PDF Download
3731755.pdf
02 February 2026
Total Citations: 2
Total Downloads:
1969

RESEARCH-ARTICLE

Bystander Privacy in Smart Homes: A Systematic Review of Concerns and Solutions

EIMAAN SAQIB, University of Waterloo, Waterloo, ON, Canada

SHIJING HE, King's College London, London, U.K.

JUNGHYUN CHOY, International Computer Science Institute, Berkeley, CA, United States

RUBA ABU-SALMA, King's College London, London, U.K.

JOSE MIGUEL SUCH, Polytechnic University of Valencia, Valencia, Valencia, Spain

JULIA BERND, International Computer Science Institute, Berkeley, CA, United States

View all

Open Access Support provided by:

International Computer Science Institute

University of Waterloo

King's College London

Polytechnic University of Valencia

Published: 15 October 2025
Online AM: 08 May 2025
Accepted: 14 March 2025
Revised: 06 March 2025
Received: 15 May 2024

Citation in BibTeX format

ACM Transactions on Computer-Human Interaction, Volume 32, Issue 5 (October 2025)
https://doi.org/10.1145/3731755
EISSN: 1557-7325

Bystander Privacy in Smart Homes: A Systematic Review of Concerns and Solutions

EIMAAN SAQIB, Lahore University of Management Sciences (LUMS), Lahore, Pakistan and University of Waterloo, Waterloo, Ontario, Canada
SHIJING HE, King's College London (KCL), London, UK
JUNGHYUN CHOY, International Computer Science Institute (ICSI), Berkeley, California, USA
RUBA ABU-SALMA, King's College London (KCL), London, UK
JOSE SUCH, King's College London (KCL), London, UK and Universitat Politècnica de València (UPV), València, Spain
JULIA BERND, International Computer Science Institute (ICSI), Berkeley, California, USA
MOBIN JAVED, Lahore University of Management Sciences (LUMS), Lahore, Pakistan and International Computer Science Institute (ICSI), Berkeley, California, USA

Smart home devices, such as security cameras and voice assistants, have seen widespread adoption due to the utility and convenience they offer to users. The deployment of these devices in homes, however, raises privacy concerns for bystanders—people who may not necessarily have a say in the deployment and configuration of these devices, and yet are exposed to or affected by their data collection. Examples of bystanders include guests, short-term tenants, and domestic workers. Prior work has studied the privacy concerns of different bystander groups and proposed design solutions for addressing these concerns. In this article, we present a systematic review of previous studies, describing how smart home bystanders are defined and classified, and illuminating the range of concerns and solutions proposed in the existing academic literature. We also discuss limitations in prior work, barriers to the uptake of research-based solutions by industry, and identify avenues for future research.

CCS Concepts: • **Security and privacy → Privacy protections**; **Human and societal aspects of security and privacy**; **Usability in security and privacy**;

Additional Key Words and Phrases: Internet of Things (IoT), smart homes, multi-user smart homes, bystanders, privacy

This work was supported in part by the U.S. National Science Foundation (award CNS-2114229), a King's-China Scholarship Council (K-CSC) PhD Scholarship, and the INCIBE's strategic SPRINT C063/23 project with funds from the EU-NextGenerationEU through the Spanish government's Plan de Recuperación, Transformación y Resiliencia.
Authors' Contact Information: Eimaan Saqib, Lahore University of Management Sciences (LUMS), Lahore, Pakistan and University of Waterloo, Waterloo, Ontario, Canada; e-mail: e2saqib@uwaterloo.ca; Shijing He, King's College London (KCL), London, UK; e-mail: shijing.he@kcl.ac.uk; Junghyun Choy, International Computer Science Institute (ICSI), Berkeley, California, USA; e-mail: jchoy@alumni.cmu.edu; Ruba Abu-Salma, King's College London (KCL), London, UK; e-mail: ruba.abu-salma@kcl.ac.uk; Jose Such, King's College London (KCL), London, UK and Universitat Politècnica de València (UPV), València, Spain; e-mail: jose.such@kcl.ac.uk; Julia Bernd, International Computer Science Institute (ICSI), Berkeley, California, USA; e-mail: jbernd@icsi.berkeley.edu; Mobin Javed (corresponding author), Lahore University of Management Sciences (LUMS), Lahore, Pakistan and International Computer Science Institute (ICSI), Berkeley, California, USA; e-mail: mobin.javed@lums.edu.pk.

ACM 1557-7325/2025/10-ART43
https://doi.org/10.1145/3731755

ACM Reference format:
Eimaan Saqib, Shijing He, Junghyun Choy, Ruba Abu-Salma, Jose Such, Julia Bernd, and Mobin Javed. 2025. Bystander Privacy in Smart Homes: A Systematic Review of Concerns and Solutions. *ACM Trans. Comput.-Hum. Interact.* 32, 5, Article 43 (October 2025), 43 pages.
https://doi.org/10.1145/3731755

1 Introduction

Smart home devices like security cameras, smart speakers, and hubs have gained widespread adoption due to the utility and convenience they offer. These devices are deployed in a variety of contexts—for example, to monitor babies, domestic workers, and visitors at the door; to play music in shared spaces with roommates; and to provide care for the elderly [5, 8, 28, 29, 55, 64, 67, 124, 143]. To provide utility, these devices collect extensive data and often continuously monitor the smart home environment in which they are deployed.

This data collection not only affects the users who choose to deploy the devices, but also other members of and visitors to the household, also known as *bystanders*, who may not have a say in device deployment and configuration. For example, a baby monitor camera may raise privacy concerns about constant surveillance and potential micromanagement for nannies [28]. These privacy concerns may further be aggravated in certain cultures and contexts, such as where a domestic worker observes Hijab, or is constrained from advocating for themself because their immigration status depends on their employer [5, 8, 67, 124].

The presence of bystanders thus complicates any efforts to design for privacy in smart homes. To begin with, designing for bystander privacy requires a systematic understanding of who may become a bystander in a smart home. Prior research has identified various smart home stakeholders that could be considered *bystanders* (whether or not the authors used that term). Visitors are obvious bystanders [12, 39, 85, 87, 89, 93, 132]. However, even household members in a smart home may have a variety of relationships and power differentials with the device owner, and may find themselves in the position of bystanders to the devices in their homes if they lack agency over deployment and configuration of those devices. Examples studied in the literature include roommates who do not have access to device controls [56], or teenagers whose parents track their activities via smart door locks [133].

Existing work on smart home bystanders has identified a range of privacy concerns and perspectives. Frequently, such work proposes design recommendations to address those concerns, and a number of studies have explored potential solutions. Implementation poses challenges and requires accommodating multiple stakeholders, since bystander privacy often conflicts with the utility a smart home device offers its owner. For instance, a bystander might prefer automatic data deletion after a short period, while owners may find this inconvenient as they may lose access to their own collected data after a specific time period. These tradeoffs may have different implications across cultures and usage contexts, making generalization challenging. Additionally, different types of bystanders may have diverse needs, adding further complexity.

To develop an understanding of the research-to-date on bystander privacy in smart homes, we conduct a systematic review of existing literature, focusing on the following **research questions (RQs)**:

- *RQ1*. How has the existing academic literature defined and classified smart home bystanders?
- *RQ2*. What privacy concerns have been identified amongst people in the role of smart home bystanders, and what factors influence variation?

— *RQ3*. What design solutions have been proposed in the existing academic literature to assist smart home bystanders in protecting or advocating for their privacy and exercising their agency?
— *RQ4*. What are the limitations of prior studies? What gaps in the literature need to be filled in future work?

Our work makes the following contributions:

— Scoping the category *bystander* in terms of the roles someone can play relative to a device and introducing a framework to categorize bystander groups based on their relationship with the smart home device owner.
— Classifying the privacy concerns presented by existing studies, and extracting influencing factors (such as power dynamics, trust, and regulations) that affect the severity of these concerns.
— Systematizing the design solutions and recommendations proposed to address bystander privacy concerns, highlighting their limitations and privacy-utility tradeoffs, as well as discussing the current state of the art in smart home products.
— Highlighting gaps in the literature and identifying avenues for future research.

Our work aims to help bridge the gap between academic research and industry practice by systematizing knowledge about the variety and severity of privacy challenges faced by various kinds of bystander groups, evaluating what kinds of privacy designs for bystanders are most likely to be feasible and desirable, and identifying what RQs still need answering to enable industrial implementation of smart home privacy solutions for bystanders.

2 Related Work

Prior literature reviews on smart home technology have examined accumulated research on adoption processes and associated design challenges, both for smart homes in general [78, 79, 115], and for specific device types such as security systems [41], home health monitoring systems [18, 97, 101, 102, 104], and energy management systems [147]. Specifically, some reviews have highlighted the necessity of a user-centric perspective in smart home technology design [69, 83, 140, 141]; however, the reviewed literature generally focuses on device owners and primary users, and does not include other stakeholders.

In some cases, these reviews include papers that cover privacy aspects, for example, as a challenge in smart TV adoption [3], or as an ethical concern [46, 120]. The narrative review of Meng-Schneider et al. [94] explores concerns expressed by primary, secondary, and incidental users of smart speakers. Though that review did not cover a full range of devices, the prominence of privacy concerns (amongst other concerns) demonstrates the importance of the topic, and of examining differences in perceptions of varying stakeholders in smart homes.

Other smart home literature reviews have been more focused on privacy and security, for example, the security and privacy of smart home personal assistants [9, 45] and smart locks [62], and a systematization of work on security threats and harms, including privacy harms [32]. Maccario and Naldi [82] review literature on privacy concerns in smart speakers, identifying trends in topics and regions of study. Reviews have covered privacy designs in smart home Wi-Fi networks [4], protections for smart home data [35], and attitudes toward smart home data collection [103]. Lipford et al. [80] offer a general overview of the state of smart home privacy research. However, again, these reviews focused on the privacy of the owner or primary user.

Some reviews have looked at multi-user smart homes; for example, Mohammad et al. [95] evaluated access control schemes and highlighted overlooked challenges (e.g., scalability, latency).

Pattnaik et al. [100] conducted a systematic review focusing on primary users' perspectives on smart home security and privacy; it also briefly reviewed literature pertaining to viewpoints of multiple users, such as bystander privacy and access control, but it did not undertake a comprehensive synthesis of ramifications for bystanders nor their implications for design. Similarly, Prange and Alt [108] discuss contextual factors in smart home privacy design, including relationships, but do not go into depth on factors for non–primary users. Several overviews have examined the specific situation of abuse or surveillance of intimate partners or family members, in which the authors consider smart home-facilitated abuse as one aspect among several [109, 116], or in a few cases specifically focusing on it [10, 91].

In sum, while prior reviews have addressed aspects of smart home devices, including privacy, none have focused specifically on synthesizing the various bystander groups, their concerns, and the solutions proposed in the literature. Our work aims to address this gap with a systematic review centered on privacy concerns affecting *bystanders* in various smart home contexts, and focusing on proposed solutions to address these concerns.

3 Methods and Dataset

In two rounds of searches, we gathered, reviewed, and systematized papers published up to and including 31 August 2024.

3.1 Literature Search

We followed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses guidelines for systematic reviews [96].

Round 1. The first three authors conducted an initial search across three databases: (1) ACM Digital Library, (2) IEEE Xplore Digital Library, and (3) DBLP Computer Science Bibliography, considering papers published up to and including 1 August 2023. We began with three core keywords: "`smart home*`" AND "`bystander*`" AND "`privacy.`" Three of the researchers then divided up and read through the titles and abstracts of an initial set of 76 papers, and discarded any that clearly did not explore bystander privacy in a smart home context, resulting in a set of 21 relevant papers. We used the role-based definition of smart home bystander mentioned in Section 4.1 to determine inclusion, regardless of whether the paper itself used the term "bystander."

We then iteratively performed backward and forward reference search on the 21 resulting papers, identifying additional papers relevant to our RQs that were cited by those 21 papers, as well as newer papers citing them in turn. This process allowed us to capture any papers we missed in our keyword searches. The papers that resulted from this process were read in detail by the three researchers to identify alternative terms or keywords used in the academic literature and relevant to our study scope, which resulted in expanding our keyword set to include additional keywords, such as "incidental user(s)" and "passenger user(s)."

We repeated the process again with the new keyword set: ("`smart home*`" OR "`multi-user smart home*`" OR "`smart home device*`" OR "`shared smart device*`" OR "`Internet of Things`" OR "`IoT`") AND "`privacy`" AND ("`bystander*`" OR "`visitor*`" OR "`incidental user*`" OR "`passenger user*`"). The search across the three databases yielded 433 papers. The three researchers then divided up and filtered this set of papers based on titles and abstracts, reducing them to 34 papers. We again performed a backward and forward reference search on these papers and obtained a total of 55 papers.

Finally, these 55 remaining papers underwent a more detailed review; the three researchers independently reviewed the RQs, key contributions, and high-level findings of each of these papers, to determine whether they met our inclusion criteria (see below), then discussed and resolved any disagreements. This process yielded 42 papers. During the deeper reading of the later systematic review process (see Section 3.2), we discarded an additional 4 papers and added 2 back in, leaving 40.

Round 2. After developing our systematic framework (see Section 3.2), we conducted a second round of searches, iterating through the citation-chaining and (expanded) keyword-search processes described above to bring the dataset up to date. Four of the researchers split up and reviewed titles and abstracts, discarding obviously irrelevant papers to create an initial dataset of additional papers published through 31 August 2024 (including some published before August 2023, via backward citation-chaining from newly identified papers). Those four researchers reviewed the papers identified as potentially relevant, using the processes described above, and agreed on 22 that met our inclusion criteria (16 of which were published between August 2023 and August 2024, and 6 earlier); we also re-added 1 paper discarded in Round 1, for 63 papers total.

Inclusion and Exclusion Criteria. We *included* papers that:

- Explored bystander privacy in smart homes, including:
    - People’s experiences and views as bystanders,
    - Responses to hypothetical scenarios or role-play described from the perspective of bystanders, or
    - Responses to scenarios about bystanders described without perspective;
- Contained significant findings about bystander privacy in smart homes; and/or
- Suggested design solutions specifically to improve bystander privacy in smart homes.

For the most part, we *excluded* papers that:

- Studied bystanders only from the perspective of primary users, without studying bystander perspectives/views of bystanders themselves:
    - Unless they included bystander-specific recommendations based on substantive discussions of how the design of smart home devices impacts bystander privacy;
- Examined bystander privacy only in terms of devices’ technical vulnerabilities, or via legal analysis or speculative inquiry, without studying bystander perspectives/views of bystanders themselves:
    - Unless technical work prototyped a design specifically for smart home bystander privacy;
- Studied only primary users’ privacy *from* bystanders;
- Studied only technical security/access control, without exploring privacy implications;
- Examined views on smart devices in non-residential buildings or on IoT generally:
    - Unless they included distinct, separable findings about smart home devices specifically;
- Focused solely on solutions that were not related to the design of the device itself nor to technology that could interact with the device, but rather aimed only to interfere with devices’ ability to collect usable data about bystanders (we view this as a separate body of work);
- Focused solely on subjects of home health monitoring (we view this as a separate body of work; see recent overviews [97, 102, 106, 107]);
- Were not peer-reviewed.

3.2 Development of Systematic Framework

For each paper, we collected relevant information such as methods, key findings, and information relevant to our RQs, such as concerns and design recommendations related to bystander privacy in smart homes.

We began the framework development relative to our RQs by documenting the definitions of “bystander,” privacy concerns of bystanders, and recommended design solutions for an initial set

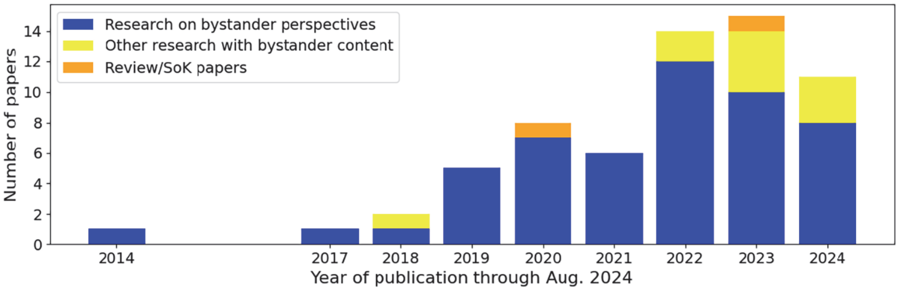

Fig. 1. Publication years of papers in our dataset. (2024 includes only those published through 31 August 2024.)

of 15 papers in a set of shared spreadsheets. Two of the authors each independently grouped the identified definitions, concerns, and recommendations into categories, then discussed and agreed on an initial categorization scheme. We then divided the remainder of the papers (in both rounds) amongst several of the authors, with each being reviewed by at least two authors. As we went along, we discussed and refined the category criteria and descriptions to incorporate relevant dimensions, and/or added any new categories that emerged. These categories are reflected in Figure 2 and Tables 1–3.

In addition to the framework categorization, we recorded detailed information about each paper, including methods used, countries and populations studied, and other characteristics such as whether they specifically involved human subjects research from the perspective of bystanders. That information is reflected in Section 3.3 and Appendix A.

3.3 Description of Dataset

The 63 papers in our final dataset included 51 papers describing original human-subjects research focusing specifically on smart home privacy of bystanders [2, 5–8, 11, 12, 26, 28, 29, 37–39, 42–44, 47, 48, 51, 56, 64, 67, 68, 70, 71, 75, 76, 81, 84–89, 93, 105, 121, 124, 125, 132–139, 142, 143, 145, 148]; 10 others with substantial relevant content about bystanders [27, 34, 98, 126, 130, 131] or developing bystander privacy solutions *without* human subjects [25, 65, 66, 144]; and 2 review/systematization papers covering subtopics of our topic [10, 94].

Figure 1 breaks down the dataset by year of publication, showing the growth of literature in this area. The majority of papers were published at conferences, including ACM CHI (15), USENIX Security (8), PETS (6), ACM DIS (6), and ACM CSCW (4). Most of the remaining papers were published in other conferences, workshops, or journals focusing on HCI, security and privacy, and/or IoT (e.g., SOUPS, MUM, MHCI, PACMHCI, and NordiCHI). Three of the papers were published in non-computer science/HCI venues *Gender, Place, and Culture*, *Ethnos*, and *New Media and Society*.

Of the 56 papers in our dataset that involved original human subjects research (including the 51 with bystanders and 5 with only primary users[1]), 39 specified the countries from which participants were recruited. Of those 39 papers, 29 were conducted entirely in the Global North, including 17 with participants only in the United States, 5 with participants only in Germany, 4 with only the United Kingdom, and 3 with other countries in Europe. Ten papers included participants in

[1] One paper on primary users used data from web fora, so we do not include it in this count.

