comber, and Gooberman-Hill 2021). Others found that telecare and environmental sensors led to concerns over what types of data were shared and with whom (Burrows, Coyle, and Gooberman-Hill 2018). In the US, wireless sensor users expressed the desire to know more about data collection, use, and storage, citing concerns about abuse or non-consensual third-party sharing (Alaiad and Zhou 2017). Finally, in Germany, Denmark, and Norway, one study of 3,851 SHT users found that privacy attitudes were not a significant factor in adoption rates (Hubert et al. 2020). Citing the privacy paradox, authors speculate such user behavior may be "related to ignorance" on the part of the users, or potentially due to trust in SHT privacy enhancing innovation (Hubert et al. 2020: 1162).

Digital Literacy

Certain subsets of participants have shown higher levels of awareness about data collection and sharing practices than others, such as older adult study participants in South Korea who had their SHT data collection features explained by researchers in advance (Jo, Ma, and Cha 2021). Elsewhere, focus groups with Dutch and American participants were generally aware that Google Home products could be used for marketing or state surveillance purposes, but generally expressed attitudes of resignation through the sentiment that they had "nothing to hide," that user profiling was "inevitable," or that it was "just out of [their] control" (Pridmore et al. 2019: 129.). However, Dutch participants were more skeptical about third-party sharing and usage and were more concerned about user anonymity (Pridmore et al. 2019). Other users were aware of the potential data misuse but ignored the risks due to the ubiquity of online surveillance. For example, one US study of fourteen legally blind voice assistant users justified their usage of such technologies since their data were already at risk through other platforms such as Gmail or iCloud (Abdolrahmani et al. 2020)— another example of privacy cynicism. The next theme further explores user attitudes in terms of the potential risks and benefits of SHTs.

Theme 3: Risks and Benefits

In regards to perceived risks and social benefits, users reported concern over issues about security (Zhang and Liu 2021), such as the risk of getting hacked (Alaiad and Zhou 2017; Brush et al. 2011). Some users found great benefits in SHTs, such as convenience (Barbosa, Zhang, and Wang 2020; Tabassum et al. 2020) or safety (Brich et al. 2017), which are further explored in the next section. We also found examples of perceived trade-offs, where users reported weighing the risks of SHTs against potential benefits

(Abdolrahmani et al. 2020; Brush et al. 2011; Gazzawe and Lock 2018; Sovacool, Martiskainen, and Furszyfer Del Rio 2021).

Trade-offs: Affordability, Security, Convenience, and Autonomy

One study reported that privacy could be traded if the SHT was considered affordable (Barbosa, Zhang, and Wang 2020). The authors note that this idea of valuing low cost over privacy could be problematic, as devices are often given away for free during promotions (Barbosa, Zhang, and Wang 2020). In a study consisting of five-hundred SHT user reviews, 1,006 survey respondents, and eighteen interviews, users engaged in trade-offs such as cost-benefit analyses to assess SHT cost, functionality, and features (Dupuis and Ebenezer 2018). Comparably, in Germany, users generally perceived SHT cost as something to consider in balance with device performance and privacy, although privacy was considered the most important factor (Burbach et al. 2019). In earlier work, participants felt that SHTs were generally too expensive and that benefits may not outweigh the drawbacks (Brush et al. 2011). Overall, it appears that SHT affordability has remained a persistent factor in assessing overall risks and benefits.

Users of smart thermostats, cameras, voice assistants, and other connected appliances (n=18) reported that safety or security benefits outweighed the risk of lost data or low levels of transparency on behalf of manufacturers (Gazzawe and Lock 2018). Relatedly, in an early US and UK study on smart home automation, semi-structured interviews (n=31) demonstrated awareness that smart locks or cameras might not only increase home security but also amplify risk due to potential hacking (Brush et al. 2011). More recently, in the UK, a study of forty-three robotic assistant users, such as voice assistants or Roomba vacuum cleaners, found that privacy concerns were pressing, especially for those with vulnerable health issues (Urquhart, Reedman-Flint, and Leesakul 2019). Respondents to a UK survey expressed related concerns related to risks. Some of those living in social housing viewed SHTs as intrusive and thus not worth the risk to their personal autonomy out of fear of increasing reliance on "outside experts" (Sovacool, Martiskainen, and Furszyfer Del Rio 2021: 15). Worth noting is that their survey results found that demographics had a limited influence on perception based on income, age, or housing tenancy (Sovacool, Martiskainen, and Furszyfer Del Rio 2021). Finally, in one US study, health protection was important, although SHT users were worried about the implications of constant monitoring and the potential of being hacked (Alaiad and Zhou 2017).

Perceived convenience sometimes led to accepting SHT surveillance risks where, again, feelings of helplessness or powerlessness were a factor in such attitudes (Sovacool, Martiskainen, and Furszyfer Del Rio 2021). As stated by one participant: "Once I bought all these devices that was it. These functions come with these risks no matter what and I can't do anything about that" (qtd. in Sovacool, Martiskainen, and Furszyfer Del Rio 2021: 444). Likewise, Tasbassum et al. (2019) found that users expressed powerlessness over the trading of data for convenience. Elsewhere, safety benefits were weighed against potential risks such as a loss of autonomy. A focus group in Finland (n=8) found that older adults were concerned about a loss of autonomy with home monitoring technologies. At the same time, older participants expressed that safety was more important, especially for those experiencing memory issues (Leikas and Kulju 2018). Potential users and early adopters of SHTs involving sensors and home automation expressed similar concerns over a loss of autonomy (Wilson, Hargreaves, and Richard Hauxwell-Baldwin 2017). Alternatively, another UK study showed individuals with intellectual disabilities found that smart speakers increased their autonomy and agency levels, helping them to live more independently (Smith et al. 2020). In short, SHT users often weigh various risks and benefits against each other as trade-offs.

Theme 4: Safety

This final theme pertains to user feelings of how SHTs can impact home safety, such as protection from outside intruders through home security features or enhanced health-related safety such as fall detection or emergency contact services. Research in this area was largely focused on older adults (50+) (Albina and

Hernandez 2018; Arthanat, Chang, and Wilcox 2020; Jo, Ma, and Cha 2021; O'Brien et al. 2020; Sultan and Yusuf 2020) or health care patients such as stroke survivors (Olsson et al. 2018; Rogerson, Burr, and Tyson 2020). It appears that age and health status are salient factors in terms of positive SHT safety perceptions. However, study participants of all ages also tended to perceive SHTs as safety-enhancing (Kim and Yoon 2016; Gazzawe and Lock 2018; Shank et al. 2021). In one example, users and non-users in South Korea reported that SHTs such as automatic gas locking services or CCTV cameras could help make the home safer (Kim and Yoon 2016). However, there were also concerns over third-party access to recorded images. As a result, users often perceived trade-offs between privacy violations and usefulness (Kim and Yoon 2016). In another study, Master's students (n=18) felt that SHTs such as smartphone-controlled fire alarms, burglar alarms, and door access alarms helped to guarantee home safety (Gazzawe and Lock 2018).