Table 1. Framework for Categorizing Groups of Bystanders Discussed in Prior Literature, by Relationship to Smart Home and Device Owner

Relationship with Smart Home	**Relationship with Device Owner**	**Examples**	**Relevant Papers**
Visiting Bystanders	Familiar visitors and guests	Family members, friends, neighbors, other invited guests (brief visits or overnight)	[11, 12, 26, 39, 42, 43, 56, 73, 85–89, 93, 94, 105, 130–132, 136, 137, 139, 148]
	Domestic workers (live-out)	Care workers, household employees, occasional workers with an ongoing relationship (e.g., tutors, housecleaners)	[5–8, 28, 29, 39, 68, 105, 124, 131, 138]
	Short-term rental tenants	Airbnb/VRBO guests, other vacation and short-term rental tenants (with live-in or live-out hosts)	[25, 37, 39, 42, 65, 84, 98, 105, 134, 139, 144]
	(Other) Strangers	Campaign door-knockers, delivery people, one-time service workers/tradespeople (e.g., exterminators), other unfamiliar visitors	[11, 12, 37, 39, 86, 131, 138]
Live-In Bystanders	Family members and roommates (cooperative relationships)	Roommates/housemates, spouses/partners, other adult family members	[26, 27, 34, 37–39, 42, 44, 48, 56, 64, 70, 75, 81, 88, 89, 93, 94, 121, 131, 132, 135, 137, 139, 142, 143]
	Children	Young children, teenagers	[56, 75, 81, 94, 105, 131, 133, 138, 143]
	Long-term tenants	Tenants (of live-in or live-out landlords), subtenants, long-term guests	[26, 47, 56, 71, 87, 105, 138, 142]
	Domestic workers (live-in)	Live-in caregivers, au pairs, household employees	[5–8, 28, 29, 67, 68, 105, 124]
	Household members in hostile environments	Victims of IPV, domestic abuse, or other hostile relationships	[10, 76, 125, 126]
Uninvolved Bystanders	Neighbors (on own property)	Neighbors on own property	[37, 39, 105, 130, 131, 145]
	Passersby	Passing neighbors, passing strangers	[39, 131]

IPV, Intimate partner violence.

Table 2. Summary of Bystander Privacy Concerns from Existing Literature

Concerns	Threat Groups	Bystander Groups	Relevant Devices	Design Recommendations	Relevant Papers
Non-disclosure: Devices already deployed are not disclosed by primary users.	Employers, hosts in smart homes, short-term rental hosts	Domestic workers, guests and familiar visitors, short-term rental tenants, strangers	Smart cameras, Smart toys, Smart speakers, and similar devices with voice assistants	Privacy Nudges, Visual/Auditory/Haptic Cues, Smart Home Dashboards, Device Display Apps, Communication and Negotiation Mechanisms	[5, 8, 12, 28, 29, 38, 43, 51, 67, 84, 125, 134, 139, 145]
Lack of data awareness: Limited awareness of device data practices, including data collection details, frequency, and storage.	Primary users, device manufacturers, landlords	All groups[a]	General	Visual/Auditory/Haptic Cues, Smart Home Dashboards, Device Display Apps, Multimodal Access to Privacy Settings, Tangible Privacy Controls	[5–8, 10, 12, 26, 39, 43, 47, 48, 51, 56, 71, 75, 84–89, 93, 94, 124, 125, 134, 139, 145]
Lack of or limited control: No data control due to lack of access to settings, absence of separate accounts for live-in bystanders, or guest modes for bystanders, risking unauthorized or unwanted access by members of the household (or even visitors). No direct control over how primary users use the data or who they share it with.	Primary users, device manufacturers	All groups	Smart cameras, Smart speakers, Smart locks	Guest Mode, Temporary Data Storage, Smart Home Dashboards, Device Display Apps, Separate Profiles, Multimodal Access to Privacy Settings, Tangible Privacy Controls, Tunable Access Control Options, Authenticated Permission, Communication and Negotiation Mechanisms, Tangible Personal Controller	[5, 7, 10, 12, 26, 28, 43, 51, 64, 68, 71, 75, 76, 81, 85, 86, 88, 93, 124, 125, 132, 134]
Lack of consent: Bystanders have little opportunity to consent to or reject data collection in smart homes, or may feel unable to reject it.	Primary users, device manufacturers	All groups	General	Limit Conditions for Data Collection/Recording, Guest Mode, Privacy Nudges, Authenticated Permission, Communication and Negotiation Mechanisms, Multimodal Access to Privacy Settings	[5, 6, 11, 12, 28, 29, 37, 39, 48, 85, 88, 93, 124, 134, 138, 145]
Data misuse—Spying and intrusive monitoring: Bystanders can be spied on, eavesdropped on, or tracked by primary users. Abusive partners may install spyware.	Primary users, abusive partners, employers, landlords	All groups	Smart cameras, Smart door locks, Smart speakers	Minimize Data Collection, Limit Conditions for Data Collection/Recording, Guest Mode, Visual/Auditory/Haptic Cues, Separate Profiles, Tangible Privacy Controls, Authenticated Permission, Tangible Personal Controller	[8, 10, 28, 29, 38, 39, 43, 48, 76, 84, 88, 94, 124–126, 133, 134, 138, 142]
Data misuse—Harassment: Sensitive and private video recordings can be used to harass or invade the privacy of bystanders.	Employers, abusive partners	Domestic workers (especially female) and people in hostile home environments	Smart cameras	Temporary Data Storage, Separate Profiles, Tunable Access Control Options, Authenticated Permission	[8, 10, 28, 67, 68, 76, 124, 125]
Data misuse—Discriminatory or unfair treatment: Data access may result in discrimination, micromanaging work or activities, or using captured audio/video to support biased actions.	Primary users, employers, parents, landlords	All groups	Smart cameras, Smart devices with microphones	Minimize Data Collection, Guest Mode, Temporary Data Storage, Separate Profiles, Multimodal Access to Privacy Settings	[5, 28, 29, 38, 47, 67, 68, 71, 81, 84, 87, 124, 133, 138]

(Continued)

Table 2. Continued

Concerns	Threat Groups	Bystander Groups	Relevant Devices	Design Recommendations	Relevant Papers
Tampering with indicators: Visual/auditory cues in devices that signal collection or recording status can be tampered with.	Employers, hosts in smart homes, short-term rental hosts	Domestic workers, guests and familiar visitors, short-term rental tenants, strangers	Smart cameras, smart microphones	Tangible Privacy Controls	[105, 132]
Data handling by manufacturers: Device manufacturer or service provider is considered untrustworthy; bystanders fear their data is being misused by manufacturers, including being shared with or sold to third parties.	Device manufacturers	All groups	General	Minimize Data Collection, Conventional Device Controls	[43, 51, 64, 84, 89, 93, 136, 139]
External threats: Inadequate device security by less tech-savvy users can inadvertently endanger bystander privacy, leaving them susceptible to external attacks such as hacking.	Primary users, External hackers	All groups	Smart cameras, Smart speakers	Minimize Data Collection	[12, 43, 48, 51, 75, 84, 88, 93]

[a] This category encompasses all groups of bystanders defined in Table 1.

countries in the Global South, including 4 studies in Jordan, 3 in China, 1 in Malawi, and 2 that included a mix of countries in both the Global North and Global South.

In terms of research methods, at a high level, 54 out of the 61 papers on original research employed qualitative research methods, 19 quantitative, and 27 employed design approaches. Fifteen used a mix of those approaches. Among the qualitative papers, 38 conducted interviews, 11 conducted focus groups, and 5 conducted an observational study; less common methods included textual analysis and qualitative analysis of open-ended surveys. (Some papers included multiple qualitative approaches.) Among the quantitative papers, 18 used surveys and questionnaires, and 2 conducted experiments. Of the papers with a design element, 9 included participatory design, 6 scenario-based design, and 3 field studies. Two of the papers involved wireframing and 13 prototyping, and 15 collected feedback on design ideas or prototypes.

Appendix A provides a breakdown of the paper types, research methodologies, and content relevant to our framework for each paper.

3.4 Limitations

Our review approach has some limitations. First, beginning our keyword search in computer science/engineering databases may have limited the selection and scope of the literature we found. To address this, we performed citation chaining to identify papers published in non-CS venues (e.g., social science/humanities journals). Citation-chaining also helped to address any potential limitations from our choice of keywords (particularly given the unsettled state of the terminology involved), including using it as a basis for expanding our keyword set as described in Section 3.1. Our review was also limited by choices we made about what we viewed as being in scope; it

Table 3. Technical Design Solutions Proposed in the Literature, along with Their Limitations and Challenges

	Design Suggestion	**Design Description**	**Limitations and Challenges**	**Relevant Papers**
Limiting Data Collection	Minimize Data Collection[a]	Minimize device data collection to essential functions, following the principle of least privilege. Use the least amount, type, and granularity of data necessary for each essential function. Minimize information required for setup, and don't require account linking. *Device types: Smart cameras, smart speakers*	Research needed to determine the least data/granularity needed for different use cases [84], balanced against functionality [5, 133]. Device needs to be able to verifiably enforce least privilege where appropriate [84].	Suggestions: [5, 27, 38, 56, 84, 133] Feedback: [26]
	Limit Conditions for Data Collection/ Recording[a]	Design cameras or other devices for to only begin recording, only trigger live view, or only use high-granularity sensors when specific events occur (e.g., pet presence, unfamiliar faces). May include ability to deactivate automatically during recognized events (e.g., privacy-sensitive situations, presence of someone who has not consented to collection) and/or automatically activate only for emergencies (e.g., smoke). Device could discard command history or audio data, perturb or obscure data like faces in video, and/or allow privacy zones to limit data collection. *Device types: Smart cameras, smart speakers*	Automatic recognition required for triggers may be viewed as more invasive [131]. May be seen as interfering with utility [7, 39, 130]; e.g., obscuring unrecognized faces may impinge on functionality, especially for security devices [5].	Suggestions: [5, 7, 8, 27, 37, 39, 93, 130, 131] Participatory: [34, 39] Feedback: [26, 85, 105]
	Guest Mode[a]	Introduce a guest mode for smart home devices, where data collection is limited or stopped (see Limit Conditions). Guests can utilize the device and may be able to modify some functions, but privacy settings remain inaccessible (unless implemented as a separate user profile; see Separate Profiles). Device could automatically enter guest mode on detecting someone who has not consented to data practices. *Device types: General (emphasis on smart speakers)*	Automatic approaches would require robust recognition to identify trigger conditions [5]. (Limiting or stopping data collection incurs challenges as listed under Limit Conditions and Temporary Storage.)	Suggestions: [5, 11, 56, 75, 86, 87, 89, 93, 139] Participatory: [34, 39, 139] Feedback: [85]
	Temporary Data Storage[a]	Implement temporary data storage and allow on-device storage, to balance owners' utility and bystanders' privacy. For instance, devices could auto-delete data after a defined time frame. *Device types: General*	Automatically deleting potential evidence can pose legal challenges for victims of abuse [10, 124, 125] or in other disputes [98, 138]. Not easily confirmable by bystanders [85].	Suggestions: [7, 10, 12, 131] Participatory: [39, 139] Feedback: [26, 85] Prototypes: [25]
	Privacy Nudges	Include nudges in set-up encouraging users to consider others' privacy in choosing device location and settings, inform bystanders or seek consent, or create separate profiles (see Profiles). Nudges could be pre-set or based on automatically detecting potential privacy violations and suggesting users reconsider, while still retaining option to follow through with the action. Add friction to setup options that don't respect bystander privacy. *Device types: Smart cameras, smart speakers*	More research needed to evaluate efficacy of nudges [124]. Not transparent to non–primary users [131]. (We note that usability is also a challenge requiring further research.)	Suggestions: [26, 28, 43, 56, 93, 124, 130, 131, 135, 143] Feedback: [105]
	Conventional Device Controls[a]	Maintain conventional controls such as physical buttons for operating smart home devices, to prevent forcing bystanders to interact with smart hubs/assistants that leave a data footprint. Also aids transparency because position of switch is visible. *Device types: General*	(No limitations noted.)	Suggestions: [2, 56, 75, 142, 143]

(Continued)

Table 3. Continued

	Design Suggestion	Design Description	Limitations and Challenges	Relevant Papers
Increasing Transparency	Visual/Auditory/Haptic Cues[a]	Provide clear auditory, visual, and/or haptic cues (e.g., LED, blinking lights, beeps, audio announcements, vibration). These indicators should signify device presence and data collection/recording status, and manufacturers should ensure they cannot be tampered with. Make sensors visible, easy to identify, and easy to understand across diverse audiences. *Device types: Smart cameras, smart speakers*	Complex visual and auditory cues can confuse bystanders, especially in devices with multiple cues for different statuses; ambiguity between “off” and “standby” especially creates difficulties [2, 94, 105, 132]. Overly intrusive signals may annoy or put people on edge [28, 132], or may not fit the aesthetic [85]. Some modalities not available to people with sensory impairments [105, 145]. (We note that consistency across manufacturers is necessary for comprehension.)	Suggestions: [2, 5, 7, 8, 86, 87, 124, 126, 132, 142, 145] Participatory: [39, 76] Feedback: [26, 85, 105, 132]
	Smart Home Dashboards	Develop physical or digital smart home dashboards to share information with guests, e.g., in Airbnbs. Can be just a transparency measure, or could be designed to share control amongst a household or with guests. Could incorporate central access controls. *Device types: General*	Information could be used to circumvent the owner’s purposes for the device, especially if used for monitoring [84, 85]. Bystanders may find it socially awkward or even invasive to look at information about others’ devices [51, 85, 132], or to ask for changes as a result [137]. Information may be difficult to understand [51, 132, 135, 137]. (We note that integrating devices from multiple manufacturers may be a challenge.)	Suggestions: [84, 88] Participatory: [137] Feedback: [85, 132] Prototypes: [42, 51, 135, 137]
	Device Display Apps	Design apps to identify all smart devices in a home, e.g., via devices’ Bluetooth beacons or upon visitor Wi-Fi connection. Devices could provide, e.g., their location on a map of the home, details about data practices, and/or access information. Devices could also broadcast notifications about state changes. App could be designed as a digital dashboard (see Dashboards). Could facilitate consent or offer control, in addition to transparency (if combined with app-compatible designs under Enabling Control). *Device types: General*	May be used to circumvent owner’s purposes, e.g., monitoring [42]. May be seen as invasive of primary users’ privacy [85, 132, 145]. Information may not be understandable to bystanders [51, 124], and too-frequent notifications may be overwhelming or disturbing [12, 51, 85, 143]. Devices broadcasting information about themselves may cause security and safety vulnerabilities [5, 42, 51, 66, 85, 132, 139].	Suggestions: [5, 8, 12, 26, 39, 86, 87, 139, 142, 145] Participatory: [76, 137, 139] Feedback: [85, 88, 105, 132] Prototypes: [6, 42, 51, 66, 143, 144]
	Separate Profiles[a]	Enable easy creation of multiple user profiles, e.g., guest and worker profiles with limited data access and control, and separate profiles for cohabitants. Could be secured by voice or biometric verification for some situations. Deleting or migrating old profiles should also be easy, and could be centralized. Can be combined with Tunable Access Control Options for optional fine-grained distinctions. *Device types: General*	Necessitates a strong but low-friction authentication system to remain usable and prevent unauthorized access to other users’ profiles [10, 64, 76, 143]. May be difficult to verifiably ensure access is revoked when it’s supposed to be [56, 84, 105]. App-based implementations require each user to have a phone [56, 84].	Suggestions: [7, 10, 43, 44, 56, 64, 75, 84, 125, 142] Participatory: [34, 76, 137] Feedback: [105] Prototypes: [143, 144]
	Multimodal Access to Privacy Settings	Provide controls for critical privacy settings that bystanders can access directly in multiple modalities without an account, e.g., physically on the device (as an interface or as tangible sensor blockers (see Tangible Controls)), using a separate dashboard (see Dashboards), by voice interaction, or via a web portal. Settings should be easy to use, comprehensible, and available in multiple languages. *Device types: General*	Owners may be concerned about bystanders choosing settings that reduce privacy or compromise functionality; works best with cooperation [70, 85].	Suggestions: [8, 70, 75, 93, 124, 143] Feedback: [85]

(Continued)

Table 3. Continued

	Design Suggestion	Design Description	Limitations and Challenges	Relevant Papers
Enabling Data and Configuration Control	Tangible Privacy Controls[a]	Design cameras with prominent lens-lids (shutters), and speakers with physical microphone blockers, or allow sensors to be detached entirely. Physical sensor blocks can aid transparency even if bystanders do not use them to control devices. *Device types: Smart cameras, smart speakers*	Blocking microphones is technically challenging [105, 121]. If remote-openable, shutters can be opened after inspection by bystanders [2, 137], but fully manual requires remembering [121]. May conflict with aesthetics [105].	Suggestions: [2, 86, 131, 137] Feedback: [105, 121] Prototypes: [137]
	Tunable Access Control Options	Enhance access control options with precision, including location-based (limited to in-house presence), time-based (access expiration), per-device/per-room (specific room/device control), and per-user role (restricting access). This mechanism could be implemented on multi-device smart home platforms. *Device types: General*	Usability challenges of complex controls may deter adoption by primary users [143] or use by non−primary users [124]. Complexity may make it more difficult to balance against functionality [143]. Location-based access control may make it difficult to provide evidence of abuse after leaving the home [124].	Suggestions: [28, 43, 124–126, 133] Prototypes: [25, 65, 133, 143, 144]
	Authenticated Permission	Include permission mechanisms, such as biometric verification, for primary users to access bystander or secondary user data, or even for the device to collect (unobscured) data about them. For instance, camera feed access for a certain time frame might need approval from everyone whose face appears in the video during that time. Could implement by creating automatic profiles when new voices or faces are detected. *Device types: Smart cameras, smart speakers*	May be structurally difficult to implement [131], e.g., without causing inaccessibility for all if one person doesn't notice a request [144]. (We note that limiting the ability to access others' data may be the least acceptable to those potential owners who would be most likely to use devices for malicious purposes.)	Suggestions: [5, 38, 75, 131] Participatory: [34, 76] Prototypes: [144]
	Communication and Negotiation Mechanisms	Design apps to broadcast bystanders' preferences (e.g., no recording, blur face/voice) and enable devices to accommodate them automatically. Incorporate negotiation tools in smart devices, Device Display Apps (above), and/or web portals in which owners/primary users and bystanders state privacy preferences, with digital agents aiding agreement. Such mechanisms could also provide transparency and establish consent. *Device types: General*	Less likely to be effective in low-trust or imbalanced relationships [6, 11, 39]. Bystanders may still feel pressure to make concessions when visiting someone else's home [11], especially if preferences conflict with the device purpose [139]. Research is needed on usability [139, 148], especially for bystanders without phones [6, 42], and how to ensure owners' privacy is not violated [87]. (We note that initiation of a negotiation interaction is another research challenge.)	Suggestions: [12, 39, 51, 75, 87, 131, 139] Participatory: [137, 139] Feedback: [88, 105] Prototypes: [6, 11, 42, 148]
	Tangible Personal Controller	Introduce user-friendly devices for tech-limited bystanders to configure smart home privacy. For example, a physical controller with toggle buttons could control nearby device sensors. *Device types: General*	May introduce security vulnerabilities [42]; requires carrying the object [42]; bystanders may find it socially unacceptable to change settings on others' devices [42].	Suggestions: [137] Prototypes: [42]

In the "Relevant Papers" column: Suggestions = Suggested by authors based on (original or reviewed) human subjects research; Participatory = Product of participatory design research; Feedback = Sought feedback on design descriptions in HSR; Prototypes = Tested an interactive prototype of the design.

[a] The design has been implemented in a commercial product (see Table 4).

therefore leaves out interesting work in some related areas (such as IoT sensor foiling, or design solutions intended to support primary user privacy that might also be useful to bystanders). We view such choices about scope as an inherent aspect of *systematic* review.

Meanwhile, the interpretation of findings and our resulting categorizations may have been influenced by our perspectives or expertise. Our strategy of having multiple researchers develop the framework collaboratively and cross-check paper categorizations aimed to mitigate such biases. In addition, for RQ1–RQ3, we aimed to categorize papers according to what they said explicitly, rather than inferences we could draw from their findings and recommendations. Lastly, as our search methods resulted in identifying papers mostly in English, our review may have missed findings or dimensions relevant in different cultural and regulatory environments. However, as even non-English computer science venues tend to circulate abstracts in English, we believe it unlikely that we missed any relevant papers.

4 RQ1: Definition and Classification of Smart Home Bystanders in the Literature

The category of *bystanders* can be defined and subclassified along multiple dimensions. In this subsection, we discuss how different researchers have defined the term *bystander* in terms of people's roles relative to a device, and what other terms have been used (Section 4.1). We then describe how bystanders have been classified by existing scholarly works in terms of relationships to the smart home and the device owner, and provide a framework for organizing those relationships (Section 4.2).

4.1 Bystanders as Defined and Classified by Relationship to Device

In a smart home, people may assume different roles in terms of their interaction with and control over a given smart home device. (The same person may be in different roles relative to different devices, or even at different times relative to the same device.) Relative to a given device, roles described in the literature include:

- *Owners* purchase and deploy the devices and (almost always) have control over privacy settings [6, 11, 12, 25, 37, 39, 65, 85, 89, 105, 130, 132, 134, 137, 139, 144, 148].
- *Primary Users* may or may not own the devices, but have significant interaction with and control over them, sometimes via admin accounts [42, 43, 64, 75, 84, 87, 105, 121, 131, 138, 142]; also called Pilot Users [70, 135], Account Owners [93, 94], Drivers [56], or Initiators [48].
- *Secondary Users*, usually residents, use the devices frequently but have less control compared to primary users [42, 43, 56, 64, 75, 76, 89, 121, 133, 143]; also called Passenger Users [70, 135], Resident Owners [93], Passive Users [56], or Co-Users [105].
- *Incidental Users*, such as visitors, may occasionally use devices [8, 39, 43, 89, 105, 139, 148].[2]
- *Non-Users* do not directly use or have control over devices, but data about them may be collected (whether or not they live in the home) [2, 8, 11, 94, 105, 121, 132, 136, 139, 145].

Someone in any of the above roles may also be a *Target of Surveillance/Monitoring* by an owner or user of the device [5, 6, 8, 28, 29, 38, 47, 68, 76, 81, 84, 125, 126, 133]; also called Surveilled Subjects [105, 131]. The roles toward the end of the list, with little or no control of a device's data collection, are more likely to be targeted for deliberate surveillance, but even regular users (secondary users or, in unusual cases, even owners) may be targeted by a cohabitant or other known party who has control of the device. (Some other works that taxonomize roles relative to devices (e.g., [105]) view surveillance targets as a separate category rather than a cross-cutting dimension.)

Figure 2 shows some different ways that smart home and IoT privacy researchers have applied the term *bystander* to different subsets of the roles listed above, depending on their focus. For example,

[2] Some researchers (e.g., [142]) use the term *incidental users* to refer to what most others call *secondary users*, though this is less common; others (e.g., [37, 39]) use the term to cover both. Conversely, other researchers have used *secondary users* to refer to a larger category including what others refer to as *secondary* and *incidental* users, and even non-users [93, 94].

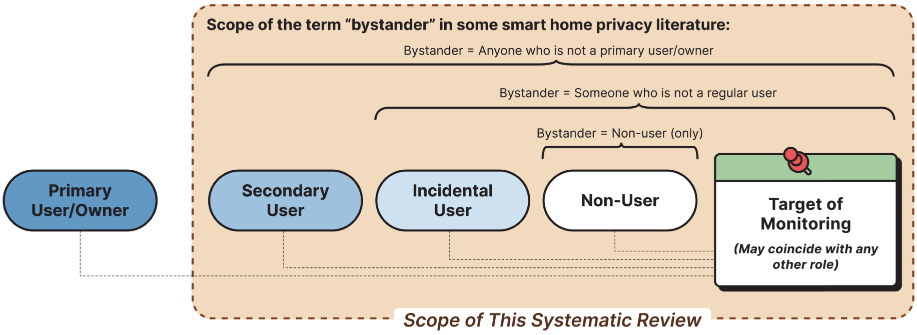
Scope of the term "bystander" in some smart home privacy literature:
Bystander = Anyone who is not a primary user/owner
Bystander = Someone who is not a regular user
Bystander = Non-user (only)
Primary User/Owner
Secondary User
Incidental User
Non-User
Target of Monitoring
(May coincide with any other role)
Scope of This Systematic Review

Fig. 2. Some uses of the term *bystander* in the literature aligned with roles relative to a device. The shaded area shows the scope of this review.

Pierce et al. [105] use *bystanders* to refer only to non-users of a device, while using *adjacent actors* for a larger category that includes incidental users, non-users, and surveillance targets. Thakkar et al. [132] include both incidental users and non-users of a device in the scope of *bystanders*, but do not include regular secondary users.

Other researchers (e.g., [8, 139]) also include non-users and even secondary users who live in the home as *bystanders*, if they did not make the decision to purchase or deploy a device and have limited control over the device and its configuration—in other words, anyone who is not an owner nor a primary user. Alternatively, some refer to this larger category collectively as *non–primary users*, rather than *bystanders* (e.g., [131])—though others use *non-primary users* to refer specifically to secondary users (e.g., [75]), or secondary and incidental users (e.g., [105, 142]). Furthermore, other dimensions may also be relevant; for example, Marky et al. [89] distinguish *bystanders* (for their purposes) as those who have some ability to perceive device output (e.g., hearing a smart speaker alarm set by an owner). However, most prior work does not make this distinction.

Regardless of the terminology used by the authors, we include in the scope of our systematic review papers that contribute findings about the privacy of anyone who is affected by a given smart home device or environment without having active control over privacy configurations or data collection. (For the most part, this excludes primary users and owners, though occasionally device owners are targets of surveillance by smart home manufacturers and governments [129, 146].) As depicted in Figure 2, this article will use the term *bystanders* for all such actors.

4.2 Bystanders as Defined and Classified by Relationship to Device Owner

In addition to roles relative to the device, some researchers have defined and subclassified the term *bystander* in terms of someone's relationship to the home or the device owner/primary user(s). Many of the papers we reviewed focused on bystanders in specific types of relationships.

To capture these classifications, we introduce a framework to classify bystanders based on their relationship to the smart home and the device owner. We include types of interpersonal relationships that have been researched within the broad category of roles we targeted as *bystanders* in Figure 2 relative to the device, regardless of whether the authors referred to them using the term *bystanders*. This framework is captured in Table 1 below, with references for each relationship category. We aim to encompass most groups studied in the literature, though gaps may exist.

At the first level, bystanders can be categorized according to their relationship to the household and frequency of their interactions with the smart home environment: *Visiting bystanders* are not residents of a given smart home, and therefore have short or limited exposure to its devices, and *live-in bystanders* are long-term residents of a multi-user smart home who do not have primary control over the devices. *Uninvolved bystanders* are not intentionally interacting with the occupants of the home at all when data is collected, nor engaged in activities involving them.

At the second level, we categorize bystanders into subgroups based on the relationship they share with the device owners. Social dynamics and power differentials between bystanders and device owners can significantly influence privacy perceptions common within the different subgroups.

4.2.1 *Visiting Bystanders.*

Amongst visiting bystanders, first, *familiar visitors and guests*, like visiting family members, known guests or friends, and visiting neighbors, often have an amicable social relationship and minimal power disparity with the device owner/primary user(s) [11, 12, 26, 39, 42, 43, 56, 73, 85–89, 93, 94, 105, 130–132, 136, 137, 139, 148]. In such balanced host-guest dynamics, bystanders are less likely to have strong concerns about malicious primary user actions, but other privacy concerns, e.g., about service providers' use of data, may still remain.

Second, *live-out domestic workers*, including care workers like babysitters and household employees (staff), often have a transactional relationship and noticeable power asymmetry with the device owner/primary users [5–8, 28, 29, 39, 68, 105, 124, 131, 138]. This may lead to them exhibiting greater mistrust toward devices—especially those equipped with recording features, such as smart cameras and microphones, that can be used to monitor work. Certain domestic workers or visitors may be granted more extensive access and control over the devices and their functionalities, leading to increased trust on the part of the bystander and reduced concerns regarding privacy infringements, but potentially increased concerns about breaches of the primary users' privacy.

Third, *short-term rental tenants* in furnished units, for example, in Airbnb settings, usually do not have primary control over the smart devices deployed, and may not be able to use them at all [25, 37, 39, 42, 65, 84, 98, 105, 134, 139, 144]. The lack of relationship with the device owner/primary user(s) can lead to high concern about data collection and use, including concerns about hidden devices.

Fourth, *other types of strangers*, such as delivery people or tradespeople with no ongoing relationship to the household, may be less comfortable with data collection than in familiar environments, but view it as something they cannot do much about [11, 12, 37, 39, 86, 131, 138].

4.2.2 *Live-In Bystanders.*

Live-in bystanders studied in existing literature can be categorized into five subgroups. The first subclass is *residents in cooperative relationships, including family members and roommates*; this subclass involves a low power differential with a negligible hierarchy among residents—though secondary or incidental users may still have less control over the device and data collection, or may not use the device at all [26, 27, 34, 37–39, 42, 44, 48, 56, 64, 70, 75, 81, 88, 89, 93, 94, 121, 131, 132, 135, 137, 139, 142, 143]. In cooperative, less-hierarchical multi-user homes, bystander privacy concerns tend to be fewer and milder than in households with more hierarchical dynamics.

The second subclass is *children* and teenagers, where there is a pronounced difference in authority, but the relationships are usually benevolent [56, 75, 81, 94, 105, 131, 133, 138, 143].[3] However, privacy conflicts may arise over parental monitoring, especially of teenagers.

The third subclass is *long-term tenants*, including tenants of live-out landlords or live-in (renting out a room), or some long-term guests/crashers [26, 47, 56, 71, 87, 105, 138, 142].[4]

[3] As per our inclusion criteria, we did not review papers studying only parents' views on their children's privacy (unless they were otherwise includable), but readers interested in the topic can find literature on parents' views of children's privacy as both secondary (e.g., [72, 111, 128]) and primary (e.g., [23, 92]) users, along with research studying children's views as primary users (rather than bystanders) (e.g., [19, 77]).

[4] Relationships with live-in vs. live-out landlords imply quite a different structure, but not all of the literature reviewed makes the distinction. Pattnaik et al. [99] investigate these nuances in detail (but not included in our review as it is after the target time period).

Fourth, *live-in domestic workers* may also be bystanders; in that case, privacy perceptions are similar to live-out workers, but with additional concerns around private spaces (bedrooms) and personal time vs. work time [5–8, 28, 29, 67, 68, 105, 124].

The final subclass captures *household members in a hostile home environment* with a high power differential (e.g., victims of domestic abuse), where smart home devices can be used for monitoring and surveillance of those individuals [10, 76, 125, 126]. Such an environment leads to a larger set of more serious privacy and safety concerns, over a wider array of smart home devices.

4.2.3 Uninvolved Bystanders. Among uninvolved bystanders, smart home devices may capture data about *neighbors on their own property*, either intentionally or unintentionally [37, 39, 105, 130, 131, 145]. Unintentional capture (at least in outdoor spaces) tends to raise less concern than devices in indoor spaces. They may also collect data about *passersby* [39, 131].

We talk more about how social dynamics, as well as other contextual factors, affect the concerns of bystanders in Section 5.2.

5 RQ2: Bystander Privacy Concerns

Prior work has extensively explored the privacy concerns of bystanders in smart homes. Regardless of the extent to which bystanders think they possess a legitimate claim to privacy while situated within another individual's domicile, almost all prior studies we reviewed found that bystanders continued to exhibit concerns about the infringement of their privacy resulting from data collection facilitated by smart home devices.[5]

5.1 Classification of Privacy Concerns

The existing academic literature has explored the privacy concerns of smart home bystanders with regard to different stakeholders, including *device owner(s)/primary user(s)*, *device manufacturers*, and *other threat actors*. Through a thorough and comprehensive examination of the existing body of knowledge, we provide a detailed analysis of the multi-faceted nature of privacy concerns of smart home bystanders and the challenges that arise due to the involvement of various parties. These privacy concerns and challenges, along with the stakeholders that are affected by them, are described in detail in Table 2. We also reference design solutions proposed in the literature (to address these concerns); we provide details about these device design proposals in Table 3 and Section 6.1.

5.1.1 Privacy Concerns about Device Owner/Primary User(s).

Non-Disclosure. One of the main concerns expressed by bystanders is the non-disclosure of devices to bystanders by the device owner/primary user(s). Often, smart home devices are not disclosed to bystanders, resulting in a breach of trust [5, 8, 12, 28, 38, 39, 43, 84, 94, 125, 139]. This is especially true for bystanders who are not long-term inhabitants of the smart home, who may easily be left unaware of the presence of devices; this may include guests and visitors, domestic workers, and short-term tenants. Moreover, as noted by Zhao et al. [145], bystanders with visual impairments are particularly affected by this non-disclosure of devices since, unlike sighted people, they cannot simply look around and try to scan their environment for smart home devices.

Lack of Data Awareness. Even when the devices are disclosed, bystanders often face a lack of awareness regarding the extent of data being collected, where even the smart device owners may not fully comprehend the scope of data gathering—or even if they do, they may not disclose it,

[5] In Section 5, we omit papers noted in Section 3 that did not investigate the concerns of bystanders themselves, even if we included them for the purposes of other sections. We also do not include here papers that suggested or tested interventions without substantive discussion of concerns *per se*, leaving 39 out of 52 papers having bystander concerns.

leading to a sense of uneasiness and mistrust on the part of bystanders [7, 8, 10, 12, 39, 43, 47, 48, 56, 70, 71, 84, 86–89, 94, 124, 125, 134, 139]. In this regard, several studies have noted that bystanders are particularly uneasy about recording devices (like smart cameras) in intimate spaces, for example, in bedrooms and bathrooms [26, 28, 93, 124]. Recording devices, especially smart speakers, may also raise concerns due to uncertainty about when they are collecting data vs. in standby mode [2, 26].

Lack of or Limited Control. Another concern is the lack of control or limited degree of control a bystander has even when devices are disclosed. This lack of or limited control over what data is collected, how it is used, and who primary users may share it with is particularly problematic when it comes to smart cameras, smart speakers, or other devices with microphones [7, 10, 12, 42, 56, 68, 70, 71, 76, 81, 86, 88, 125, 132, 134]. In such cases, bystanders frequently find themselves confused about the actions they can take to mitigate potential privacy risks [10, 12, 26, 39, 42, 56, 70, 75, 76, 88, 94, 125, 132, 139].

This is particularly true for care workers and other types of domestic workers, given the inherent power dynamics stemming from the employer-employee relationship [8, 28, 29, 68]. However, it is worth noting that houseguests, including family and friends, also frequently encounter this issue, especially when they do not have their own separate user accounts for the devices. As described by Cobb et al. [39], while bystanders wish to be informed of the data collection practices and have mechanisms that motivate a conversation between the device owner/primary user(s) and bystanders, they often feel hesitant to voice their concerns while visiting the homes of family or friends, fearing potential strain on their relationships. Moreover, Meng-Schneider et al. [94] have depicted how bystanders perceive that their expressions of discomfort regarding smart home devices may not be adequately acknowledged. Concerns about primary users' data access and use are exacerbated by the potential for excessive data access to result in discriminatory or unfair treatment (see below), impacting Airbnb guests (whose opinions on data collection often clash with the Airbnb owners), long-term renters/tenants who don't own the smart devices in their homes (especially in public housing), domestic workers, visitors, and even co-inhabitants [28, 71, 84, 87, 134].

Lack of Consent. Challenges associated with the power dynamics in smart home environments extend to the complexities surrounding consent. While consent needs to be freely given (see [127]), several factors hinder the ability of bystanders to provide such consent to primary users in smart homes and lack of consent has been cited as a major concern [93]. Bystanders may face social awkwardness when communicating their preferences to device owners, which also affects their ability to reverse consent [11, 28, 43, 138], and they may feel the only choice they are given is "opt-in" [39]. Further, unlike device owners, bystanders do not have an opportunity to consent to the privacy policies of the devices [5, 6, 11, 37, 75, 85, 93].

Bystanders may have different levels of comfort with consenting to different types of data collection, for example, they may not be comfortable with the device storing voice recordings, but might be okay with non-PII data [12, 37, 85]. Alshehri et al. [12] note that in some US states such recording without consent is illegal; although the US federal law only requires one-party consent, some states in the US require two-party consent. Bernd et al. [28] highlight issues of implicit consent assumed by signing a job contract or continuing to work after camera disclosure. Similarly, Meng et al. [93] highlight how implicit consent might be assumed in shared living arrangements, which contradicts the guidelines provided by Strengers et al. [127] that consent should not be assumed until it is explicitly given. Chiang et al. [37] explicitly traded off these aspects of consent against each other, finding that participants put the most emphasis on whether consent was freely given.

Data Misuse. The misuse of data collected from smart home devices is another concern leading to fears of surveillance, eavesdropping, *spying, and intrusive monitoring* of bystanders' activities and conversations, by the device owner/primary user(s), without their explicit consent [7, 8, 28, 38, 39, 43, 47, 48, 51, 64, 67, 70, 71, 75, 84, 86, 87, 89, 138, 142]. A growing body of research is investigating such concerns among victims of **intimate partner violence (IPV)** or other technology-facilitated abuse, where non-disclosure and surveillance through smart home devices can amplify abuse [10, 76, 125, 126].

Past research has uncovered concerns relating to potential misuse of sensitive audio/video recordings or sharing of collected data without consent [7, 8, 28, 39, 64, 67, 76, 84, 88, 105, 124, 125, 131, 133], leading to *harassment* or invasion of a bystander's personal space, and inappropriate use of personal information.

A number of studies have identified that concerns about surveillance and non-disclosure of devices are particularly prevalent among domestic workers, including care workers such as nannies and nurses, and household employees such as housekeepers [8, 28, 67, 68, 124]. Domestic workers are concerned that such surveillance may lead to micromanaging and *discriminatory or unfair treatment*. Children and teenagers also worry about unfair over-management [81, 133]; similar views are expressed by women within patriarchal family structures [38]. Even people who are unintended bystanders to monitoring of someone else may see their data misused [28, 81]. Concerns about discrimination have also been identified in various types of rental situations [71, 84, 87, 138].