Older Adults and Safety Perceptions

Through an analysis of 125 Amazon Echo smart speaker customer reviews, older adults and caregivers often praised safety-enhancing features, such as emergency contact skills (e.g., Ask My Buddy) that notify users' contacts in the case of a fall (O'Brien et al. 2020). Similarly, Ambient Assistive Technology (AAT) users in the Netherlands (n=12) found comfort in emergency contact functions in the event of a fall (Van Hoof et al. 2011). Interview data indicated that privacy was often seen as less important than safety for older participants. In some cases, AATs were considered to enhance privacy by allowing older adults to age in place, as opposed to living in a care home (Van Hoof et al. 2011). In the Philippines, Assistive Technology users over sixty years old (n=118) reported heightened perceptions of safety and security, despite privacy concerns relating to manufacturers or relatives accessing their data (Albina and Hernandez 2018). In the US, users (n=447) with a previous fall or injury tended to feel less safe in the home and were more willing to adopt SHTs for safety and independence (Arthanat, Chang, and Wilcox 2020). In South Korea, focus groups demonstrated that older adults were more concerned with enhanced safety than managing privacy (Jo, Ma, and Cha 2021). In this case, monitoring sensors were seen as unobtrusive and as helping to facilitate independent living. In Bahrain, surveys with users and non-users (n=112) revealed that security and safety were perceived as the most important SHT features (Sultan and Yusuf 2020).

Additionally, a study of nineteen stroke survivors reported that SHTs gave users a sense of physical security and peace of mind. Users were unconcerned about privacy, often forgetting about the sensors over time (Rogerson, Burr, and Tyson 2020). Another study on video recording and environmental and wearable sensors showed that older adults were most often concerned with the humans monitoring their health data. Here, participants expressed distrust in humans monitoring their data to respond quickly to emergencies (Ghorayeb, Comber, and Gooberman-Hill 2021). Overall, in regards to safety, it is clear that SHTs are perceived as valuable to many older adults and healthcare patients, alongside other populations.

Discussion

The results of this review were focused on users' varied and nuanced perceptions of privacy, purpose, risks and benefits, and safety as they relate to SHTs. While many users found SHTs beneficial for different reasons, including safety, improved health outcomes, convenience, and entertainment, privacy and other risk concerns were often present. Users are often faced with making personal decisions about trade-offs such as affordability over privacy, indicating that the comfort and use of SHTs is not contingent upon privacy access or a strong understanding of why and how data are collected and used. Further, the prevalence of uninformed users may contribute to misleading assumptions about user acceptance levels of SHT surveillance. Power dynamics are inextricably linked to these SHTs as they can be enabled or amplified, which requires further critical discussion.

Many of the issues with SHTs flagged in the surveillance literature were not necessarily reflected by participants in our review. For example, although some users mentioned the potential for SHT data to contribute toward targeted advertisements (e.g., Pridmore et al. 2019; Sovacool, Martiskainen, and

Furszyfer Del Rio 2021), users rarely provided detailed explanations of potential harm. In contrast, academic researchers have warned that user profiling can have detrimental or discriminatory effects on the life chances and choices of marginalized groups (e.g., Chu et al. 2022; Kuempel 2016; Lyon 2003). Additionally, as voice-enabled SHT devices are growing in popularity, voice data themselves are valuable to marketers (Turow 2021). Inferred health status and mood from online behaviour and other biometric markers can be valuable to advertisers too (Hunter and Merrill 2022; Kroger, Lutz, and Raschke 2019; Pasquale 2021; Yoo 2021). The ability of voice enabled devices to infer health status or mood, such as through the sound of a user's voice, was not mentioned in the reviewed articles. While patient data in healthcare settings are highly protected, health status inferred by online applications often is not. In the US, the popularity of commercial "MHealth" apps has already led to calls to amend The Health Insurance Portability and Accountability Act (HIPAA) to further protect user health data in such contexts (Fang 2019). It follows that commercial smart home devices used for healthcare purposes would face the same scrutiny. Moreover, insurance companies can use SHT data for personalized pricing and discounted rates for cooperative users, while those who forget to change their smoke alarm battery, delay home repairs, or watch excessive television could see higher premium rates (Maalsen and Sadowski 2019). Those who refuse to share SHT data may be excluded from receiving critical services, such as home insurance (Maalsen and Sadowski 2019). As further highlighted by Carver and Mackinnon (2020), SHTs or wearable data collection for insurance purposes can serve to further disadvantage low-income older adults with a propensity towards health issues. While implications for personalized insurance rates were not mentioned in our reviewed studies, it is another potential risk for users to consider.

As noted, several participants were concerned about government or "Big Brother" watching (e.g., Furszyfer Del Rio, Sovacool, and Martiskainen 2021). However, Carver and Mackinnon (2020: 218) echo Zuboff (2015) in arguing that decentralized surveillance mechanisms and their potential to "modify social relations and politics" are more pressing issues than government surveillance alone. Others have made similar observations about the ways that "Big Brother" may no longer be an adequate metaphor in describing today's surveillance environments (Lyon 2003; Monahan and Murakami Wood 2018). This is due to the merging of public and private data and the decentralized nature of data collection, sharing, and disclosure (see Deibert 2020). Notably, the potential for SHT data sharing with law enforcement was scarcely mentioned as a key concern in any of the user perception studies reviewed. However, journalists and academics have raised alarms about the recent partnerships between US law enforcement and commercial SHTs such as Amazon Ring doorbells (Guariglia and Maass 2021; Ng 2022). Such partnerships can lead to unwarranted access to private spaces by law enforcement (Murakami Wood and Steeves 2021). For these reasons, further research should examine the potential chilling effects that SHTs may have on users, as have already been explored in other online spaces (Büchi, Festic, and Latzer 2022).

Strengths and Limitations

To our knowledge, we are the first to evaluate SHT user perception under four categories: privacy, purpose, risks and benefits, and safety. Where previous review articles have tended to focus on rehabilitation or healthcare settings exclusively, we have also incorporated user perception of commercial SHT surveillance. To put various academic perspectives in conversation with each other, our review included references from interdisciplinary fields across social sciences, computer sciences, engineering, legal studies, and nursing. Due to the high number of articles reviewed in our study, we were unable to fully explore the nuance of perspectives based on demographic categories such as gender, age, income levels, or geographic locations and their respective regulatory regimes in depth. As our inclusion and exclusion criteria led us to reject studies that were focused on non-users alone, we may have missed important insights into why people do not adopt SHTs. Due to their ability to be worn outside the home, we excluded studies focused solely on wearables that may have enriched our findings. Only English publications were accepted, so relevant non-English papers may have been excluded. Finally, adding Google Scholar and ACM Digital Library to our list of databases may have resulted in relevant studies that were otherwise missed.