Tampering with Indicators. Furthermore, tampering with the visual or auditory indicators in devices that signal recording status (e.g., physically masking LED lights used for this purpose or turning off camera shutter sounds) is frequently observed as a concern in literature, primarily among domestic workers, guests, and Airbnb guests. This issue relates to devices like smart cameras and microphones [8, 132, 145].

5.1.2 Privacy Concerns about Data Handling by Device Manufacturers. In addition to concerns related to the device owner/primary user(s), prior work has found that bystanders are concerned about the actions of device manufacturers and governmental bodies. These fears are centered around manufacturers' data handling practices and the potential misuse of data. There are worries that manufacturers could exploit data to predict user behavior for targeted advertising or sell the data to third parties without obtaining proper consent [51, 56, 64, 93].

Bystanders often feel a lack of agency in controlling their data once it is collected by smart home devices, as they have limited control over how manufacturers store, access, and utilize this information, which further exacerbates their privacy concerns [43, 64, 89, 93].

5.1.3 Privacy Concerns about External Threats. Some bystanders are concerned about how their data could be exploited by malicious external actors including technically unsophisticated actors unintentionally compromising bystander privacy and potentially making the system vulnerable to external privacy attacks by hackers or malicious perpetrators. Devices such as smart home cameras and speakers are particularly deemed vulnerable in this context [12, 84]. Bystanders fear that compromising these devices may lead to security risks, like burglars being aware of when the residents are not at home by accessing data from smart cameras.

5.2 Influencing Factors

The degree of concern arising from the use of smart home devices by bystanders is influenced by a number of factors. These factors include power dynamics within relationships, shared experiences between bystanders and device owners, the actions of primary users, past privacy experiences, the environment in which devices are deployed, device features and capabilities, regulatory frameworks, awareness, and trust. Understanding how these elements interact can shed light on the complex nature of bystanders' concerns in the context of smart home technology.

Power Dynamics. The dynamics of the relationship between bystanders and the device owner/primary user(s) exert a significant impact on the degree of concern arising from the use of these devices. In scenarios where a bystander is unfamiliar with the owner, is a temporary visitor, or is not in control of how their own housing is equipped may give rise to heightened unease concerning potential data collection and surveillance activities [5, 8, 28, 39, 47, 71, 81, 84, 86, 89, 138].

In contrast, when bystanders have a close affiliation with the owner, such as family members or friends, they tend to feel more reassured and exhibit higher levels of trust in the owner's intentions regarding data use and data privacy [48, 132, 136, 139, 142, 145]. However, even in these more equitable relations, complexities in privacy perceptions may arise [37, 38, 142].

Additionally, power dynamics between bystanders and device owners can significantly influence the former's willingness to voice concerns about privacy. For instance, domestic workers may be hesitant to inquire about smart devices or express discomfort due to fears related to job security and potential repercussions [6, 8, 28, 68]. At a broader level, as bystanders, people feel more pressure to adhere to social norms, especially as a visitor, and may sacrifice personal comfort and privacy in order to not violate these norms [11, 29, 43, 132].

Shared Experiences. Furthermore, bystanders may be more comfortable about their privacy when they perceive that the device owner/primary user shares similar experiences with the device. For example, bystanders with visual impairments were more comfortable and trusting around the device owner/primary users who were also visually impaired as they believed such users would be more empathetic toward their unique privacy needs [145].

Actions of Primary Users. Bystanders' perceptions of smart home devices are also shaped by the actions of primary users—whether they attempt to surreptitiously collect data about bystanders [28, 38, 39, 43, 48, 64, 76, 84, 94, 133] or intentionally withhold information about the presence of devices [8, 12, 28, 39, 84, 94, 134]—and by the bystanders' own past experiences of privacy breaches, security incidents, or data misuses. Incidents of privacy violations in the past can deeply affect individuals when in the role of bystanders, leading them to exercise greater caution and apprehension when encountering smart home devices [10, 76, 125].

Environment and Cultural Context. The environment in which smart home devices are deployed also influences bystanders' level of concern. Bystanders may tend to be more vigilant about potential privacy risks in unfamiliar environments or when they are guests in others' homes [8, 28, 39, 43, 84, 86, 88, 89], and when the devices are deployed in intimate spaces, like bedrooms and bathrooms [37, 124, 136]. Moreover, the prevailing cultural norms and privacy expectations in different contexts can impact bystanders' attitudes toward smart home devices [1, 5, 7, 8, 37, 71, 81]. Despres et al. [43] found significant differences in whether participants had concerns about others' smart home devices, including privacy concerns, between participants in four different countries. Chidziwisano and Jalakasi [38] note concerns about how devices could reinforce prevalent practices of patriarchal control.

Device Features and Capabilities. The design and features of smart home devices emerge as crucial factors in shaping bystanders' concerns. Devices that closely resemble ordinary household items may raise privacy and security concerns, as they can lead to clandestine surveillance/data collection and a bystander may fail to recognize their true capabilities. For example, Yao et al. [139] noted that houseguests expressed discomfort over smart home devices that could be mistaken for children's toys. On the other hand, transparent devices that provide clear indicators of data collection may alleviate some concerns, as bystanders can be more aware of when the devices are actively collecting data [85, 105].

The user experience and interface design of smart home devices also influence bystanders' perceptions, with a well-designed and user-friendly interface that offers transparent information on data collection and sharing practices being more likely to mitigate concerns [132]. Moreover, bystanders may have different levels of privacy concerns toward devices with different sensors [7, 37, 43]. As noted by Windl and Mayer [136] and Benton et al. [26], bystanders are more concerned about smart home devices with audio/video recording capabilities than about devices with motion sensors (like smart lights).

Regulations and Legal Frameworks. The presence of relevant privacy laws and regulations can significantly impact bystanders' concerns [10, 76, 84, 119]. Conversely, being unaware of existing legal protections for privacy rights can become a source of discomfort to bystanders in their interactions with smart home devices [6].

Awareness and Trust. Bystanders' awareness of and level of knowledge about smart home devices and their data practices are further determinants of their concerns. Those with a deeper understanding of the technology may be more cognizant of potential risks, while individuals with limited knowledge may experience uncertainty and discomfort [8, 12, 38, 56, 75, 88, 118, 132]. Additionally, the level of trust a bystander places in the device owner and manufacturers *a priori*, for example, based on their past relationship, can shape their concerns [7, 11, 84, 93, 142]. Trustworthy owners who demonstrate a commitment to privacy and security are more likely to assuage bystanders' apprehensions, whereas mistrust in manufacturers' data handling practices may lead to heightened concerns [64].

Intersectionality. Differences across gender, immigration status, and socioeconomic status influenced the degree of bystander privacy concerns. For example, a domestic worker with precarious immigration status may be exploited by their employer, including as a target of smart home surveillance, with employers threatening to report workers to the police [6, 124].

6 RQ3: Proposed Design Solutions and Recommendations

Several solutions have been proposed in the literature to address the privacy concerns of bystanders; we classify these into three categories: *technical*, *social or educational*, and *legal.*

6.1 Technical Solutions

In this subsection, we systematize the technical solutions proposed and/or tested in the literature; 51 out of the 63 papers in our review made some kind of recommendations for technical design solutions. We classify the recommended solutions into three overall categories according to their primary goal, discussed below: (i) limiting data collection, (ii) increasing transparency, and (iii) enabling data and configuration controls.

Table 3 captures the types of proposed technical solutions, along with any limitations mentioned in the source papers. (For the most part, Table 3 aims to capture every type of proposed solution mentioned in our dataset of papers, but we left out a few that either were too vague, were tailored only to a very narrow situation, or were described by the authors as likely too problematic to be workable. Where the solution proposed in a given paper could fall into more than one category, we cited the paper in both places.) We also cross-reference these solutions in Table 2, mapping specific privacy concerns of bystanders to technical solutions that can mitigate them. Below we discuss each of the categories of solution; the following subsections discuss levels of industry uptake and some general limitations of these types of solutions.

Many of the solutions are suggested by authors based on the needs and preferences identified in qualitative or quantitative research with bystanders and secondary users.[6] However, in some cases, the research included participatory design exercises specifically to shape such suggestions [6, 34, 38, 39, 76, 137, 139]. On the other hand, some researchers have explicitly asked participants for feedback about potential protections, often synthesized from prior recommendations (ranging from short descriptions to elaborate graphical mock-ups) [26, 85, 88, 105, 121, 132]. Some designs have been prototyped and tested in academic research (or have seen industry uptake; see Section 6.2). Most such prototypes have been user-tested [6, 11, 42, 51, 133, 135, 137, 143, 148], but we include a few that have not [25, 65, 66, 144].

6.1.1 Proposals to Limit Data Collection.

Minimize Data Collection. One approach to safeguard privacy is reducing amount or granularity of data collection by smart home devices, following the principle of least privilege sensing [5, 26, 27, 84, 133]. This involves limiting the device access to only necessary data or data types, and consequently mitigates the concerns of bystanders who fear being surveilled/micromanaged and having their sensitive data or recordings shared. For example, audio devices in rented homes can be programmed to record only decibel levels instead of complete speech [84].

Limit Conditions for Data Collection/Recording. Using automatic recognition, security cameras inside the house can be programmed to start recording only if certain trigger sounds are detected like glass shattering or if certain events are detected like smoke or a stranger's face [84]. At the same time, voice and facial recognition could also be used in the opposite way, to *limit* collection of data about strangers or bystanders. Devices can be designed to filter the data collected by masking the voice or blurring the faces of unknown people [5, 7, 39, 75, 85, 105, 131], or discarding data about them entirely [7, 26, 37, 39, 75, 85, 93, 131, 139]. Other suggestions include limiting the field of view of cameras, AKA "privacy zones" [34, 39, 105, 130, 131, 139].

Guest Mode. Use of automatic recognition is one version of a common recommendation for "guest modes" that limit device activity or offer guests access [5, 11, 39, 56, 75, 85–87, 89, 93, 139]. Without requiring recognition, devices could limit data collection/storage at certain times [27, 93], or (for cameras) selectively block parts of the field of view [34, 139].

Generally, a guest mode may provide a balance between utility and privacy, enabling guests to utilize certain functions without gaining access to the full scope of device controls. Pierce et al. [105] sketched a design for a smart camera with separate guest mode to improve bystanders' privacy and trust. With this interactive version of a "guest mode," owners can share location and status of their smart cameras with visiting bystanders (like short-term tenants and domestic workers), enable them to turn off certain cameras or request they be disabled, and mask their faces and voices from appearing on the owner's mobile app for the camera.

Temporary Data Storage. More broadly, several studies have proposed that devices come pre-configured to delete recorded data after a certain time period (e.g., 2–3 days), or even as soon as the bystander leaves [10, 12, 25, 26, 39, 85, 131, 139]. This automatic deletion mechanism aims to prevent primary users from utilizing bystanders' data for prolonged periods, particularly in cases where bystanders themselves lack control over the devices and data collected through them.

[6] In general, insights in this article are drawn from research that specifically studies bystanders, not only primary users. However, as noted in Section 3, a couple of papers studied primary users only, but we included them because their goal includes bystander privacy. These latter types of research have been especially illuminating in surfacing potential limitations of common recommendations.

Privacy Nudges. In addition to limiting capabilities, devices could be designed to provide alerts or nudges during set-up about bystander privacy, for example, suggesting the primary user block views of sensitive areas like a bedroom [124] or a neighbor's property [105, 130, 131]. These nudges can aid in limiting data collection. Nudges could also suggest implementing other features [43, 56, 93, 124, 142] such as allowing limited access to device features [28] or alerting and seeking consent from other household members and potential bystanders [26, 93, 124, 142].

Conventional Device Controls. In cases where hubs or devices with voice assistants are used to control other home devices (e.g., smart lights), old-fashioned physical controls for those devices should be maintained so bystanders are not forced to interact with the assistant to accomplish basic actions such as turning lights on and off [2, 56, 75, 124, 142]. The provision of such conventional controls will prevent bystanders leaving a data footprint.

6.1.2 Proposals to Increase Transparency. A recurring concern voiced by people when in the role of bystanders is the lack of awareness regarding when and how smart home devices are collecting their data.

Visual/Auditory/Haptic Cues. Research has proposed that devices come with clearer recording status indicators. Devices could add or improve visual indicators (including LED and blinking lights), auditory cues, and/or haptic indicators (e.g., vibration) for when devices start or stop recording [5, 8, 26, 39, 76, 85–87, 105, 124–126, 132, 142, 145]. For example, Ahmad et al. [2] suggested using indicators to clearly distinguish between when cameras (and all their sensors) are deactivated vs. when they are merely in standby mode, with some sensors still operational. Albayaydh and Flechais [5–7] also recommend using consistent signs and symbols in smart homes to convey presence and data collection capabilities of the devices to nearby people, with attention to ease of interpretation of those signals by different populations. (For more recommendations about signage, see Section 6.4.)

Smart Home Dashboards. Smart home dashboards—which display complete information about the smart devices deployed in a home, their working/recording status, and the kind of data they are collecting—can significantly enhance comfort and privacy for bystanders, allowing them to take precautions where possible [42, 51, 84, 85, 132, 135, 137]. Such dashboards would enable them to be aware of the data collection practices in their environment and take necessary precautions where possible. For example, Windl et al. [135] developed physical and digital dashboards that display the devices present in a smart house to any bystanders, and evaluated these dashboards with eight households in the wild. These dashboards should ideally be open source to enhance transparency and user trust [137]. Such dashboards can significantly alleviate the concerns of bystanders regarding having limited awareness of device data collection practices.

Device Display Apps. Researchers have also proposed smart phone apps that could detect smart devices present in a home, for example, when a visitor connects to the home Wi-Fi, using information supplied by the device [5, 6, 8, 12, 39, 42, 51, 66, 76, 85, 86, 88, 105, 132, 137, 139, 142–145]. Such apps may provide users and visitors with information about connected smart devices, their data collection practices, and access patterns. They could also provide channels to find more information about smart home privacy in general (including privacy rights), as well as the information about specific devices [6] (see Section 6.4).

For example, Escher et al. [51] developed a smartphone app that offers transparency to bystanders about nearby audiovisual IoT devices and their data handling practices. It utilizes Bluetooth Low Energy beacons on these devices to transmit information, including device's recording channel, type, name, data retention time, third-party involvement, trigger/wake word usage, and encryption status. (Designs have also been proposed for camera-detection apps that can identify smart cameras, their functioning status, and the collected data (e.g., [39, 86, 105, 139]), even when primary users hide the devices and devices do not reveal themselves, as well as apps or other technologies that could be used by bystanders to jam or interfere with data collection (e.g., [2, 105, 131]). However, we do not cover these in detail in Section 6.1 and Table 3 as they are not recommendations for the design of the smart home devices themselves.)

6.1.3 Proposals to Enable Data and Configuration Controls.

Separate Profiles. A commonly proposed solution is the separation of profiles for guests and for different household members [7, 10, 34, 43, 44, 56, 64, 75, 76, 84, 105, 137, 142–144]. Such profiles can be created for those bystanders who visit a given smart home frequently or for longer duration (for example, Airbnb guests and care workers like nannies). Segregated profiles will ensure that sensitive bystander data, including recordings, cannot be accessed by the primary user without the bystander's permission. Moreover, separate profiles with robust voice recognition systems can also serve to protect the privacy of live-in bystanders in multi-user smart home environment [10, 56, 64, 75, 93]. In certain cases, a tunable guest profile can also provide limited access control and authority to a bystander (see below).

Separate profiles could even be automatically generated on detection of unfamiliar voices [76]—though the detection process presents its own privacy concerns. Such profiles could address the fears of bystanders who feel that they have limited control over their collected data or are at the risk of being spied on/surveilled (particularly in the case of domestic violence victims [76]). Separate profiles or accounts for children would allow parents to turn over data and control when the children are older [56, 75].

Multimodal Access to Privacy Settings. Koshy et al. [70] suggest making privacy mechanisms accessible in multiple interfaces, so phone apps are not required. They note how such interfaces could be limited by tunable access control options (see below) to provide access to controls relevant to bystanders without compromising primary users' privacy. Physical dashboards (see Section 6.1.2) are one option for app-less access [85].

Tangible Privacy Controls. In addition to indicators like lights and beeps (see Section 6.1.2), devices could include tangible privacy controls such as buttons/switches, lens-lids, and camera shutters that also serve as reliable indicators [2, 86, 105, 121, 131, 137]. Since currently, smart home video monitoring and data collection still present ambiguities for users and bystanders, Ahmad et al. [2] proposed using such tangible mechanisms to definitively indicate whether the camera has been turned off. The study also emphasized the need for further research to identify tangible mechanisms that can unambiguously signal the recording status of smart microphones. Pierce et al. [105] developed a detailed design for a smart camera that clearly signals its recording status to nearby individuals, including bystanders, by incorporating an electromagnetic lens-lid that operates similarly to a remote-controlled webcam cover. The design worked with visual and auditory indicators to provide feedback regarding the camera's operational state.

Tunable Access Control Options. To serve both live-in and visiting bystanders, Zeng and Roesner [143] developed a prototype application for Samsung SmartThings devices that provides role-based access control (including remote access) for live-in bystanders and location-based access control for visitors (like guests and domestic workers) when they are inside the house. Under these access control mechanisms, device owners can grant bystanders the ability to turn a device on/off, change its recording status, and be notified when another user changes the device state. They suggest that such a complex mechanism is most likely to be useful in low-trust situations. On the other hand, Bernd et al. [28] suggest that settings that provide limited access to device features can allow childcare workers like nannies and babysitters to access camera feeds to monitor children, and Słupska et al. [124] note domestic workers might need to prove what happened while they were in the house. Complex access control could even be used so the *owner* can intentionally limit their own access to data, for example, in short-term rentals [25, 65, 144]—or could provide a structure for limiting owners' access in IPV cases [125, 126].

Authenticated Permission. Moreover, verification mechanisms can be implemented for bystanders to have greater control over their data [38, 75, 144]. For instance, camera feed access for a certain time frame might need biometric approval (e.g., via facial ID) from all household members present in the house during that time [5, 76]. To offset unequal control of devices in patriarchal families, Chidziwisano and Jalakasi [38] suggested requiring distinct fingerprints from both wife and husband, with notifications sent to the phones of both for transparent authentication. Such approaches ensure all household members and bystanders are aware of access and help reduce concerns about unauthorized use.

Communication and Negotiation Apps. Researchers have also proposed negotiation apps that allow primary users and bystanders in a given context to compare their privacy preferences and collaborate in setting device preferences [6, 11, 12, 87, 88, 131, 139, 148]. For example, when an individual visits a smart home as a bystander and connects to the home Wi-Fi, such an app could inform them if any data collection practices in that home do not match the bystander's predetermined preferences [11, 88]. Preferences for notification and negotiation may be set by the user for specific data practices, or through use of privacy-preference prediction models [88]. The bystander can then verbally communicate with the primary user or send relevant notifications through the app about diverging preferences. The primary user may or may not choose to disable such data collection afterwards. Apps may also use automated negotiation protocols to propose a compromise solution [148].

Tangible Personal Controller. Rodriguez et al. [42] developed a prototype gadget "PriKey" that not only lets device owners grant access to other users and bystanders to know which smart devices are present in a room and what data they are collecting (through audio, video, and proximity sensors) through a dashboard, but also allows them to disable any of these sensors.

6.2 Industry Uptake of Proposed Technical Solutions

We reviewed video- and audio-based devices from major smart home product manufacturers, such as Google, Amazon, Apple, Ezviz, Wyze, SimpliSafe, and Yale to study the industry uptake of bystander privacy features proposed in the literature. We focused on smart cameras, smart speakers, and smart doorbells from these companies, since these devices raise the most significant bystander privacy concerns in our review. We also looked for any device awareness or smart home dashboard solutions offered by these companies. We reviewed the company Web pages since we did not have access to the devices themselves. We summarize our findings in Table 4. Notably, we found that a number of smart home devices, particularly smart cameras and speakers, now feature *visual and auditory* like LED indicators and beep reminders. Therefore, we have not included them in the table, as these basic features are exceedingly common.

Among the solutions proposed in literature, the most notable uptake is smart home manufacturers *limiting conditions for data collection/recording*. Amazon Blink and Ring cameras and doorbells now include "Privacy zones" to block camera monitoring and recording in areas specified as off-limits by the users, for example, a neighbor's front door [114]. These zones appear as black rectangles in

Table 4. Features Implemented by Major Smart Home Product Manufacturers That Can Help Address Bystander Privacy Needs

Device Types	Smart Home Device	Design Suggestions Implemented
Smart Camera	SimpliSafe SimpliCam	*Tangible Privacy Controls* [122]: An automated shutter ensures privacy and links to the security system, closing by default in Off or Home mode and opening automatically in Away mode. Primary users can close it for guest privacy as required.
	Amazon Blink Cam	*Limit Conditions for Data Collection/Recording* [30]: Up to two Privacy Zones can be set to block camera recording in specific areas according to user's preferences. *Temporary Data Storage* [31]: Photo capture clips are stored in the cloud for up to 60 days (30 days in the EU and UK), then automatically deleted.
	Amazon Ring Indoor Cam/Spotlight Cam Pro	*Tangible Privacy Controls* [112]: Enable users to deactivate their cam and mic by utilizing a manual Privacy Cover. This can be achieved by simply swiveling the lid to another side. *Limit Conditions for Data Collection/Recording* [113]: Users can set Privacy Zones to block the camera from recording or monitoring certain areas, for example, to preserve a neighbor's privacy.
	Ezviz Smart Camera	*Limit Conditions for Data Collection/Recording* [53]: Offers a Sleep Mode which halts all camera functions.
	Arlo Essential Indoor Camera	*Tangible Privacy Controls* [24]: The camera comes with a tangible privacy shield that can cover the camera lens for added privacy and protection.
Smart Doorbell (with Camera)	Amazon Blink Doorbell	*Limit Conditions for Data Collection/Recording* [30]: Up to two Privacy Zones can be set to block camera recording in specific areas according to user's preferences. *Temporary Data Storage* [31]: Photo capture clips are stored in the cloud for up to 60 days (30 days in the EU and UK) then automatically deleted.
	Amazon Ring Doorbell	*Limit Conditions for Data Collection/Recording* [114]: Utilize privacy zones to obscure specific areas from Live View or video recording, like a neighbor's apartment door.
	Ezviz Doorbell	*Limit Conditions for Data Collection/Recording* [52]: User can establish non-recording zones to ensure that filming occurs only when suitable and permissible.
Smart Speaker	Amazon Echo Dot/Show	*Tangible Privacy Controls* [15]: Constructed with various privacy layers, featuring a button to deactivate the mic/cam and an integrated cover to shield/close the camera. *Tangible Privacy Controls* [16]: User can swipe the tangible toggle to turn on/off the mic/cam. *Temporary Data Storage* [14]: User can manually or ask Alexa to remove the voice recordings, request histories, or have them automatically deleted after 3 or 18 months on an ongoing basis. *Minimize Data Collection* [17]: The device only captures the Wake word and responds accordingly, ensuring it doesn't listen to or record users' personal conversations.
	Apple HomePod/Mini	*Separate Profiles* [20, 21]: Can recognize up to six family members' voices, setting separate profiles and providing personalized services accordingly. *Minimize Data Collection* [20]: When users and/or bystanders ask HomePod something, their request gets linked to a random identifier instead of their Apple ID. *Minimize Data Collection* [22]: Siri listens for certain wake words ("Siri" or "Hey Siri") so recordings are not sent out of the house until the wake word is detected.
	Google Nest/Home Speaker	*Guest Mode* [59]: Users can turn on Guest Mode to ensure that their interactions with the Assistant, including all voice queries, are not stored to their Google account, or used to personalize their experience/recommendations. Anyone interacting with the device can turn the Guest Mode on or off through a simple voice command. *Temporary Data Storage* [58]: Audio recordings made by users are not stored by default, and users have the ability to delete them whenever they choose. *Tangible Privacy Controls* [57]: To manually disable the microphones, slide the mic switch on the back until the orange indicator is visible. *Limit Conditions for Data Collection/Recording* [60]: When inactive the speaker does not transmit voice recordings to Google or any third party.

the Ring app and video. Smart speakers from Amazon, Google Home, and Apple only record based on certain wake words [17, 22, 60].

Another notable feature implemented by Google is the *guest mode*. When activated, Google Home smart speakers do not store Google Assistant activity in the user account, and anyone can activate the guest mode using the simple voice command: "Hey Google, turn on Guest Mode" [59]. This reduces the burden on users to configure the settings, as suggested in recent work [11]. However, this feature is not available in all languages and countries. Similarly, *separate profiles* have been implemented in Google Home, Amazon Echo, and Apple HomePod devices.

Several devices also maintain *conventional device controls*, which can also function as *tangible privacy controls*, such as Google Home Speaker contains a mic switch: Flipping the switch cuts off the mic on a hardware level—adding a sense of privacy—and displays an orange indicator that makes it easy for anyone (including bystanders) to know that the mic is disconnected. Amazon Echo devices and Ring Indoor Camera also adopt similar tangible mechanism to disable camera and microphone [112]. Amazon Echo Show devices, Arlo's Indoor Camera, and SimpliCam come with a built-in physical shutter to cover the camera [15, 24, 122].

Further, *temporary data storage* has been implemented by various manufacturers. For example, Amazon blink camera limits photo capture clips storage for up to 60 days in the cloud (30 days in the EU and UK), after which they are automatically deleted. Amazon has introduced Alexa Smart Properties for Hospitality (for hotels, guest houses, and holiday properties), Senior Living (for the elderly, their caregivers, and their families), Healthcare (for patients in healthcare and their caregivers), and Residential (for residential buildings and communities) [74].

In addition to adopting *conventional controls*, and *tangible privacy controls*, Alexa for Residential allows users to delete their recordings manually or deletes them automatically 24 hours [13]. Furthermore, the property staff, manager, or smart home provider cannot listen to these recordings if the user links their own account to the device.

We did not find uptake of several of the other recommendations proposed in the literature. Notably, mechanisms for device awareness (for example, device detection apps and smart home dashboards), privacy nudges and negotiation mechanisms, and data access control mechanisms (such as tunable access control and authenticated permission) have currently not been adopted by the industry, leaving a significant gap in uptake of features that can address bystander privacy needs.

6.3 Limitations of Proposed Technical Solutions

Table 3 notes limitations of technical solutions recommended in the research literature in detail; here we discuss some common issues.

Compatibility. Solutions like smart home dashboards are not necessarily intended to be device-specific, but we note that they pose the challenge of compatibility across different manufacturers[7]; they can also pose potential security issues [25, 42, 51, 85, 132, 139]. Compatibility may also be an issue for apps that display device information or help negotiate preferences, if they rely on information transmitted by the device itself [6, 148]. At the same time, we note that some solutions that would be implemented at the level of individual devices, such as status indicators, would require consistency across manufacturers if they are to be understood.

Accessibility and Usability. Making complex bystander privacy designs accessible for bystanders with sensory or mobility impairments is an ongoing challenge (e.g., [105, 145]). Even for secondary

[7] The Matter standard is an open source connectivity protocol developed by the Connectivity Standards Alliance (formerly the Zigbee Alliance) to enhance interoperability among smart home devices from different manufacturers [90]; such efforts may mitigate these issues in future.

users or bystanders who simply aren't as familiar with smart home technology, usability can be an issue (e.g., [7, 64, 85, 124, 132, 143]), and usability friction may deter even tech-savvy primary users from choosing a bystander-friendly setup (e.g., [143]). Researchers looking at the intersection of smart homes and IPV have noted that, if someone has generally been shut out of controlling the smart home, they are likely to have particular trouble revising the privacy and security setup under stress [10, 76].

Balancing Stakeholder Preferences. It would be difficult to balance the privacy and utility of different stakeholders with some of these design solutions. In some cases, privacy designs may risk interfering with function [5, 7, 11, 12, 39, 70, 85, 87, 130, 133, 138, 139, 143], for example, limiting a security camera's facial recognition (e.g., [5]) or preventing it from sensing at all, if someone forgets to remove a lens lid [121]. Generally, defining what data is "necessary" for a device's function is already a source of privacy conflict between manufacturers and owners. We note that this gets even more complicated when bystanders are involved, as what seems unnecessary to a bystander may feel necessary to the primary user. Furthermore, several of the designs require significant commitment by device owners to set up, and/or assume a cooperative relationship (e.g., [70, 85, 137, 139, 143, 144]). Yao et al. [139] point out that such protections are more likely be adopted if they offer obvious benefits to owners as well.

Conflicts and Power. When devices are used for monitoring, conflicts may become more explicit (e.g., [5, 7, 42, 84, 85, 105, 139]). For example, it would be difficult to decide what information to share with short-term tenants through privacy dashboards in a way that prevents them from misusing this information to break house rules [84]. Manufacturers have some incentive to allow for smoother sharing of device control with secondary users in multi-user households. However, in situations with more power imbalance between primary users and bystanders or surveillance targets, if there are conflicting preferences, companies are likely to focus on their primary customers (e.g., [105]). And as Alshehri et al. [10] note with reference to privacy labels, the customers most likely to abuse smart devices are probably the least likely to choose products with bystander privacy protections.

Privacy Solutions May Incur New Privacy Problems. Designs intended to support bystander privacy may cause new hazards, due to the data they need to operate. For example, recognition-based privacy features may require devices to generate (at least temporarily) models of bystanders' faces or voices [5–7, 131]. Apps that allow bystanders to view information about or communicate with others' devices link those devices to the bystander's phone [42, 132]. Allowing bystanders to view logs of access to their data in turn generates a trace of them accessing the log [10, 125, 126].

Protecting bystanders is therefore a matter of tradeoffs even for the bystander (not just bystander vs. owner). Where they can choose, bystanders may need to consider what their strongest concerns are in a given context, e.g., whether they are more concerned about the device owner vs. the manufacturer accessing their data or knowing what protective actions they've taken.

Technical Solutions Are Not Enough. Because many of the described technical solutions are, in the end, up to the device owner (to implement via settings, or to allow by their choice of device brand), many researchers have suggested that technical solutions alone may not be sufficient to address limitations arising from conflicting stakeholder needs and potential power imbalances. They should be supplemented by education (of both primary users and bystanders), social interventions to support respectful norms, regulation or guidelines from authorities (e.g., nanny agencies, Airbnb), and—to allow for recourse if other measures are not effective—legislation to prevent abuse of smart home technology. These types of recommended solutions are covered in the following subsections.

6.4 Educational and Social Solutions

Educational and social solutions were proposed in 26 papers to complement the technical solutions and help address the privacy needs of bystanders. These solutions vary by the point of intervention and the entity responsible for implementing the solution. Broadly, three points of intervention have been proposed in the literature for educational and social solutions: government and NGOs, online platforms (e.g., for short-term rentals), smart home product vendors (manufacturers or retailers), and recruitment agencies that facilitate the hiring of domestic workers.

Several papers propose general awareness mechanisms and campaigns to raise awareness about the potential privacy violations in a smart home setting, as awareness is crucial for facilitating privacy-related discussions and resolving conflicts in scenarios involving asymmetric power dynamics [5–8, 64, 86, 125]. Similarly, education and information for device owners is important as well; even those who want to protect bystander privacy often don't have the understanding to do so [130]. Marky et al. [86] propose short TV commercials or poster advertisements as an awareness raising mechanism. Albayaydh and Flechais [7, 8] propose that government and NGOs collaborate to conduct awareness campaigns. In addition, they propose developing information booklets on potential privacy violations for users, and guidance materials for domestic worker recruitment agencies on improving privacy practices, which should be available in multiple languages and tailored to cultural frameworks of the target audience [7, 8].

Słupska et al. [124] prototype an online digital security and privacy guide for domestic workers that can be used by organizations that protect the rights of migrant workers, such as Voice of Domestic Workers in the UK [123]. Along similar lines, Albayaydh and Flechais [5, 6] propose establishing a privacy advice channel to serve as a platform for workers and household members to seek guidance on privacy matters, discuss best practices, and offer opportunities to report autocratic practices and privacy violations. Stephenson et al. [125] propose information resources that could help victims of intimate partner abuse specifically with IoT-based abuse or surveillance.

Wang et al. [134] and Park et al. [98] highlight potential improvements for short-term rental platforms like Airbnb, suggesting that they develop mechanisms to facilitate privacy negotiations, and educate tenants to set preferences during booking. These authors, along with Mare et al. [84], also suggest Airbnb hosts should disclose data practices related to smart devices, not just the presence of the devices, and that Airbnb should implement guidelines or standardized templates (e.g., privacy labels) for smart home devices to inform tenants about data handling practices.

Marky and coauthors [85–87] propose that vendors employ QR codes or security labels (similar to nutrition labels in groceries) to communicate what data is collected and with what frequency (following prior work on IoT privacy labels generally, e.g., [36, 49, 50, 54]). Although labels have the advantage that they do not require modification of the device itself, the authors note several shortcomings, such as that visitors do not have access to the packaging. Even if the labels are implemented on the devices themselves, the visitors may not notice them or have trouble correctly understanding the information displayed by them. Further, it is questionable whether the owners would deploy such QR codes since it may interfere with aesthetics of the space [85]. Such labels might be more effective in temporary residency scenarios, where the QR codes might be noticed by the visitors, and the owners can display physical signs next to the devices, providing the tenants an option to opt-out from these devices [84, 139]; however, verifiability is a challenge [84]. Alshehri et al. [10] and Stephenson et al. [125] propose that such labels should not only list device capabilities, but also include safety features, such as guides to support services, to mitigate tech facilitated abuse. However, they note that abusers may choose to not buy devices with such safety features.

Vendors can also help improve user mental models—for instance, tutorials during the voice profile set-up phase can help improve user mental models on privacy and data sharing practices

[64]. Researchers have also suggested that smart speakers be set up to answer questions about their own privacy features [75, 93, 132]. Benton et al. [26] suggest direct education by vendors in cases where smart home systems are deployed *en masse*, for example, in low-income housing—along with noting how landlords could involve tenants in the process of choosing systems.

Albayaydh and Flechais [5–7] propose domestic worker recruitment agencies can help by informing and educating workers about privacy risks in smart homes, obtaining worker's consent through job contracts, and facilitating negotiations between workers and households to mitigate power imbalances.

6.5 Legal Solutions and Regulatory Reforms

Suggestions for regulatory reforms to protect bystander privacy, both legal and industrial, tend to be less detailed in the relevant literature. However, 11 papers made suggestions, including introduction of design guidelines for camera product teams (like adding options for turning off recordings) [28], introducing reforms to ensure that restraining orders against domestic abusers account for surveillance or violations carried out through smart home devices [10, 125, 126], and legislation for work contracts to account for privacy rights of workers in smart homes (including regulating or banning covert surveillance devices and clarifying routes for restitution) [5, 8, 124].

Albayaydh and Flechais propose innovative legislation is required to hold household members accountable for their utilization of user data and establish guidelines for obtaining informed user consent [5], including channels for reporting violations [6]. However, they also note that current regulation is quite patchy and inconsistent between countries, suggesting that a coordinated effort between governments may be needed to make compliance easier for businesses [7]. Alshehri et al. [10] and Stephenson et al. [125] suggest support services should be continuously trained on emerging technologies so that they can effectively combat smart home-facilitated abuse.

Despres et al. [43] emphasized the need for policymakers from both WEIRD and non-WERID countries to regulate smart home device companies, for example, by requiring transparent data handling practices like privacy nutrition labels. Chiang et al. [37] suggested establishing specific legal frameworks for smart homes to protect incidental users in vulnerable situations from being pressured into accepting unfair data collection practices. They also recommended that policymakers modify right-to-delete laws to cover bystanders, but simplified to avoid cumbersome processes.

Overall, all of the recommendations mentioned in Section 6 reflect efforts to strike a balance between smart home functionality and the privacy concerns of bystanders. They aim to empower both users and bystanders in a given smart home with greater control over data access and usage, ultimately fostering a more privacy-conscious smart home environment.

7 RQ4: Research Gaps

Based on our systematic review, in this section we outline recommendations for study design that should be incorporated by future research in this field, as well as new avenues for future research that are currently unexplored or understudied in the literature.

7.1 Recommendations for Study Design

In this subsection, we discuss recommendations for improving study designs for future research works studying or addressing bystander privacy. These recommendations highlight the considerations researchers should take into account when selecting the participant pool for studies, in light of our systematic review.

Consider Intersectionality. We noted in Section 5.2 that intersectionality is one of the factors influencing smart home bystander privacy concerns. For example, Bernd et al. [28] conducted a study with female nannies in the US (in which they did not ask about immigration status), finding that participants were mainly concerned about employer monitoring. In contrast, Słupska et al. [124] found that female migrant domestic workers in the UK were concerned about government surveillance, scams and harassment, and employer monitoring, in that order. These findings show that intersecting characteristics like gender, job type, immigration status, and country of residence could lead to a unique set of concerns. Hence, future work should consider intersectionality of demographic, geographic, and other characteristics when studying concerns and perceived threat groups, to design better solutions.

Study Bystanders in Non-WEIRD Countries and the Global South. As we noted in Section 3, 29 out of the 39 studies in our dataset that specify populations were conducted only in countries in the Global North, particularly the US, Germany, and the UK, creating a biased body of knowledge, as well as limiting the generalizability of research findings and feasibility of suggested solutions. We believe that people in non-WEIRD countries and understudied geographic regions may have differing views and concerns with regard to smart home bystander privacy, for example, due to differences in culture and religion. This is reinforced by a few studies conducted in non-WEIRD countries. For example, Albayaydh and Flechais [5, 6, 8] found that female domestic workers in Jordan who wear Hijab expressed a heightened discomfort with cameras because they might capture them without their Hijab. Research with bystanders residing in understudied geographic regions will be especially beneficial to manufacturers like Google and Amazon that have a considerable market for their products across the world.