Conclusion: Key Considerations

Throughout our analysis of the sixty-eight selected studies, examples of uninformed users, trade-offs, and privacy cynicism emerged throughout. Each has been previously used to explain the gap between privacy preferences and actions in other areas (e.g., see Draper and Turow 2019; Hargittai and Marwick 2016; Lutz, Hoffmann, and Ranzini 2020). Uninformed users may be prevalent because SHT surveillance practices need higher levels of transparency (Pasquale 2015). In the case of voice assistants, privacy controls are often located on associated profiles and devices and not on the devices themselves, creating further difficulty for some users (Percy Campbell 2023). The following examples demonstrate the difficulty of making meaningful privacy decisions in the current SHT ecosystem. For example, Amazon had publicly denied that Alexa interactions were used for marketing purposes for years, a claim that has since been called into question by an audit conducted by computer scientists (Iqbal et al. 2022). In the case of third-party applications for Google and Amazon smart speakers, many are in violation of their host company's data collection standards, and others have no privacy policy at all (Iqbal et al. 2022). In some cases, the onus of responsibility is placed on users to decide to either use a service and give up their data to be used in ways outside of their control or to forgo using SHTs altogether. However, consistent with surveys on consumer behavior with online and offline retailers (Turow, Hennessy, and Draper 2015), even informed SHT users tend to give up their data in exchange for services, or convenience, even if they feel companies are collecting excessive information (Tabassum, Kosinski, and Lipford 2019).

Next, the trends toward perceived trade-offs and digital resignation may be directly related. Factors such as convenience are sometimes weighed against data protection, leading to resigned users (Abdolrahmani et al. 2020). According to Turow, Hennessy, and Draper (2015) many users who appear to be engaged in trade-offs may be digitally resigned, as the majority of US consumers are. Perhaps indicative of the current lack of sweeping consumer privacy protection in the US, the more people learn about the surveillance practices of the services and products they interact with, the more resigned they become (Turow, Hennessy, and Draper 2015). Outside of the US, SHT users may have access to higher data protection standards, such as the General Data Protection Regulation (GDPR) in the European Union (Pridmore and Mols 2020). At the same time, even under the GDPR, informed consent has proven difficult to obtain for some users, such as older adults (Zhu et al. 2021).

Finally, as has been shown in the results of this review, privacy is often seen as desirable yet incompatible with other SHT features, such as those relating to home security or physical safety. This type of thinking is dangerous as it creates a false trade-off between privacy and security (Solove 2008, 2011). SHTs that aim to secure the physical home from outside intrusion should also secure user data from external access, or at least provide users with meaningful and easily accessible choices. Further, the fact that affordability is sometimes weighed against privacy is concerning. If presented with meaningful choices, SHTs that are affordable, convenient, security-enhancing, and privacy-preserving may be the preferred option for many.

The purpose of our integrative literature review has been to explore SHT user perspectives on privacy, safety, the purpose of data collection, and risk. We noted examples of privacy cynicism as one potential reason for user discrepancy between preferences and action, in the sense that users often believe their data are already "out there" or out of their control and thus use SHTs despite concerns or risk awareness. We also see evidence of self-reported trade-offs—which may sometimes be outcomes of digital resignation (Draper and Turow 2019). However, meaningful trade-off decisions cannot be made when SHT users are not well informed about their devices' surveillance capabilities or implications. This suggests that all three explanations (uninformed users, perceived trade-offs, and privacy cynicism)—or even a combination of the three—are valid in terms of understanding the gap between SHT user privacy attitudes and behavior or the lack of privacy concern among some users. Even as SHTs continue to rise in popularity and contribute to perceptions of safety, it is important to avoid conflating adoption rates with full user acceptance of their surveillance capabilities (Cannizzaro et al. 2020; Pridmore and Mols 2020).

User education programs alongside higher standards of transparency, accountability, and stronger data protection regulation would be welcome improvements (Vimalkumar et al. 2021). Incorporating users at all levels of the design process, particularly older adults and persons with disabilities, could encourage equitable access to SHT settings and non-discriminatory outcomes of data usage and sharing (see Costanza-Chock 2020). Finally, stricter regulatory regimes could further limit the availability of user data for marketing, insurance, and non-consensual third-party access. Regulation underpinned by Taylor's (2017) conception of data justice, for example, could increase transparency and accountability for SHT manufacturers and partners while respecting privacy as a human right and advancing user autonomy while limiting the potential for future AI-based discrimination. Whether the current trend in SHT adoption rates will continue is yet to be seen; however, stronger levels of user data protection alongside respect for user consent and autonomy are required to limit the potential for individual and societal harm.

Appendix 1

Table 1: *Data extraction table, available at:*
https://borealisdata.ca/dataset.xhtml?persistentId=doi:10.5683/SP3/E4IT6O

References

Abaquita, Denielle, Paritosh Bahirat, Karla A. Badillo-Urquiola, and Pamela Wisniewski. 2020. Privacy Norms Within the Internet of Things Using Contextual Integrity. In *Companion of the 2020 ACM International Conference on Supporting Group Work, Sanibel Island, Florida, January 6–8,* 131–134. New York: Association for Computing Machinery.

Abdi, Noura, Kopo M. Ramokapane, and Jose M. Such. 2019. More Than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants. In *Proceedings of the Fifteenth Symposium on Usable Privacy and Security, Santa Clara, California, August 12–13*, 451–466. Berkeley, CA: USENIX Association.

Abdolrahmani, Ali, Kevin M. Storer, Antony Rishin Mukkath Roy, Ravi M. Kuber, and Stacy M. Branham. 2020. Blind Leading the Sighted: Drawing Design Insights from Blind Users Towards More Productivity-Oriented Voice Interfaces. *ACM Transactions on Accessible Computing* 12 (4): 1–35.

Abomhara, Mohamed, and Geir M. Køien. 2014. Security and Privacy in the Internet of Things: Current Status and Open Issues. In *2014 International Conference on Privacy and Security in Mobile Systems (PRISMS), Aalborg, Denmark, Mau 11–14,* 1–8. Los Alamitos, CA: Institute of Electrical and Electronics Engineers.