Involve Multiple Stakeholder Groups. Some of the papers in our dataset explored how privacy perspectives differ between stakeholder groups. For example, researchers have compared views of primary users with those of visitors [12, 85, 87, 93], or of primary vs. secondary users within households (e.g., [56, 70, 75, 81, 133]). Other studies compared views of Airbnb hosts and guests [84]and of domestic workers and employers of domestic workers [8, 29]. These two-sides studies were particularly effective at surfacing sources of conflict and identifying disconnects between the privacy expectations and assumptions of each side about the other.

Studies have also included other stakeholders like worker advocacy organizations [5, 124] and service providers for victim-survivors of IPV [125], which helped the researchers develop a fuller picture of what type of protections are *needed*, and have included policymakers and technology developers [5–7] to help the researchers develop a fuller picture of what type of protections are most *feasible*.

We anticipate that future work comparing different smart home stakeholder groups will produce new insights that can be used to design both technical solutions and social or sociotechnical solutions, including negotiation mechanisms, to balance conflicting needs and concerns in shared spaces.

7.2 Future Research Directions

In this subsection, we identify opportunities for future research, dividing them into two categories: studies on bystander needs and concerns, and developing and evaluating solutions for bystander privacy. These directions highlight areas where current research is thin or lacking, necessitating further investigation by the academic community to comprehensively address bystander privacy.

7.2.1 Studies on Bystander Needs and Concerns.

Consider Bystander Relationships to Homes and Device Owners. Although prior work has explored privacy perspectives of smart home bystanders defined by their relationship to the home and the device owners/primary users, as we described in Section 4.2, more work needs to be done, especially with bystanders in potentially vulnerable situations. For example, prior work (e.g., [5, 8, 39, 124]) has not generally distinguished between different types of domestic workers, with the exception of childcare workers [28, 29, 67, 68], and none has compared different domestic roles. However, different types of domestic work may lead to varying experiences and concerns due to differences in social prestige and opportunities to build relationships with employers. For example, elder-care work is less prestigious, less well-paid, and more often government- or agency-managed than childcare. Meanwhile, unlike care workers, housecleaners, gardeners, and maintenance people move amongst many homes and may have less mutual personal accountability and less opportunity—or need—to build mutual trust with employers. Future work could explore how smart home monitoring is viewed in these different types of relationships.

As another example, bystanders in hostile or severely power-imbalanced households, from general patriarchal structures to clear situations of abuse such as IPV, have unique privacy concerns. They therefore may need safety mechanisms that aren't relevant for most smart home situations, e.g., means to revoke abusers' control of devices [10, 76, 125, 126], or even to facilitate access to support services. The growing body of literature about smart home surveillance in abusive or controlling relationships often highlights the particular challenge in designing safety features when, paradoxically, many of those features could be used against a target of surveillance or abuse, for example, better logging of data access actions or changes to settings [10, 125, 126].

More research is needed to understand how smart home companies should build safety features given these constraints. Focus groups and participatory design workshops involving IPV survivors, building on the co-design work of Leitão [76]. Beyond academic research, several papers in our dataset suggest smart home designers need to learn more about considerations for at-risk or vulnerable groups [5, 10, 28, 38, 126], enabling them to develop better privacy and security protections for such populations—which may in turn aid other groups of bystanders.

Develop New Privacy Scales. The recent development of a psychometric scale to measure how much an individual values other people's privacy [61] is a significant step toward understanding people's views on the privacy of others. However, the works reviewed in this article show that there is a wide range of privacy concerns, influencing factors, and potential solutions specific to bystander privacy in smart homes. This may warrant developing novel privacy scales that account for any potential specific constructs in this domain, from the point of view of bystanders and of those responsible for the devices. Research has shown that even when there are general scales, having domain-specific ones can add constructs and key domain-specific considerations (e.g., [63]). For example, such new privacy scales would be useful for large-scale survey studies measuring concerns of smart home bystanders across different countries and contexts.

7.2.2 Developing and Evaluating Solutions for Bystander Privacy.

Evaluate Deployed Bystander Privacy Features and Solutions. As we noted in Section 6.1, some of the proposed design solutions, such as guest modes and restricting camera field-of-view (privacy zones), have seen industry uptake, and have been deployed for some time. However, we did not come across many studies evaluating users' and bystanders' real-world experiences with these features. Exceptions include Tabassum and Lipford [130], who found that some smart home owners wanted to use controls to protect bystanders' privacy, but were concerned about effects on functionality. Recommendations of Ahmad et al. [2] for tangible privacy signals and controls were based in part on bystander interviewees' dissatisfaction with current status indicators and controls.

Similar additional studies would be crucial to understanding how well the proposed solutions work in practice, how various stakeholders in smart homes manage the privacy-utility tradeoff, and where improvements to solutions are required. In particular, research is needed on how solutions work for people in vulnerable or power-imbalanced situations (see Section 6.3); for example, research on IPV in smart homes has noted how usability issues with privacy and security settings can impede victims' ability to protect themselves [10, 76, 125]. Such studies might also uncover barriers to adoption of these features, such as lack of awareness, that highlight where social and regulatory solutions should complement development and deployment of technical solutions.

Meanwhile, smart homes are getting smarter, as continuous advances in AI expand systems' capabilities (e.g., Amazon aims to use generative AI to allow Alexa to infer intents, like turning up the temperature if someone says "I'm cold" [33]). In addition, **trigger-action platforms (TAPs)** amplify surveillance risks to bystanders by allowing users to create rules that trigger automatic actions based on specific conditions, such as the presence of certain individuals or devices, often implemented using **"If This, Then That" (IFTTT)** logic. Cobb et al. [40] analyzed IFTTT rules set by primary users and found evidence of rules that pose such surveillance risks. For example, the rule "If [name] presence detected, then create Journal entry" explicitly tracks a specific individual using timestamped log entries. Motion alert rules on outdoor cameras could indirectly expose neighbors' daily routines. While prior research has primarily examined privacy and security concerns from the perspective of primary users, including mention of their concerns about bystanders' privacy [40, 110, 117], no studies have yet directly studied bystanders to understand their specific concerns about TAPs, nor how TAPs could be designed to better protect bystanders' privacy.

Future work will need flexible approaches to evaluating bystander privacy as device capabilities change, in particular how these changes affect the applicability and efficaciousness of privacy designs currently in use. In addition to suggesting specific solutions, some papers in our dataset extracted design dimensions or general sets of criteria for smart home device designs to protect bystander privacy [10, 27, 85, 126, 132, 138, 139, 145]. Along with our framework, such criteria could inform flexible evaluation rubrics for bystander privacy designs in commercial products.

Study Educational and Social Interventions for Improving Bystander Privacy. Many papers in our dataset argue that educational and social solutions will be essential to adoption of smart home bystander privacy measures. However, few studies have actually developed and tested such solutions, with the exception of prototype online digital security and privacy guide of Słupska et al. [124] for migrant domestic workers in the UK, and resources included in the device detection and negotiation app of Albayaydh and Flechais [6] for domestic workers in Jordan. Future studies should explore additional awareness campaigns to inform both primary users and bystanders about bystanders' privacy risks and how they can be mitigated, and assess their effectiveness in driving adoption of bystander privacy features. Further, longitudinal studies could study the effects of such interventions over time.

Explore Privacy Practices of Smart Home Product Teams and Study Feasibility of Design Recommendations. While quite a number of design solutions have been proposed in academic literature, the smart home industry does not necessarily implement many of them, especially sociotechnical solutions like privacy nudges and negotiation mechanisms. There is also little empirical research involving smart home product teams to explore how or whether they think about privacy in multiuser smart homes; how they design for different stakeholders; and their views on the feasibility of solutions for addressing bystander privacy. Further, most studies in our dataset that evaluated a prototype solution [except 6] tested it with device owners and/or bystanders, without input from smart home developers. Therefore, future research should incorporate empirical user studies such as in-depth interviews with smart home product team members, to understand and inform industry practices.

8 Discussion

Our work presents a systematic review of literature to date on bystander privacy concerns and solutions to address these concerns. First, we define and classify smart home bystanders according to both their role relative to the devices and their relationship with the devices' owners/primary users (RQ1). These classifications are essential for understanding the nuances of privacy concerns that arise in different contexts, as different bystander groups (such as household members, visitors, or domestic workers) may have distinct privacy expectations and experiences. Having a nuanced categorization of bystanders is an important step forward, as it serves as a foundation for addressing a diverse range of privacy concerns.

Next, we systematize the privacy concerns of these groups and the factors influencing the degree of concerns (RQ2), such as cultural context, power dynamics, and trust. By highlighting these factors, our work emphasizes the complexity of designing privacy solutions that are sensitive to the unique needs and risks faced by different bystander groups.

We then categorize the technical, social, educational, and legal solutions suggested by the academic literature to address smart home bystander privacy concerns, providing a holistic view of how the privacy challenges can be addressed (RQ3). Importantly, we accompany these solutions with a discussion of their limitations, giving both researchers and product developers a clearer sense of what might be feasible given different resource constraints, and which specific concerns are effectively addressable by a given solution.

Finally, our work identifies several opportunities for strengthening study designs, including by considering intersectionality and studying bystanders in non-WEIRD countries, along with avenues for future research, including designing privacy scales for smart homes, studying smart home product teams' views and practices on bystander privacy, and studying experiences of bystanders with currently deployed privacy features (RQ4).

Our systematization is captured in a set of frameworks that categorize prior work in these dimensions, as represented in Figure 2 and Tables 1–3. These frameworks, along with the outline of gaps in research to date, can serve as a blueprint that can be used by our community to inform future research, and by smart home device manufacturers and product teams to guide smart home device design and development to improve bystander privacy. Smart home device manufacturers and product teams can use our framework to better support bystanders in the design and development of their products, potentially in combination with the design criteria proposed in some papers (e.g., [10, 27, 85, 126, 132, 138, 139, 145]). For example, although our frameworks do not replace direct engagement with smart home bystanders, and we advocate for such engagement to design solutions that are bystander-centric, some smart home device manufacturers may not be able to conduct empirical research with bystanders to inform the design of their products due to limited resources. Some may also not be equipped with the knowledge and expertise needed to conduct ethical and non-extractive research with at-risk bystander groups like IPV survivors. Further, some bystander groups may be difficult to recruit and establish trust with, such as migrant domestic workers, especially if they are undocumented [124].

Therefore, our frameworks offer a blueprint that captures the privacy concerns of different bystander groups (see Table 2), which smart home device manufacturers can use to guide them when designing products and privacy features. For example, manufacturers designing products specifically for bystanders in hostile environments like domestic workers living with an abusive employer can prioritize solutions to address or mitigate the privacy concerns of this bystander group over the concerns of other bystander groups like family members or short-term rental tenants living in less hostile environments. Further, Table 3 provides a wide range of technical design solutions and their limitations based on our systematic review of the academic literature. Manufacturers can decide which solutions are feasible to implement based on the resources available and challenges that they may face when implementing a specific solution.

9 Conclusion

In conclusion, this systematic review provides a valuable resource for both future research and for smart home device manufacturers, emphasizing the importance of addressing diverse bystander privacy needs in product design. By incorporating the perspectives of diverse bystander groups, manufacturers can develop more inclusive and effective privacy solutions. We also advocate for future research to address gaps in the diversity of studied populations, particularly in regions where cultural and regional practices influence privacy perceptions. Furthermore, we highlight the need for more empirical evaluations of privacy design solutions, encouraging feedback from real-world users to assess the practicality and effectiveness of interventions—an area currently underexplored in the literature.

Acknowledgments

We are grateful also to Franziska Roesner and Alisa Frik for ideas and suggestions, and to Shafay Kashif for his contributions in documenting the methods and populations of the dataset. The article has benefited from the comments and interesting questions of audience members at the USENIX Symposium on Privacy Engineering and Respect (PEPR) 2023, and from the suggestions of anonymous reviewers for ACM CHI and for *TOCHI*.

References

[1] Noura Abdi, Xiao Zhan, Kopo Ramokapane, and Jose Such. 2021. Privacy norms for smart home personal assistants. In *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI)*, 558:1–558:14.

[2] Imtiaz Ahmad, Rosta Farzan, Apu Kapadia, and Adam J. Lee. 2020. Tangible privacy: Towards user-centric sensor designs for bystander privacy. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW2 (2020), 1–28.

[3] Iftikhar Alam, Shah Khusro, and Muhammad Naeem. 2017. A review of smart TV: Past, present, and future. In *Proceedings of the 2017 International Conference on Open Source Systems and Technologies (ICOSST)*. IEEE, 35–41.

[4] Ahlam Alami, Laila Benhlima, and Slimane Bah. 2015. An overview of privacy preserving techniques in smart home wireless sensor networks. *In Proceedings of the 2015 10th International Conference on Intelligent Systems: Theories and Applications (SITA)*, 1–4. DOI: https://doi.org/10.1109/SITA.2015.7358409

[5] Wael Albayaydh and Ivan Flechais. 2023. Examining power dynamics and user privacy in smart technology use among Jordanian households. In *Proceedings of the 32nd USENIX Security Symposium (USENIX Security '23)*. USENIX Association, Anaheim, CA, 4643–4659. Retrieved from https://www.usenix.org/conference/usenixsecurity23/presentation/albayaydh

[6] Wael Albayaydh and Ivan Flechais. 2024. Co-designing a mobile app for bystander privacy protection in Jordanian smart homes: A step towards addressing a complex privacy landscape. In *33rd USENIX Security Symposium (USENIX Security 24)*. USENIX Association, Philadelphia, PA, 4963–4980. Retrieved from https://www.usenix.org/conference/usenixsecurity24/presentation/albayaydh

[7] Wael Albayaydh and Ivan Flechais. 2024. "Innovative technologies or invasive technologies?": Exploring design challenges of privacy protection with smart home in Jordan. *Proceedings of the ACM on Human-Computer Interaction* 8, CSCW1 (2024), 1–54.

[8] Wael S. Albayaydh and Ivan Flechais. 2022. Exploring bystanders' privacy concerns with smart homes in Jordan. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing (CHI '22)*. ACM, New York, NY, 1–24. DOI: https://doi.org/10.1145/3491102.3502097

[9] Abdulrhman Alorini, Abdullah Bin Sawad, Sultan Alharbi, Kiran Ijaz, Mukesh Prasad, and A. Baki Kocaballi. 2024. Understanding privacy in smart speakers: A narrative review. In *Proceedings of the Australasian Conference on Information Security and Privacy*. Springer, 143–157.

[10] Ahmed Alshehri, Malek, Ben Salem, and Lei Ding. 2020. Are smart home devices abandoning IPV victims? In *Proceedings of the 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. IEEE, Los Alamitos, CA. DOI: https://doi.org/10.1109/trustcom50675.2020.00184

[11] Ahmed Alshehri, Eugin Pahk, Joseph Spielman, Jacob T. Parker, Benjamin Gilbert, and Chuan Yue. 2023. Exploring the negotiation behaviors of owners and bystanders over data practices of smart home devices. In *Proceedings of the*

2023 CHI Conference on Human Factors in Computing Systems (CHI '23). ACM, New York, NY, Article 67, 27 pages. DOI: https://doi.org/10.1145/3544548.3581360

[12] Ahmed Alshehri, Joseph Spielman, Amiya Prasad, and Chuan Yue. 2022. Exploring the privacy concerns of bystanders in smart homes from the perspectives of both owners and bystanders. In *Proceedings on Privacy Enhancing Technologies Symposium*, 99–119. DOI: https://doi.org/10.56553/popets-2022-0064

[13] Amazon. 2023. A4R Move-In FAQs. Retrieved December 12, 2023 from https://www.amazon.com/alexaresidential/faq

[14] Amazon. 2023. Designed to Protect Your Privacy. Retrieved December 7, 2023 from https://www.amazon.co.uk/b/?node=17084411031

[15] Amazon. 2023. Echo Show 10 (3rd Generation): HD Smart Display with Motion and Alexa. Retrieved December 7, 2023 from https://www.amazon.co.uk/all-new-echo-show-10-hd-smart-display-with-motion-and-alexa-charcoal/dp/B084P3KP2R

[16] Amazon. 2023. Echo Show 5 (3rd Generation) I Smart Display and Alarm Clock with Clearer Sound I Cloud Blue. Retrieved December 7, 2023 from https://www.amazon.co.uk/echo-show-5-3rd-gen/dp/B09B2RV31Z

[17] Amazon. 2023. How Alexa Works: Wake Word. Retrieved December 7, 2023 from https://www.amazon.co.uk/b/?node=21350175031

[18] Mohsen Amiribesheli, Asma Benmansour, and Hamid Bouchachia. 2015. A review of smart homes in healthcare. *Journal of Ambient Intelligence and Humanized Computing* 6, 4 (Mar. 2015), 495–517. DOI: https://doi.org/10.1007/s12652-015-0270-2

[19] Valentina Andries and Judy Robertson. 2023. Alexa doesn't have that many feelings: Children's understanding of AI through interactions with smart speakers in their homes. *Computers and Education: Artificial Intelligence* 5 (2023), 100176. DOI: https://doi.org/10.1016/j.caeai.2023.100176

[20] Apple. 2023. HomePod Mini. Retrieved December 7, 2023 from https://www.apple.com/uk/homepod-mini/

[21] Apple. 2023. Share Control of Your Home. Retrieved December 7, 2023 from https://support.apple.com/en-gb/HT208709

[22] Apple. 2023. HomePod Mini. Retrieved December 12, 2023 from https://www.apple.com/homepod-mini/

[23] Noah Apthorpe, Sarah Varghese, and Nick Feamster. 2019. Evaluating the contextual integrity of privacy regulation: Parents' IoT toy privacy norms versus COPPA. In *Proceedings of the 28th USENIX Security Symposium (USENIX Security '19)*, 123–140. Retrieved from https://www.usenix.org/conference/usenixsecurity19/presentation/apthorpe

[24] Arlo. 2023. Essential Indoor Wired Security Camera. Retrieved December 12, 2023 from https://www.arlo.com/en-us/cameras/essential/arlo-essential-indoor.html

[25] Yechan Bae, Sarbartha Banerjee, Sangho Lee, and Marcus Peinado. 2024. Spacelord: Private and secure smart space sharing. *Digital Threats: Research and Practice* 5, 2, Article 14 (June 2024), 1–27. DOI: https://doi.org/10.1145/3637879

[26] Laura Benton, Asimina Vasalou, and Sarah Turner. 2023. Location, location, security? Exploring location-based smart device security concerns and mitigations within low-rent homes. In *Proceedings of the 2023 ACM Designing Interactive Systems Conference (DIS '23)*. ACM, New York, NY, 1060–1077. DOI: https://doi.org/10.1145/3563657.3596077

[27] Arne Berger, Albrecht Kurze, Andreas Bischof, Jesse Josua Benjamin, Richmond Y. Wong, and Nick Merrill. 2023. Accidentally evil: On questionable values in smart home co-design. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23)*. ACM, New York, NY, Article 629, 14 pages. DOI: https://doi.org/10.1145/3544548.3581504

[28] Julia Bernd, Ruba Abu-Salma, Junghyun Choy, and Alisa Frik. 2022. Balancing power dynamics in smart homes: Nannies' perspectives on how cameras reflect and affect relationships. In *Proceedings of the 18th Symposium on Usable Privacy and Security (SOUPS '22)*. USENIX Association, Boston, MA, 687–706.