Abrokwa, Desiree, Shruti Das, Omer Akgul, and Michelle L. Mazurek. 2021. Comparing Security and Privacy Attitudes Among US Users of Different Smartphone and Smart-Speaker Platforms. In *Proceedings of the 17th Symposium on Usable Privacy and Security, Virtual, August 8–10,* 139–158. Berkeley, CA: USENIX Association.

Al-Turkistani, Hilalah F., and Nourah K. AlSa'awi. 2020. Poster: Combination of Blockchains to Secure Smart Home Internet of Things. In *First International Conference of Smart Systems and Emerging Technologies, Riyadh, Saudi Arabia, November 3–5,* 261–262. https://doi.org/10.1109/SMART-TECH49988.2020.00069.

Alaiad, Ahmad, and Lina Zhou. 2017. Patients' Adoption of WSN-Based Smart Home Healthcare Systems: An Integrated Model of Facilitators and Barriers. *IEEE Transactions on Professional Communication* 60 (1): 4–23.

Albina, Erlito M., and Alexander A. Hernandez. 2018. Assessment of the Elderly on Perceived Needs, Benefits and Barriers: Inputs for the Design of Intelligent Assistive Technology. In *Proceedings of the 16th International Conference on ICT and Knowledge Engineering, Bangkok, Thailand, November 21–23,* 1–10. Los Alamitos, CA: Institute of Electrical and Electronics Engineers.

Ammari, Tawfiq, Jofish Kaye, Janice Y. Tsai, and Frank Bentley. 2019. Music, Search, and IoT: How People (Really) Use Voice Assistants. *ACM Transactions on Computer-Human Interaction* 26 (3): 1–28.

Arthanat, Sajay, Hong Chang, and John Wilcox. 2020. Determinants of Information Communication and Smart Home Automation Technology Adoption for Aging-in-Place. *Journal of Enabling Technologies* 14 (2): 73–86.

Auxier, Brooke, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner. 2019. Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information. *Pew Research Center: Internet, Science & Tech*, November 15. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ [accessed September 3, 2022].

Barbosa, Natã M., Zhuohao Zhang, and Yang Wang. 2020. Do Privacy and Security Matter to Everyone? Quantifying and Clustering User-Centric Considerations About Smart Home Device Adoption. In *Proceedings of the Sixteenth Symposium on Usable Privacy and Security, Virtual, August 10–11,* 417–435. Berkeley, CA: USENIX Association.

Belanger, France, Jessica Resor, Robert E. Crossler, Travis A. Finch, and Katherine R. Allen. 2021. Smart Home Speakers and Family Information Disclosure Decisions. In *Proceedings of AMCIS 2021, Virtual, August 9–13*. https://aisel.aisnet.org/amcis2021/adv_info_systems_general_track/adv_info_systems_general_track/3.

Benlian, Alexander, Johannes Klumpe, and Oliver Hinz. 2020. Mitigating the Intrusive Effects of Smart Home Assistants by Using Anthropomorphic Design Features: A Multimethod Investigation. *Information Systems Journal* 30 (6): 1010–1042.

Bennett, Colin J., Kevin D. Haggerty, David Lyon, and Valerie Steeves, eds. 2014. *Transparent Lives: Surveillance in Canada.* Athabasca, CA: Athabasca University Press.

Berridge, Clara, and Terrie Fox Wetle. 2020. Why Older Adults and Their Children Disagree About in-home Surveillance Technology, Sensors, and Tracking. *The Gerontologist* 60 (5): 926–934.

Brich, Julia, Marcel Walch, Michael Rietzler, Michael Weber, and Florian Schaub. 2017. Exploring End User Programming Needs in Home Automation. *ACM Transactions on Computer-Human Interaction* 24 (2): 1–35.

Brush, Bernheim A.J., Bongshin Lee, Ratul Mahajan, Sharad Agarwal, Stefan Saroiu, and Colin Dixon. 2011. Home Automation in the Wild: Challenges and Opportunities. In *Proceedings of the 29th Annual CHI Conference on Human Factors in Computing Systems, Vancouver, Canada, May 7–12*, 2115–2124. New York: Association for Computing Machinery.

Büchi, Moritz, Noemi Festic, and Michael Latzer. 2022. The Chilling Effects of Digital Dataveillance: A Theoretical Model and an Empirical Research Agenda. *Big Data & Society* 9 (1): 1–14.

Burbach, Laura, Patrick Halbach, Nils Plettenberg, Johannes Nakayama, Martina Ziefle, and Andre Calero Valdez. 2019. "Hey, Siri," "Ok, Google," "Alexa." Acceptance-Relevant Factors of Virtual Voice-Assistants. In *Proceeedings of the IEEE International Professional Communication Conference, Aachen, Germany, July 23–26*, 101–111. New York: Institute of Electronics Engineers.

Burrows, Alison, David Coyle, and Rachael Gooberman-Hill. 2018. Privacy, Boundaries and Smart Homes for Health: An Ethnographic Study. *Health & Place* 50: 112–118.

Cannizzaro, Sara, Rob Procter, Sinong Ma, and Carsten Maple. 2019. Adoption and Acceptability of Smart Devices for the Home. In *Living in the Internet of Things, London, England, May 1–2,* 1-6. Stevenage, UK: Institution of Engineering and Technology.

———. 2020. Trust in the Smart Home: Findings from a Nationally Representative Survey in the UK. *PloS One* 15 (5): 1–30.

Carver, Lisa F., and Debra Mackinnon. 2020. Health Applications of Gerontechnology, Privacy, and Surveillance: A Scoping Review. *Surveillance & Society* 18 (2): 216–230.

Chan, Marie, Eric Campo, Daniel Estève, and Jean-Yves Fourniols. 2009. Smart Homes—Current Features and Future Perspectives. *Maturitas* 64 (2): 90–97.

Cho, Hichang. 2022. Privacy Helplessness on Social Media: Its Constituents, Antecedents and Consequences. *Internet Research* 32 (1): 150–171.

Choi, Hanbyul, Jonghwa Park, and Yoonhyuk Jung. 2018. The Role of Privacy Fatigue in Online Privacy Behavior. *Computers in Human Behavior* 81: 42–51.

Choukou, Mohamed-Amine, Taylor Shortly, Nicole Leclerc, Derek Freier, Genevieve Lessard, Louise Demers, and Claudine Auger. 2021. Evaluating the Acceptance of Ambient Assisted Living Technology (AALT) in Rehabilitation: A Scoping Review. *International Journal of Medical Informatics* 150: https://doi.org/10.1016/j.ijmedinf.2021.104461.