[29] Julia Bernd, Ruba Abu-Salma, and Alisa Frik. 2020. Bystanders' privacy: The perspectives of nannies on smart home surveillance. In *Proceedings of the 10th USENIX Workshop on Free and Open Communications on the Internet (FOCI '20)*. USENIX Association. Retrieved from https://www.usenix.org/conference/foci20/presentation/bernd

[30] Blink. 2023. How to Set Up Privacy Zones. Retrieved December 7, 2023 from https://support.blinkforhome.com/en_US/camera-settings/how-to-configure-privacy-zones

[31] Blink. 2023. Photo Capture FAQ. Retrieved December 7, 2023 from https://support.blinkforhome.com/en_US/using-your-camera/photo-capture-faq

[32] David Buil-Gil, Steven Kemp, Stefanie Kuenzel, Lynne Coventry, Sameh Zakhary, Daniel Tilley, and James Nicholson. 2023. The digital harms of smart home devices: A systematic literature review. *Computers in Human Behavior* 145 (2023), 107770. DOI: https://doi.org/10.1016/j.chb.2023.107770

[33] Melissa Cha. 2023. Introducing a New Era for the Alexa Smart Home. Retrieved December 11, 2023 from https://www.aboutamazon.com/news/devices/amazon-smart-home-announcements-2023

[34] George Chalhoub, Martin J. Kraemer, and Ivan Flechais. 2024. Useful shortcuts: Using design heuristics for consent and permission in smart home devices. *International Journal of Human-Computer Studies* 182 (2024), 103177.

[35] Bing Chen, Yaping Liu, Shuo Zhang, Jie Chen, and Zhiyu Han. 2021. A survey on smart home privacy data protection technology. In *Proceedings of the 2021 IEEE 6th International Conference on Data Science in Cyberspace (DSC)*. IEEE, 583–590.

[36] Claire, C. Chen, Dillon Shu, Hamsini Ravishankar, Xinran Li, Yuvraj Agarwal, and Lorrie Faith Cranor. 2024. Is a trustmark and QR code enough? The effect of IoT security and privacy label information complexity on consumer comprehension and behavior. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems (CHI '24)*. ACM, New York, NY, Article 832. DOI: https://doi.org/10.1145/3613904.3642011

[37] Yi-Shyuan Chiang, Omar Khan, Adam Bates, and Camille Cobb. 2024. More than just informed: The importance of consent facets in smart homes. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, 1–21.

[38] George Hope Chidziwisano and Maureen Jalakasi. 2023. Understanding women's perspectives on smart home security systems in patriarchal societies of Malawi. In *Proceedings of the 2023 ACM Designing Interactive Systems Conference*, 1078–1092.

[39] Camille Cobb, Sruti Bhagavatula, Kalil Anderson Garrett, Alison Hoffman, Varun Rao, and Lujo Bauer. 2020. "I would have to evaluate their objections": Privacy tensions between smart home device owners and incidental users. In *Proceedings on Privacy Enhancing Technologies Symposium*, 54–75. DOI: https://doi.org/10.2478/popets-2021-0060

[40] Camille Cobb, Milijana Surbatovich, Anna Kawakami, Mahmood Sharif, Lujo Bauer, Anupam Das, and Limin Jia. 2020. How risky are real users' IFTTT applets? In *Proceedings of the 16th Symposium on Usable Privacy and Security (SOUPS '20)*. USENIX Association, 505–529. Retrieved from https://www.usenix.org/conference/soups2020/presentation/cobb

[41] Jessamyn Dahmen, Diane Cook, Xiaobo Wang, and Wang Honglei. 2017. Smart secure homes: A survey of smart home technologies that sense, assess, and respond to security threats. *Journal of Reliable Intelligent Environments* 3, 2 (Aug. 2017), 83–98. DOI: https://doi.org/10.1007/s40860-017-0035-0

[42] Sarah Delgado Rodriguez, Sarah Prange, Christina Vergara Ossenberg, Markus Henkel, Florian Alt, and Karola Marky. 2022. PriKey—Investigating tangible privacy control for smart home inhabitants and visitors. In *Proceedings of the Nordic Human-Computer Interaction Conference (NordiCHI '22)*. ACM, New York, NY, Article 74, 13 pages. DOI: https://doi.org/10.1145/3546155.3546640

[43] Tess Despres, Marcelino Ayala Constantino, Naomi Zacarias Lizola, Gerardo Sánchez Romero, Shijing He, Xiao Zhan, Noura Abdi, Ruba Abu-Salma, Jose Such, and Julia Bernd. 2024. "My best friend's husband sees and knows everything": A cross-contextual and cross-country approach to understanding smart home privacy. *Proceedings on Privacy Enhancing Technologies* 2024, 4 (2024), 413–449. Retrieved from https://petsymposium.org/popets/2024/popets-2024-0124.php

[44] Frank Ebbers and Murat Karaboga. 2022. Influencing factors for users' privacy and security protection behavior in smart speakers: Insights from a Swiss user study. In *Proceedings of the European Symposium on Research in Computer Security*. Springer, 195–211.

[45] Jide Edu, Jose Such, and Guillermo Suarez-Tangil. 2020. Smart home personal assistants: A security and privacy review. *ACM Computing Surveys* 53, 6 (2020), 1–36.

[46] Nils Ehrenberg. 2024. Smart home technologies: Convenience and control. In *Humane Autonomous Technology: Re-Thinking Experience with and in Intelligent Systems*. Rebekah Rousi, Catharina von Koskull, and VirpiRoto (Eds.), Springer International Publishing, Cham, 181–198. DOI: https://doi.org/10.1007/978-3-031-66528-8_8

[47] Nils Ehrenberg and Turkka Keinonen. 2021. Co-living as a rental home experience: Smart home technologies and autonomy. *Interaction Design and Architecture(s)* 50 (2021), 82–101.

[48] Nils Ehrenberg and Turkka Keinonen. 2021. The technology is enemy for me at the moment: How smart home technologies assert control beyond intent. In *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI '21)*. ACM, New York, NY, Article 407. DOI: https://doi.org/10.1145/3411764.3445058

[49] Pardis Emami-Naeini, Yuvraj Agarwal, Lorrie Faith Cranor, and Hanan Hibshi. 2020. Ask the experts: What should be on an IoT privacy and security label? In *Proceedings of the IEEE Symposium on Security and Privacy (SP)*, 771–788. DOI: https://doi.org/10.1109/SP40000.2020.00043

[50] Pardis Emami-Naeini and Janarth Dheenadhayalan, Yuvraj Agarwal, and lorrie Faith Cranor. 2022. An informative security and privacy "nutrition" label for Internet of Things devices. *IEEE Security & Privacy* 20, 2 (2022), 31–39. DOI: https://doi.org/10.1109/MSEC.2021.3132398

[51] Stephan Escher, Katrin Etzrodt, Benjamin Weller, Stefan Köpsell, and Thorsten Strufe. 2022. Transparency for bystanders in IoT regarding audiovisual recordings. In *Proceedings of the 2022 IEEE International Conference on Pervasive Computing and Communications Workshops and Other Affiliated Events (PerCom Workshops)*, 649–654. DOI: https://doi.org/10.1109/PerComWorkshops53856.2022.9767212

[52] Ezviz. 2023. DB2-B Pro Battery-Powered Video Doorbell Kit. Retrieved December 7, 2023 from https://www.ezviz.com/product/DB2-B-Pro/44386

[53] Ezviz. 2023. Ezviz CB1 Wi-Fi Smart Home Battery Camera. Retrieved December 7, 2023 from https://www.ezviz.com/product/CB1/47474

[54] Yuanyuan Feng, Yaxing Yao, and Norman Sadeh. 2021. A design space for privacy choices: Towards meaningful privacy control in the Internet of Things. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 1–16.

[55] Vaibhav Garg, L. Jean Camp, Lesa L. Huber, Kalpana Shankar, and Kay Connelly 2014. Privacy concerns in assisted living technologies. *Annals of Telecommunications—Annales Des Télécommunications* 69 (2014), 75–88. Retrieved from https://api.semanticscholar.org/CorpusID:14437399

[56] Christine Geeng and Franziska Roesner. 2019. Who's in control? Interactions in multi-user smart homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing (CHI '19)*. ACM, New York, NY, 1–13. DOI: https://doi.org/10.1145/3290605.3300498

[57] Google. 2023. Control Your Smart Devices with Your Voice. Retrieved December 7, 2023 from https://store.google.com/gb/product/nest_audio?hl=en-GB#voice-control

[58] Google. 2023. Designed for Privacy. Retrieved December 7, 2023 from https://safety.google/intl/en_gb/assistant/#assistant-privacy-by-design

[59] Google. 2023. Hey Google, Tell Me about Guest Mode. Retrieved December 7, 2023 from https://safety.google/intl/en_gb/assistant/#guest-mode-section

[60] Google. 2023. Starts in Standby. Retrieved December 7, 2023 from https://safety.google/intl/en_gb/assistant/#assistant-standby-mode-new-assistant-copy

[61] Rakibul Hasan, Rebecca Weil, Rudolf Siegel, and Katharina Krombholz. 2023. A psychometric scale to measure individuals' value of other people's privacy (VOPP). In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, 1–14.

[62] Hussein Hazazi and Mohamed Shehab. 2023. Protect the gate: A literature review of the security and privacy concerns and mitigation strategies related to IoT smart locks. In *Internet of Things Security and Privacy: Practical and Management Perspectives*. Ali Ismail Awad, Atif Ahmad, Kim-Kwang Raymond Choo, and Saqib Hakak (Eds.), CRC Press, 146–164.

[63] Hsiao-Ying Huang, Soteris Demetriou, Muhammad Hassan, Güliz Seray Tuncay, Carl A. Gunter, and Masooda Bashir. 2023. Evaluating user behavior in smartphone security: A psychometric perspective. In *Proceedings of the 19th Symposium on Usable Privacy and Security (SOUPS '23)*. USENIX Association, Anaheim, CA, 509–524. Retrieved from https://www.usenix.org/conference/soups2023/presentation/huang

[64] Yue Huang, 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 2020 CHI Conference on Human Factors in Computing Systems (CHI '20)*. ACM, New York, NY, 1–13. DOI: https://doi.org/10.1145/3313831.3376529

[65] Md Nazmul Islam and Sandip Kundu. 2018. Poster abstract: Preserving IoT privacy in sharing economy via smart contract. In *Proceedings of the 2018 IEEE/ACM 3rd International Conference on Internet-of-Things Design and Implementation (IoTDI)*, 296–297. DOI: https://doi.org/10.1109/IoTDI.2018.00047

[66] Sashidhar Jakkamsetti, Youngil Kim, and Gene Tsudik. 2023. Caveat (IoT) emptor: Towards transparency of IoT device presence. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (CCS '23)*. ACM, New York, NY, 1347–1361. DOI: https://doi.org/10.1145/3576915.3623089

[67] Mark Johnson, Maggy Lee, Michael McCahill, and Ma Rosalyn Mesina. 2020. Beyond the 'all seeing eye': Filipino migrant domestic workers' contestation of care and control in Hong Kong. *Ethnos* 85, 2 (Mar. 2020), 276–292. DOI: https://doi.org/10.1080/00141844.2018.1545794

[68] Bei Ju, Xiao Yang, Xiao Hong Pu, and T. L. Sandel. 2024. (Re)making live-in or live-out choice: The lived experience of Filipina migrant domestic workers in Macao. *Gender, Place & Culture* 31, 12 (2024), 1713–1734.

[69] Mi Jeong Kim, Myoung Won Oh, Myung Eun Cho, Hyunsoo Lee, and Jeong Tai Kim. 2013. A critical review of user studies on healthy smart homes. *Indoor and Built Environment* 22, 1 (2013), 260–270. DOI: https://doi.org/10.1177/1420326X12469733

[70] Vinay Koshy, Joon Sung Sung Park, Ti-Chung Cheng, and Karrie Karahalios. 2021. "We just use what they give us": Understanding passenger user perspectives in smart homes. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21)*. ACM, New York, NY, 1–14. DOI: https://doi.org/10.1145/3411764.3445598

[71] Sandjar Kozubaev, Fernando Rochaix, Carl DiSalvo, Christopher, and A. Le Dantec. 2019. Spaces and traces: Implications of smart technology in public housing. In *Proceedings of the 2019 ACM CHI Conference on Human Factors in Computing Systems (CHI '19)*. ACM, New York, NY, 1–13. DOI: https://doi.org/10.1145/3290605.3300669

[72] Martin J. Kraemer, George Chalhoub, Helena Webb, and Ivan Flechais. 2023. "It becomes more of an abstract idea, this privacy"—Informing the design for communal privacy experiences in smart homes. *International Journal of Human-Computer Studies* 180 (2023), 103138. DOI: https://doi.org/10.1016/j.ijhcs.2023.103138

[73] Martin J. Kraemer, Ivan Flechais, and Helena Webb. 2019. Exploring communal technology use in the home. In *Proceedings of the Halfway to the Future Symposium 2019 (HTTF '19)*. ACM, New York, NY, Article 5, 8 pages. DOI: https://doi.org/10.1145/3363384.3363389

[74] Charles De Lamberterie. 1990. Alexa Smart Properties. Retrieved from https://developer.amazon.com/en-US/alexa/alexa-smart-properties

[75] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. 2018. Alexa, are you listening? Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW, Article 102 (Nov. 2018), 31 pages. DOI: https://doi.org/10.1145/3274371

[76] Roxanne Leitão. 2019. Anticipating smart home security and privacy threats with survivors of intimate partner abuse. In *Proceedings of the 2019 on Designing Interactive Systems Conference (DIS '19)*. ACM, New York, NY, 527–539. DOI: https://doi.org/10.1145/3322276.3322366

[77] Leigh Levinson, Christena Nippert-Eng, Randy Gomez, and Selma Sabanović. 2024. Snitches get unplugged: Adolescents' privacy concerns about robots in the home are relationally situated. In *Proceedings of the 2024 ACM/IEEE International Conference on Human-Robot Interaction (HRI '24)*. ACM, New York, NY, 423–432. DOI: https://doi.org/10.1145/3610977.3634946

[78] Wenda Li, Tan Yigitcanlar, Isil Erol, and Aaron Liu. 2021. Motivations, barriers and risks of smart home adoption: From systematic literature review to conceptual framework. *Energy Research & Social Science* 80 (2021), 102211.

[79] Wenda Li, Tan Yigitcanlar, Aaron Liu, and Isil Erol. 2022. Mapping two decades of smart home research: A systematic scientometric analysis. *Technological Forecasting and Social Change* 179 (2022), 121676. DOI: https://doi.org/10.1016/j.techfore.2022.121676

[80] Heather Richter Lipford, Madiha Tabassum, Paritosh Bahirat, Yaxing Yao, and Bart P. Knijnenburg. 2022. Privacy and the Internet of Things. In *Modern Socio-Technical Perspectives on Privacy*. Bart P. Knijnenburg, Xinru Page, Pamela Wisniewski, Heather Richter Lipford, Nicholas Proferes, and Jennifer Romano (Eds.), Springer, 233.

[81] Na Liu. 2024. CCTV cameras at home: Temporality experience of surveillance technology in family life. *New Media & Society* (2024), 21 pages. DOI: https://doi.org/10.1177/14614448241229175

[82] Guglielmo Maccario and Maurizio Naldi. 2023. Privacy in smart speakers: A systematic literature review. *Security and Privacy* 6, 1 (2023), e274. DOI: https://doi.org/10.1002/spy2.274

[83] Chenlu Mao and Danni Chang. 2023. Review of cross-device interaction for facilitating digital transformation in smart home context: A user-centric perspective. *Advanced Engineering Informatics* 57 (2023), 102087.

[84] Shrirang Mare, Franziska Roesner, and Tadayoshi Kohno. 2020. Smart devices in Airbnbs: Considering privacy and security for both guests and hosts. In *Proceedings on Privacy Enhancing Technologies Symposium*, 436–458.

[85] Karola Marky, Nina Gerber, Michelle Gabriela Pelzer, Mohamed Khamis, and Max Mühlhäuser. 2022. "You offer privacy like you offer tea": Investigating mechanisms for improving guest privacy in IoT-equipped households. In *Proceedings on Privacy Enhancing Technologies*, 400–420. DOI: https://doi.org/10.56553/popets-2022-0115

[86] Karola Marky, Sarah Prange, Florian Krell, Max Mühlhäuser, and Florian Alt. 2020. "You just can't know about everything": Privacy perceptions of smart home visitors. In *Proceedings of the 19th International Conference on Mobile and Ubiquitous Multimedia (MUM '20)*. ACM, New York, NY, 83–95. DOI: https://doi.org/10.1145/3428361.3428464

[87] Karola Marky, Sarah Prange, Max Mühlhäuser, and Florian Alt. 2022. Roles matter! Understanding differences in the privacy mental models of smart home visitors and residents. In *Proceedings of the 20th International Conference on Mobile and Ubiquitous Multimedia (MUM '21)*. ACM, New York, NY, 108–122. DOI: https://doi.org/10.1145/3490632.3490664

[88] Karola Marky, Alina Stöver, Sarah Prange, Kira Bleck, Paul Gerber, Verena Zimmermann, Florian Müller, Florian Alt, and Max Mühlhäuser. 2024. Decide yourself or delegate-user preferences regarding the autonomy of personal privacy assistants in private IoT-equipped environments. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, 1–20.

[89] Karola Marky, Alexandra Voit, Alina Stöver, Kai Kunze, Svenja Schröder, and Max Mühlhäuser. 2020. "I don't know how to protect myself": Understanding privacy perceptions resulting from the presence of bystanders in smart environments. In *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society (NordiCHI '20)*. ACM, New York, NY, 1–11. DOI: https://doi.org/10.1145/3419249.3420164

[90] matter-smarthome. 2024. Alexa Smart Properties. Retrieved from https://matter-smarthome.de/en/

[91] Dana McKay and Charlynn Miller. 2021. Standing in the way of control: A call to action to prevent abuse through better design of smart technologies. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21)*. ACM, New York, NY, Article 332. DOI: https://doi.org/10.1145/3411764.3445114

[92] Emily McReynolds, Sarah Hubbard, Timothy Lau, Aditya Saraf, Maya Cakmak, and Franziska Roesner. 2017. Toys that listen: A study of parents, children, and internet-connected toys. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, 5197–5207. DOI: https://doi.org/10.1145/3025453.3025735

[93] Nicole Meng, Dilara Keküllüoğlu, and Kami Vaniea. 2021. Owning and sharing: Privacy perceptions of smart speaker users. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW1, Article 45 (Apr. 2021), 29 pages. DOI: https://doi.org/10.1145/3449119

[94] Nicole Meng-Schneider, Rabia Yasa Kostas, Kami Vaniea, and Maria K. Wolters. 2023. Multi-user smart speakers—A narrative review of concerns and problematic interactions. In *Proceedings of the Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems (CHI EA '23)*. ACM, New York, NY, Article 213, 7 pages. DOI: https://doi.org/10.1145/3544549.3585689

[95] Ziarmal Nazar Mohammad, Fadi Farha, Adnan O. M. Abuassba, Shunkun Yang, and Fang Zhou. 2021. Access control and authorization in smart homes: A survey. *Tsinghua Science and Technology* 26, 6 (2021), 906–917.