Chu, Charlene, H., Rune Nyrup, Kathleen Leslie, Jiamin Shi, Andria Bianchi, Alexandra Lyn, Molly McNicholl, Shehroz Khan, Samira Rahimi, Amanda Grenier. 2022. Digital Ageism: Challenges and Opportunities in Artificial Intelligence for Older Adults. *The Gerontologist* 62 (7): 947–955.

Copos, Bogdan, Karl Levitt, Matt Bishop, and Jeff Rowe. 2016. Is Anybody Home? Inferring Activity from Smart Home Network Traffic. In *2016 IEEE Security and Privacy Workshops (SPW), San Jose, California, May 23–25,* 245–251. New York: IEEE.

Costanza-Chock, Sasha. 2020. *Design Justice: Community-led Practices to Build the Worlds We Need*. Cambridge, MA: The MIT Press.

Deibert, Ronald J. 2020. *Reset: Reclaiming the Internet for Civil Society.* Toronto, CA: House of Anansi Press.

Demiris, George, and Brian K. Hensel. 2008. Technologies for an Aging Society: A Systematic Review of "Smart Home" Applications. *Yearbook of Medical Informatics* 17 (1): 33–40.

Dencik, Lina, and Jonathan Cable. 2017. The Advent of Surveillance Realism: Public Opinion and Activist Responses to the Snowden Leaks. *International Journal of Communication* 11 (2017): 763–781.

Dommeyer, Curt J., and Barbara L. Gross. 2003. What Consumers Know and What They Do: An Investigation of Consumer Knowledge, Awareness, and Use of Privacy Protection Strategies. *Journal of Interactive Marketing* 17 (2): 34–51.

Draper, Nora, A. 2017. From Privacy Pragmatist to Privacy Resigned: Challenging Narratives of Rational Choice in Digital Privacy Debates. *Policy & Internet* 9 (2): 232–251.

Draper, Nora A., and Joseph Turow. 2019. The Corporate Cultivation of Digital Resignation. *New Media & Society* 21 (8): 1824–1839.

Dupuis, Marc, and Mercy Ebenezer. 2018. Help Wanted: Consumer Privacy Behavior and Smart Home Internet of Things (IoT) Devices. In *Proceedings of the 19th Annual SIG Conference on Information Technology Education, Fort Lauderdale, Florida, October 3–6,* 117–122. New York: Association for Computing Machinery.

Eliot, David, and David Murakami Wood. 2022. Culling the FLoC: Market Forces, Regulatory Regimes and Google's (Mis)Steps on the Path away from Targeted Advertising. *Information Polity* 27 (2): 259–274.

Fang, Jianyan. 2019. Health Data at Your Fingertips: Federal Regulatory Proposals for Consumer-Generated Mobile Health Data. *Georgetown Law Technology Rev*iew 4: 125–180.

Fritz, Roschelle L., and Gordana Dermody. 2019. A Nurse-driven Method for Developing Artificial Intelligence in Smart Homes for Aging-in-place. *Nursing Outlook* 67 (2): 140–153.

Furszyfer Del Rio, Dylan D., Benjamin K. Sovacool, and Mari Martiskainen. 2021. Controllable, Frightening, or Fun? Exploring the Gendered Dynamics of Smart Home Technology Preferences in the United Kingdom. *Energy Research & Social Science* 77: https://doi.org/10.1016/j.erss.2021.102105.

Gazzawe, Foziah, and Russell Lock. 2018. Smart Home: Devices, Applications and Their Potential Benefits and Challenges. *Advances in Intelligent Systems and Computing* 858: 1086–1097.

Geeng, Christine, and Franziska Roesner. 2019. Who's In Control?: Interactions in Multi-User Smart Homes. In *CHI 2019: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, Glasgow, Scotland, May 4–9,* 1–13. New York: Association for Computing Machinery.

Ghorayeb, Abir, Rob Comber, and Rachael Gooberman-Hill. 2021. Older Adults' Perspectives of Smart Home Technology: Are We Developing the Technology That Older People Want? *International Journal of Human-Computer Studies* 147: https://doi.org/10.1016/j.ijhcs.2020.102571.

Gilliom, John, and Torin Monahan. 2012. *SuperVision: An Introduction to the Surveillance Society.* Chicago, IL: University of Chicago Press.

Guariglia, Matthew, and Dave Maass. 2021. LAPD Requested Ring Footage of Black Lives Matter Protests. *Electronic Frontier Foundation*, February 16. https://www.eff.org/deeplinks/2021/02/lapd-requested-ring-footage-black-lives-matter-protests [accessed September 5, 2022].

Guo, Eileen, and Abby Ohlheiser. 2022. Ring's New TV Show Is a Brilliant but Ominous Viral Marketing Ploy. *MIT Technology Review,* August 19. https://www.technologyreview.com/2022/08/19/1058259/ring-nation-new-tv-show-viral-marketing/ [accessed September 5, 2022].

Hargittai, Eszter, and Alice Marwick. 2016. "What Can I Really Do?" Explaining the Privacy Paradox with Online Apathy. *International Journal of Communication* 10: 3737–3757.

Hoffmann, Christian Pieter, Christoph Lutz, and Giulia Ranzini. 2016. Privacy Cynicism: A New Approach to the Privacy Paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 10 (4): https://doi.org/10.5817/CP2016-4-7.

Hoofnagle, Chris Jay, and Jennifer M. Urban. 2014. Alan Westin's Privacy Homo Economicus. *Wake Forest Law Rev*iew 49: 261–371.

Huang, Yue, Borke Obada-Obieh, and Konstantin (Kosta) Beznosov. 2020. Amazon Vs. My Brother: How Users of Shared Smart Speakers Perceive and Cope with Privacy Risks. In *Proceedings of the Conference on Human Factors in Computing Systems – Proceedings, Honolulu, Hawaii, April 25–30*, 1–13. New York: Association for Computing Machinery.

Hubert, Marco, Andrea Carugati, Christian Brock, and Børge Obel. 2020. Take It Personally – The Role of Consumers' Perceived Value of Personalization on Cross-Category Use in a Smart Home Ecosystem. In *Proceedings of the 53rd Hawaii International Conference on System Sciences, Maui, Hawaii, January 7–10,* 1155–1164. https://doi.org/10.24251/HICSS.2020.144.

Hunter, Tatum, and Jeremy B. Merrill. 2022. Health Apps Share Your Concerns with Advertisers. HIPAA Can't Stop It. *The Washington Post*, September 22. https://www.washingtonpost.com/technology/2022/09/22/health-apps-privacy/ [accessed September 22, 2022].

Iqbal, Umar, Pouneh Nikkhah Bahrami, Rahmadi Trimananda, Hao Cui, Alexander Gamero-Garrido, Daniel Dubois, David Choffnes, Athina Markopoulou, Franziska Roesner, and Zubair Shafiq. 2022. Your Echos Are Heard: Tracking, Profiling, and Ad Targeting in the Amazon Smart Speaker Ecosystem. ArXiv Preprint, April 22. https://doi.org/10.48550/ARXIV.2204.10920.

Javed, Yousra, Shashank Sethi, and Akshay Jadoun. 2019. Alexa's Voice Recording Behavior: A Survey of User Understanding and Awareness. In *Proceedings of the 14th International Conference on Availability, Reliability and Security, Canterbury, United Kingdom, August 26–29*, 1–10. New York: Association for Computing Machinery.

Jo, Tae Hee, Jae Hoon Ma, and Seung Hyun Cha. 2021. Elderly Perception on the Internet of Things-Based Integrated Smart-Home System. *Sensors* 21 (4): 1–29.

Kim, Dongyeon, Kyuhong Park, Yongjin Park, and Jae-Hyeon Ahn. 2019. Willingness to Provide Personal Information: Perspective of Privacy Calculus in Iot Services. *Computers in Human Behavior* 92: 273–281.

Kim, Sunwoo, and Jeonghyuk Yoon. 2016. An Exploratory Study on Consumer's Needs on Smart Home in Korea. In *Design, User Experience, and Usability: Technological Contexts* 9748: 337–345.

Kröger, Jacob Leon. 2018. Unexpected Inferences from Sensor Data: A Hidden Privacy Threat in the Internet of Things. In *Internet of Things: Information Processing in an Increasingly Connected World*, edited by Leon Strous and Vinton G. Cerf, 147–159. Cham, CH: Springer Nature.

Kröger, Jacob Leon, Otto Hans-Martin Lutz, and Philip Raschke. 2019. Privacy Implications of Voice and Speech Analysis–Information Disclosure by Inference. In *IFIP International Summer School on Privacy and Identity Management* 576: 242–258.

Kuempel, Ashley. 2016. The Invisible Middlemen: A Critique and Call for Reform of the Data Broker Industry. *Northwestern Journal of International Law & Business* 36: 207–234.

Lasquety-Reyes, Jeremiah. 2022. Number of Smart Homes Forecast in the World from 2017 to 2025. *Statista*, June 15. https://www.statista.com/forecasts/887613/number-of-smart-homes-in-the-smart-home-market-in-the-world [accessed September 1, 2022].

Lau, Josephine, Benjamin Zimmerman, and Florian Schaub. 2018. Alexa, Are You Listening? Privacy Perceptions, Concerns and Privacy-seeking Behaviors with Smart Speakers. In *Proceedings of the ACM on Human-Computer Interaction* 2: 1–31.

Leikas, Jaana, and Minna Kulju. 2018. Ethical Consideration of Home Monitoring Technology: A Qualitative Focus Group Study. *Gerontechnology* 17 (1): 38–47.

Lie, Mabel L. S., Stephen Lindsay, and Katie Brittain. 2016. Technology and Trust: Older People's Perspectives of a Home Monitoring System. *Ageing & Society* 36 (7): 1501–1525.

Lin, Vanessa Z, and Simon Parkin. 2020. Transferability of Privacy-Related Behaviours to Shared Smart Home Assistant Devices. In *Proceedings of the 2020 7th International Conference on Internet of Things: Systems, Management and Security, Paris, France, December 14–26,* 1–8. Los Alamitos, CA: Institute of Electrical and Electronics Engineers.

Lopatovska, Irene, Alice London Griffin, Kelsey Gallagher, Caitlin Ballingall, Clair Rock, and Mildred Velazquez. 2020. User Recommendations for Intelligent Personal Assistants. *Journal of Librarianship and Information Science* 52 (2): 577–591.

Lutz, Christoph, Christian Pieter Hoffmann, and Giulia Ranzini. 2020. Data Capitalism and the User: An Exploration of Privacy Cynicism in Germany. *New Media & Society* 22 (7): 1168–1187.

Lutz, Christoph, and Gemma Newlands. 2021. Privacy and Smart Speakers: A Multi-Dimensional Approach. *The Information Society* 37 (3): 147–162.

Lyon, David, ed. 2003. *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*. London: Routledge.

———. 2007. *Surveillance Studies: An Overview*. Oxford, UK: Polity Press.

———. 2018. *The Culture of Surveillance: Watching as a Way of Life*. New York: John Wiley & Sons.

Maalsen, Sophia, and Jathan Sadowski. 2019. The Smart Home on FIRE: Amplifying and Accelerating Domestic Surveillance. *Surveillance & Society* 17 (1/2): 118–124.

Mäkinen, Liisa Annukka. 2016. Surveillance On/Off: Examining Home Surveillance Systems from the User's Perspective. *Surveillance & Society* 14 (1): 59–77.

Malkin, Nathan, Joe Deatrick, Allen Tong, Primal Wijesekera, Serge Egelman, and David Wagner. Privacy Attitudes of Smart Speaker Users. 2019. *Proceedings on Privacy Enhancing Technologies* 2019 (4): 250–271.

Marikyan, Davit, Savvas Papagiannidis, and Eleftherios Alamanos. 2019. A Systematic Review of the Smart Home Literature: A User Perspective. *Technological Forecasting and Social Change* 138: 139–154.

Monahan, Torin, and David Murakami Wood, eds. 2018. *Surveillance Studies: A Reader.* Oxford, UK: Oxford University Press.

Mortenson, W. Ben, Andrew Sixsmith, and Ryan Woolrych. 2015. The Power(s) of Observation: Theoretical Perspectives on Surveillance Technologies and Older People. *Ageing & Society* 35 (3): 512–530.

Murakami Wood, David, and Valerie Steeves. 2021. Smart Surveillance. *Surveillance & Society* 19 (2): 150–153.

Neville, Stephen J. 2020. Eavesmining: A Critical Audit of the Amazon Echo and Alexa Conditions of Use. *Surveillance & Society* 18 (3): 343–356.

———. 2021. The Domestication of Privacy-invasive Technology on YouTube: Unboxing the Amazon Echo with the Online Warm Expert. *Convergence* 27 (5): 1288–1307.

Ng, Alfred. 2022. Amazon Gave Ring Videos to Police Without Owners' Permission. *Politico*, July 13. https://www.politico.com/news/2022/07/13/amazon-gave-ring-videos-to-police-without-owners-permission-00045513 [accessed September 1, 2022].

Nissenbaum, Helen. 2009. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Redwood City, CA: Stanford University Press.

Noble, Safiya Umoja. 2018. *Algorithms of Oppression*. New York: New York University Press.

O'Brien, Katherine, Anna Liggett, Vanessa Ramirez-Zohfeld, Priya Sunkara, and Lee A. Lindquist. 2020. Voice-Controlled Intelligent Personal Assistants to Support Aging in Place. *Journal of the American Geriatrics Society* 68 (1): 176–179.

O'Neil, Cathy. 2016. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York: Broadway Books.

Obar, Jonathan A., and Anne Oeldorf-Hirsch. 2020. The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services. *Information, Communication & Society* 23 (1): 128–147.

Olsson, Anna, Ann-Christine Persson, Aniko Bartfai, and Inga-Lill Boman. 2018. Sensor Technology More Than a Support. *Scandinavian Journal of Occupational Therapy* 25 (2): 79–87.

Paetz, Alexandra-Gwyn, Birger Becker, Wolf Fichtner, and Hartmut Schmeck. 2011. Shifting Electricity Demand with Smart Home Technologies–an Experimental Study on User Acceptance. In *30th USAEE/IAEE North American Conference Online Proceedings, Washington, DC, October 9–12*, 1–19. https://www.scirp.org/reference/referencespapers?referenceid=912715.

Pal, Debajyoti, and Chonlameth Arpnikanondt. 2021. An Integrated TAM/ISS Model Based PLS-SEM Approach for Evaluating the Continuous Usage of Voice Enabled IoT Systems. *Wireless Personal Communications* 119 (2): 1065–1092.

Park, Kyuhong, Yong Jin Park, Junyeong Lee, Jae-Hyeon Ahn, and Dongyeon Kim. 2022. Alexa, Tell Me More! The Effectiveness of Advertisements through Smart Speakers. *International Journal of Electronic Commerce* 26 (1): 3–24.

Park, Yong Jin. 2013. Digital Literacy and Privacy Behavior Online. *Communication Research* 40 (2): 215–236.

Parkin, Simon, Trupti Patel, Isabel Lopez-Neira, and Leonie Tanczer. 2019. Usability Analysis of Shared Device Ecosystem Security: Informing Support for Survivors of IoT-facilitated Tech-abuse. In *Proceedings of the New Security Paradigms Workshop, San Carlos, Costa Rica, September 23–26*: 1–15. https://doi.org/10.1145/3368860.3368861.

Parzen, Maurine, Sheila O'Keefe-McCarthy, Jenn Salfi, and Karyn Taplay. 2021. Perceptions of Informal Caregivers Use of Smart Technology in Caring for an Older Adult. *Journal of Nursing and Occupational Health* 3 (1): 230–239.

Pasquale, Frank. 2015. *The Secret Algorithms that Control the Economy and Information*. Cambridge, MA: Harvard University Press.

———. 2021 Promoting Data for Well-Being While Minimizing Stigma. In *Regulating Big Tech*, edited by Martin Moore and Damian Tambini, 180–192. Oxford, UK: Oxford University Press.

Percy Campbell, Jessica. 2023. *Aging in Place with Google and Amazon Smart Speakers: Privacy and Surveillance Implications for Older Adults*. PhD Dissertation, The University of Victoria.

Pirzada, Pireh, Adriana Wilde, Gayle Helane Doherty, and David Harris-Birtill. 2022. Ethics and Acceptance of Smart Homes for Older Adults. *Informatics for Health and Social Care* 47 (1): 10–37.

Pitardi, Valentina, and Hannah R. Marriott. 2021. Alexa, She's Not Human but… Unveiling the Drivers of Consumers' Trust in Voice-Based Artificial Intelligence. *Psychology & Marketing* 38 (4): 626–642.

Pridmore, Jason, Anouk Mols. 2020. Personal Choices and Situated Data: Privacy Negotiations and the Acceptance of Household Intelligent Personal Assistants. *Big Data & Society* 7 (1): 1–13.

Pridmore, Jason, Michael Zimmer, Jessica Vitak, Anouk Mols, Daniel Trottier, Priya C. Kumar, and Yuting Liao. 2019. Intelligent Personal Assistants and the Intercultural Negotiations of Dataveillance in Platformed Households. *Surveillance & Society* 17 (1/2): 125–131.

Psychoula, Ismini, Deepika Singh, Liming Chen, Feng Chen, Andreas Holzinger, and Huansheng Ning. 2018. Users' Privacy Concerns in IoT Based Applications. In *2018 IEEE Smartworld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation, Guangzhou, China, October 8–12*, 1887–1894. Los Alamitos, CA: Institute of Electrical and Electronics Engineers.

Rajapaksha, Subhash, Shivam Thakrar, Matt Kinzler, Haochen Sun, Justin Smith, and Debbie Perouli. 2021. Field Study on Usability and Security Perceptions Surrounding Social Robots. In *2021 IEEE 45th Annual Computers, Software, and Applications Conference, Madrid, Spain, July 12–16,* 1593–1598. Los Alamitos, CA: Institute of Electrical and Electronics Engineers.

Read, Emily, Cora Woolsey, Lorie Donelle, Lori Weeks, and Norma Chinho. 2022. Passive Remote Monitoring and Aging in Place: A Scoping Review. *Canadian Journal on Aging/La Revue Canadienne du Vieillissement* 42 (1): 20–32.

Richards, Olivia K. 2019. Family-Centered Exploration of the Benefits and Burdens of Digital Home Assistants. In *CHI EA '19 Extended Abstracts: Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems, Glasgow Scotland, May 4–9,* 1–6. New York: Association for Computing Machinery.

Rogerson, Louise, Jonathan Burr, and Sarah Tyson. 2020. The Feasibility and Acceptability of Smart Home Technology Using the Howz System for People with Stroke. *Disability and Rehabilitation: Assistive Technology* 15 (2): 148–152.

Sadowski, Jathan. 2020. *Too Smart: How Digital Capitalism is Extracting Data, Controlling our Lives, and Taking Over the World*. Cambridge, MA: MIT Press.

Shank, Daniel B., David Wright, Rohan Lulham, and Clementine Thurgood. 2021. Knowledge, Perceived Benefits, Adoption, and Use of Smart Home Products. *International Journal of Human-Computer Interaction* 37 (10): 922–937.

Smith, Elizabeth, Petroc Sumner, Craig Hedge, and Georgina Powell. 2020. Smart-Speaker Technology and Intellectual Disabilities: Agency and Wellbeing. *Disability and Rehabilitation: Assistive Technology* 18 (4): 432–442.

Solove, Daniel J. 2008. I've Got Nothing to Hide and Other Misunderstandings of Privacy. *San Diego Law Review* 44: 745–772.

———. 2011. *Nothing to Hide: The False Tradeoff between Privacy and Security*. New Haven, CT: Yale University Press.

Sovacool, Benjamin K., Mari Martiskainen, and Dylan D. Furszyfer Del Rio. 2021. Knowledge, Energy Sustainability, and Vulnerability in the Demographics of Smart Home Technology Diffusion. *Energy Policy* 153: https://doi.org/10.1016/j.enpol.2021.112196.

Statistics Canada. 2022. Canadian Internet Use Survey, 2022. https://www150.statcan.gc.ca/n1/daily-quotidien/230720/dq230720b-eng.htm [accessed August 1, 2023].

Sultan, Reem, and Ammar Yusuf. 2020. Smart Homes: End Users' Perception - Case of Bahrain. In *Proceedings of the 3rd Smart Cities Symposium, virtual, September 21–23,* 663–667. https://doi.org/10.1049/icp.2021.0936.

Tabassum, Madiha, Jess Kropczynski, Pamela Wisniewski, and Heather Richter Lipford. 2020. Smart Home Beyond the Home: A Case for Community-Based Access Control. In *Proceedings of the Conference on Human Factors in Computing Systems, Honolulu, Hawaii, April 25–30*, 1–12. New York: Association for Computing Machinery.

Tabassum, Madiha, Tomasz Kosiński, and Heather Richter Lipford. 2019. "I Don't Own the Data": End User Perceptions of Smart Home Device Data Practices and Risks. In *Proceedings of the 15th Symposium on Usable Privacy and Security, Santa Clara, California, August 12–13,* 435–450. Berkeley, CA: USENIX Association.

Taylor, Linnet. 2017. What Is Data Justice? The Case for Connecting Digital Rights and Freedoms Globally. *Big Data & Society* 4 (2): https://doi.org/10.1177/2053951717736335.

Thormundsson, Bergur. 2023. Smart Home Device u.s. Household Penetration Rate 2023. 2023. Statista. https://www.statista.com/statistics/1247351/smart-home-device-us-household-penetration/ [accessed August 1, 2023].

Troullinou, Pinelopi. 2017. *Exploring the Subjective Experience of Everyday Surveillance: The Case of Smartphone Devices as Means of Facilitating Seductive Surveillance*. PhD dissertation, The Open University.

Tu, Gengyang, Corinne Faure, Joachim Schleich, and Marie-Charlotte Guetlein. 2021. The Heat Is Off! The Role of Technology Attributes and Individual Attitudes in the Diffusion of Smart Thermostats: Findings from a Multi-Country Survey. *Technological Forecasting & Social Change* 163: https://doi.org/10.1016/j.techfore.2020.120508.

Turow, Joseph. 2021. *The Voice Catchers: How Marketers Listen in to Exploit Your Feelings, Your Privacy, and Your Wallet*. New Haven, CT: Yale University Press.

Turow, Joseph, Michael Hennessy, and Nora Draper. 2015. The Trade-off Fallacy: How Marketers are Misrepresenting American Consumers and Opening Them up to Exploitation. SSRN, August 10. https://dx.doi.org/10.2139/ssrn.2820060.

Urquhart, Lachlan, Dominic Reedman-Flint, and Natalie Leesakul. 2019. Responsible Domestic Robotics: Exploring Ethical Implications of Robots in the Home. *Journal of Information, Communication and Ethics in Society* 17 (2): 246–272.

Van Hoof, J, Helianthe S.M Kort, P.G.S Rutten, and M.S.H Duijnstee. 2011. Ageing-in-Place with the Use of Ambient Intelligence Technology: Perspectives of Older Users. *International Journal of Medical Informatics* 80 (5): 310–331.

Vimalkumar, M., Sujeet Kumar Sharma, Jang Bahadur Singh, and Yogesh K. Dwivedi. 2021. "Okay Google, What About My Privacy?": User's Privacy Perceptions and Acceptance of Voice Based Digital Assistants. *Computers in Human Behavior* 120: https://doi.org/10.1016/j.chb.2021.106763.

Westin, Alan F. 1967. *Privacy and Freedom*. New York: Atheneum Press.

———. 2003. Social and Political Dimensions of Privacy. *Journal of Social Issues* 59 (2): 431–453.

Wilson, Charlie, Tom Hargreaves, and Richard Hauxwell-Baldwin. 2017. Benefits and Risks of Smart Home Technologies. *Energy Policy* 103: 72–83.

Whittemore, Robin, and Kathleen Knafl. 2005. The Integrative Review: Updated Methodology. *Journal of Advanced Nursing* 52 (5): 546–553.

Wright, David, and Charles D. Raab. 2012. Constructing a Surveillance Impact Assessment. *Computer Law & Security Review* 28 (6): 613–626.

Yang, Heetae, Hwansoo Lee, and Hangjung Zo. 2017. User Acceptance of Smart Home Services: An Extension of the Theory of Planned Behavior. *Industrial Management & Data Systems* 117 (1): 68–89.

Yoo, Noah. 2021. New Spotify Patent Involves Monitoring Users' Speech to Recommend Music. *Pitchfork*, January 28. https://pitchfork.com/news/new-spotify-patent-involves-monitoring-users-speech-to-recommend-music/?mbid=social_twitter&utm_social-type=owned&utm_brand=p4k&utm_source=twitter&utm_medium=social [accessed September 1, 2022].

Zeng, Eric, Shrirang Mare, and Franziska Roesner. 2017. End User Security and Privacy Concerns with Smart Homes. In *Proceedings of the Thirteenth Symposium on Usable Privacy and Security, Santa Clara, California, July 12–14*, 65–80. Berkeley, CA: USENIX Association.

Zhang, Nan, Xianghang Mi, Xuan Feng, XiaoFeng Wang, Yuan Tian, and Feng Qian. 2018. Understanding and Mitigating the Security Risks of Voice-Controlled Third-Party Skills on Amazon Alexa and Google Home. ArXiv Preprint, May 3. https://doi.org/10.48550/arXiv.1805.01525.

Zhang, Wenqing, and Liangliang Liu. 2021. Unearthing Consumers' Intention to Adopt Eco-Friendly Smart Home Services: An Extended Version of the Theory of Planned Behavior Model. *Journal of Environmental Planning and Management* 65 (2): 216–239.

Zheng, Serena, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. User Perceptions of Smart Home IoT Privacy. *Proceedings of the ACM on Human-computer Interaction* 2 (CSCW): https://doi.org/10.1145/3274469.

Zhu, Junhong, Kaiyuan Shi, Chengyue Yang, Yanping Niu, Yingchun Zeng, Ning Zhang, Tao Liu, and Charlene H. Chu. 2021. Ethical Issues of Smart Home-based Elderly Care: A Scoping Review. *Journal of Nursing Management* 30 (8): 3686–3699.

Zuboff, Shoshana. 2015. Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology* 30 (1): 75–89.

———. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. London: Profile Books.