[96] David Moher, Alessandro Liberati, Jennifer Tetzlaff, Douglas G. Altman, and PRISMA Group. 2009. Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *Annals of Internal Medicine* 151, 4 (2009), 264–269.

[97] Tamara Mujirishvili, Caterina Maidhof, Francisco Florez-Revuelta, Martina Ziefle, Miguel Richart-Martinez, and Julio Cabrero-García. 2023. Acceptance and privacy perceptions toward video-based active and assisted living technologies: Scoping review. *Journal of Medical Internet Research* 25, 1 (May 2023), e45297. DOI: https://doi.org/10.2196/45297

[98] Sunyup Park, Weijia He, Elmira Deldari, Pardis Emami-Naeini, Danny Yuxing Huang, Jessica Vitak, Yaxing Yao, and Michael Zimmer. 2024. Well-intended but half-hearted: Hosts' consideration of guests' privacy using smart devices on rental properties. In *Proceedings of the 20th Symposium on Usable Privacy and Security (SOUPS '24)*, 179–198.

[99] Nandita Pattnaik, Shujun Li, and Jason R. C. Nurse. 2024. Security and privacy perspectives of people living in shared home environments. *Proceedings of the ACM on Human-Computer Interaction* 8, CSCW2, Article 368 (Nov. 2024), 1–39. DOI: https://doi.org/10.1145/3686907

[100] Nandita Pattnaik, Shujun Li, Jason, and R. C. Nurse. 2023. A survey of user perspectives on security and privacy in a home networking environment. *ACM Computing Surveys* 55, 9, Article 180 (Jan. 2023), 38 pages. DOI: https://doi.org/10.1145/3558095

[101] Kirsten Peetoom, Monique Lexis, Manuela Joore, Carmen Dirksen, and Luc Witte. 2014. Literature review on monitoring technologies and their outcomes in independently living elderly people. *Disability and Rehabilitation. Assistive Technology* 10, 4 (Sept. 2014), 271–294. DOI: https://doi.org/10.3109/17483107.2014.961179

[102] Jessica Percy Campbell, Jacob Buchan, Charlene H. Chu, Andria Bianchi, Jesse Hoey, and Shehroz S. Khan. 2024. User perception of smart home surveillance among adults aged 50 years and older: Scoping review. *JMIR mHealth and uHealth* 12 (Feb. 2024), e48526. DOI: https://doi.org/10.2196/48526

[103] Jessica Percy-Campbell, 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 (2024), 304–324. DOI: https://doi.org/10.24908/ss.v22i3.16084

[104] Nada Y. Philip, Joel J. P. C. Rodrigues, Honggang Wang, Simon James Fong, and Jia Chen. 2021. Internet of Things for in-home health monitoring systems: Current advances, challenges and future directions. *IEEE Journal on Selected Areas in Communications* 39, 2 (2021), 300–310.

[105] James Pierce, Claire Weizenegger, Parag Nandi, Isha Agarwal, Gwenna Gram, Jade Hurrle, Hannah Liao, Betty Lo, Aaron Park, Aivy Phan, et al. 2022. Addressing adjacent actor privacy: Designing for bystanders, co-users, and surveilled subjects of smart home cameras. In *Proceedings of the Designing Interactive Systems Conference (DIS '22)*. ACM, New York, NY, 26–40. DOI: https://doi.org/10.1145/3532106.3535195

[106] Gayle Helane Doherty, Pireh Pirzada, Adriana Wilde, and David Harris-Birtill. 2022. Ethics and acceptance of smart homes for older adults. *Informatics for Health and Social Care* 47, 1 (2022), 10–37. DOI: https://doi.org/10.1080/17538157.2021.1923500

[107] Javad Pool, Saeed Akhlaghpour, Farhad Fatehi, and Leonard C. Gray. 2022. Data privacy concerns and use of telehealth in the aged care context: An integrative review and research agenda. *International Journal of Medical Informatics* 160 (Apr. 2022), 104707. DOI: https://doi.org/10.1016/j.ijmedinf.2022.104707

[108] Sarah Prange and Florian Alt. 2023. Increasing users' privacy awareness in the Internet of Things: Design space and sample scenarios. In *Human Factors in Privacy Research*. Nina Gerber, Alina Stöver, and Karola Marky (Eds.), Springer International Publishing, Cham, 321–336.

[109] Saida Hafsa Rafique, Amira Abdallah, and Khaled Shuaib. 2023. IoT-facilitated intimate partner abuse. In *Proceedings of the 2023 15th International Conference on Innovations in Information Technology (IIT)*, 190–195. DOI: https://doi.org/10.1109/IIT59782.2023.10366425

[110] Kopo Marvin Ramokapane, Caroline Bird, Awais Rashid, and Ruzanna Chitchyan. 2022. Privacy design strategies for home energy management systems (HEMS). In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (CHI '22)*. ACM, New York, NY, Article 405, 15 pages. DOI: https://doi.org/10.1145/3491102.3517515

[111] Olivia K. Richards. 2019. Family-centered exploration of the benefits and burdens of digital home assistants. In *Proceedings of the Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, 1–6.

[112] Ring. 2023. Indoor Camera. Retrieved December 11, 2023 from https://en-uk.ring.com/products/mini-indoor-security-camera-plug-in

[113] Ring. 2023. Ring Indoor Cam, 2nd Gen. Retrieved December 12, 2023 from https://ring.com/products/mini-indoor-security-camera-plug-in

[114] Ring Support Center. 2023. Understanding Privacy Zones. Retrieved August 25, 2023 from https://support.ring.com/hc/en-us/articles/360027979331-Understanding-Privacy-Zones

[115] Biljana Risteska Stojkoska and Kire Trivodaliev. 2017. A review of Internet of Things for smart home: Challenges and solutions. *Journal of Cleaner Production* 140 (Jan. 2017), 1454–1464. DOI: https://doi.org/10.1016/j.jclepro.2016.10.006

[116] Michaela M. Rogers, Colleen Fisher, Parveen Ali, Peter Allmark, and Lisa Fontes. 2023. Technology-facilitated abuse in intimate relationships: A scoping review. *Trauma, Violence & Abuse* 24, 4 (2023), 2210–2226. DOI: https://doi.org/10.1177/15248380221090218

[117] Piero Romare, Victor Morel, Farzaneh Karegar, and Simone Fischer-Hübner. 2023. Tapping into privacy: A study of user preferences and concerns on trigger-action platforms. In *Proceedings of the 2023 20th Annual International Conference on Privacy, Security and Trust (PST)*, 1–12. DOI: https://doi.org/10.1109/PST58708.2023.10320180

[118] William Seymour, Mark Cote, and Jose Such. 2023. Ignorance is bliss? The effect of explanations on perceptions of voice assistants. In *Proceedings of the PACM on Human-Computer Interaction—ACM Conference on Computer-Supported Cooperative Work and Social Computing (CSCW)*.

[119] William Seymour, Mark Coté, and Jose Such. 2023. Legal obligation and ethical best practice: Towards meaningful verbal consent for voice assistants. In *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI)*, 166:1–166:16.

[120] William Seymour, Xiao Zhan, Mark Cote, and Jose Such. 2023. A systematic review of ethical concerns with voice assistants. In *Proceedings of the 2023 AAAI/ACM Conference on AI, Ethics, and Society*, 131–145.

[121] Sujay Shalawadi, Christopher Getschmann, Niels van Berkel, and Florian Echtler. 2024. Manual, hybrid, and automatic privacy covers for smart home cameras. In *Proceedings of the 2024 ACM Designing Interactive Systems Conference*, 3453–3470.

[122] SimpliSafe. 2023. A Smart Home Security Camera Engineered to Protect. Retrieved December 7, 2023 from https://simplisafe.co.uk/simplicam-security-camera

[123] Julia Słupska, Marissa Begonia, Nayana Prakash, Selina Cho, Ruba Abu-Salma, Mallika Balakrishnan, and Natalie Sedacca. 2021. Digital Privacy & Security Guide for Migrant Domestic Workers. Technical Report. University of Oxford, King's College London, Voice of Domestic Workers, and Migrants Organise. Retrieved February 14, 2022 from https://domesticworkerprivacy.github.io/

[124] Julia Słupska, Selina Cho, Marissa Begonia, Ruba Abu-Salma, Nayanatara Prakash, and Mallika Balakrishnan. 2022. "They look at vulnerability and use that to abuse you": Participatory threat modelling with migrant domestic workers. In *Proceedings of the 31st USENIX Security Symposium (USENIX Security '22)*. USENIX Association, Boston, MA, 323–340. Retrieved from https://www.usenix.org/conference/usenixsecurity22/presentation/slupska-vulnerability

[125] Sophie Stephenson, Majed Almansoori, Pardis Emami-Naeini, and Rahul Chatterjee. 2023. "It's the equivalent of feeling like you're in jail": Lessons from firsthand and secondhand accounts of IoT-enabled intimate partner abuse. In *Proceedings of the 32nd USENIX Security Symposium (USENIX Security '23)*.

[126] Sophie Stephenson, Majed Almansoori, Pardis Emami-Naeini, Danny Yuxing Huang, and Rahul Chatterjee. 2023. Abuse vectors: A framework for conceptualizing IoT-enable interpersonal abuse. In *32nd USENIX Security Symposium (USENIX Security 23)*. USENIX Association, Anaheim, CA, 69–86. Retrieved from https://www.usenix.org/conference/usenixsecurity23/presentation/stephenson-vectors

[127] Yolande Strengers, Jathan Sadowski, Zhuying Li, Anna Shimshak, and Floyd Mueller. 2021. What can HCI learn from sexual consent? A feminist process of embodied consent for interactions with emerging technologies. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21)*. Pernille Bjørn and Steven Drucker (Eds.), ACM, New York, NY. DOI: https://doi.org/10.1145/3411764.3445107

[128] Kaiwen Sun, Yixin Zou, Jenny Radesky, Christopher Brooks, and Florian Schaub. 2021. Child safety in the smart home: Parents' perceptions, needs, and mitigation strategies. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW2 (Oct. 2021), 1–41. DOI: https://doi.org/10.1145/3479858

[129] Madiha Tabassum, 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 USENIX Conference on Usable Privacy and Security (SOUPS '19)*. USENIX Association, 435–450.

[130] Madiha Tabassum and Heather Lipford. 2023. Exploring privacy implications of awareness and control mechanisms in smart home devices. *Proceedings on Privacy Enhancing Technologies* 2023 (Jan. 2023), 571–588. DOI: https://doi.org/10.56553/popets-2023-0033

[131] Neilly H. Tan, Richmond Y. Wong, Audrey Desjardins, Sean A. Munson, and James Pierce. 2022. Monitoring pets, deterring intruders, and casually spying on neighbors: Everyday uses of smart home cameras. In *Proceedings of the ACM CHI Conference on Human Factors in Computing Systems*, 25.

[132] Parth Kirankumar Thakkar, Shijing He, Shiyu Xu, Danny Yuxing Huang, and Yaxing Yao. 2022. "It would probably turn into a social faux-pas": Users' and bystanders' preferences of privacy awareness mechanisms in smart homes. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (CHI '22)*. ACM, New York, NY, 1–13. DOI: https://doi.org/10.1145/3491102.3502137

[133] Blase Ur, Jaeyeon Jung, and Stuart Schechter. 2014. Intruders versus intrusiveness: Teens' and parents' perspectives on home-entryway surveillance. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '14)*. ACM, New York, NY, 129–139. DOI: https://doi.org/10.1145/2632048.2632107

[134] Zixin Wang, Danny Yuxing Huang, and Yaxing Yao. 2023. Exploring tenants' preferences of privacy negotiation in Airbnb. In *Proceedings of the 32nd USENIX Security Symposium (USENIX Security '23)*, 535–551.

[135] Maximiliane Windl, Alexander Hiesinger, Robin Welsch, Albrecht Schmidt, and Sebastian S. Feger. 2022. SaferHome: Interactive physical and digital smart home dashboards for communicating privacy assessments to owners and bystanders. *Proceedings of the ACM on Human-Computer Interaction* 6, ISS, Article 586 (Nov. 2022), 680–699. DOI: https://doi.org/10.1145/3567739

[136] Maximiliane Windl and Sven Mayer. 2022. The skewed privacy concerns of bystanders in smart environments. *Proceedings of the ACM on Human-Computer Interaction* 6 (Sept. 2022), 1–21. DOI: https://doi.org/10.1145/3546719

[137] Maximiliane Windl, Albrecht Schmidt, and Sebastian S. Feger. 2023. Investigating tangible privacy-preserving mechanisms for future smart homes. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23)*. ACM, New York, NY, Article 70, 16 pages. DOI: https://doi.org/10.1145/3544548.3581167

[138] Richmond Y. Wong, Jason Caleb Valdez, Ashten Alexander, Ariel Chiang, Olivia Quesada, and James Pierce. 2023. Broadening privacy and surveillance: Eliciting interconnected values with a scenarios workbook on smart home cameras. In *Proceedings of the 2023 ACM Designing Interactive Systems Conference (DIS '23)*. ACM, New York, NY, 1093–1113. DOI: https://doi.org/10.1145/3563657.3596012

[139] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata McDonough, and Yang Wang. 2019. Privacy perceptions and designs of bystanders in smart homes. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW Article 59 (2019), 24 pages. DOI: https://doi.org/10.1145/3359161

[140] Yuan Yao, Li Huang, Yi He, Zhijun Ma, Xuhai Xu, and Haipeng Mi. 2023. Reviewing and reflecting on smart home research from the human-centered perspective. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23)*. ACM, New York, NY, Article 143, 21 pages. DOI: https://doi.org/10.1145/3544548.3580842

[141] Kaja Fjørtoft Ystgaard, Luigi Atzori, David Palma, Poul Einar Heegaard, Lene Elisabeth Bertheussen, Magnus Rom Jensen, and Katrien De Moor. 2023. Review of the theory, principles, and design requirements of human-centric Internet of Things (IoT). *Journal of Ambient Intelligence and Humanized Computing* 14, 3 (2023), 2827–2859.

[142] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End user security and privacy concerns with smart homes. In *Proceedings of the 13th Symposium on Usable Privacy and Security (SOUPS '17)*. USENIX Association, Santa Clara, CA, 65–80. Retrieved from https://www.usenix.org/conference/soups2017/technical-sessions/presentation/zeng

[143] Eric Zeng and Franziska Roesner. 2019. Understanding and improving security and privacy in multi-user smart homes: A design exploration and in-home user study. In *Proceedings of the 28th USENIX Security Symposium (USENIX Security '19)*. USENIX Association, Santa Clara, CA, 159–176. Retrieved from https://www.usenix.org/conference/usenixsecurity19/presentation/zeng

[144] Han Zhang, Yuvraj Agarwal, and Matt Fredrikson. 2022. TEO: Ephemeral ownership for IoT devices to provide granular data control. In *Proceedings of the 20th Annual International Conference on Mobile Systems, Applications and Services (MobiSys '22)*. ACM, New York, NY, 302–315. DOI: https://doi.org/10.1145/3498361.3539774

[145] Yuhang Zhao, Yaxing Yao, Jiaru Fu, and Nihan Zhou. 2022. 'If sighted people know, I should be able to know:' Privacy perceptions of bystanders with visual impairments around camera-based technology. arXiv:2210.12232. Retrieved from https://arxiv.org/abs/2210.12232

[146] Serena Zheng, 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, Article 200 (Nov. 2018), 20 pages. DOI: https://doi.org/10.1145/3274469

[147] Bin Zhou, Wentao Li, K. W. Chan, Yijia Cao, Yonghong Kuang, Xi Liu, and Xiong Wang. 2016. Smart home energy management systems: Concept, configurations, and scheduling strategies. *Renewable and Sustainable Energy Reviews* 61 (Aug. 2016), 30–40. DOI: https://doi.org/10.1016/j.rser.2016.03.047

[148] Haozhe Zhou, Mayank Goel, and Yuvraj Agarwal. 2024. Bring privacy to the table: Interactive negotiation for privacy settings of shared sensing devices. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, 1–22.

Appendix

A Overview of Papers in Dataset

Table A1 describes some characteristics of the papers in the final dataset informing our framework:

- Paper Type:
  - Orig = Original research

- Byst = Included human subjects research with or from perspective of bystanders (unfilled circles involved scenarios with no perspective)
- Methods Employed:
  - Qual = Qualitative
  - Quant = Quantitative
  - Design = Developed and/or tested technical designs, or used design-based methods
- Content of Interest for Review:
  - Concern = Studied concerns of bystanders
  - TechRec = Included recommendations for design of technical solutions based on the research (author suggestions or participatory designs)
  - TechTest = Tested a design for a technical solution (feedback-gathering, prototypes, and so on)
  - OtherRec = Included social, educational, and/or regulatory recommendations based on the research

Table A1. Characteristics of Papers in the Dataset for This Systematic Review

Citation	Paper Type		Methods Employed			Content of Interest for Review			
	Orig	Byst	Qual	Quant	Design	Concern	TechRec	TechTest	OtherRec
Ahmad et al. [2]	●	●	●		●		●		
Albayaydh and Flechais [6]	●	●	●		●	●	●	●	●
Albayaydh and Flechais [7]	●	●	●			●	●		●
Albayaydh and Flechais [5]	●	●	●			●	●		●
Albayaydh and Flechais [8]	●	●	●			●	●		●
Alshehri et al. [10]					●	●	●		●
Alshehri et al. [11]	●	●	●	●	●	●	●	●	●
Alshehri et al. [12]	●	●	●	●		●	●		●
Bae et al. [25]	●				●			●	
Benton et al. [26]	●	●	●		●	●	●	●	●
Berger et al. [27]	●		●		●		●		●
Bernd et al. [28]	●	●	●			●	●		●
Bernd et al. [29]	●	●	●			●			
Chalhoub et al. [34]	●		●		●		●		
Chiang et al. [37]	●	○	●	●		●	●		●
Chidziwisano and Jalakasi [38]	●	●	●		●	●	●		●
Cobb et al. [39]	●	●	●	●	●	●	●		
Rodriguez [42]	●	●	●	●	●			●	
Despres et al. [43]	●	●	●	●		●	●		●
Ebbers and Karaboga [44]	●	●		●			●		
Ehrenberg and Keinonen [47]	●	●	●			●			
Ehrenberg and Keinonen [48]	●	●	●			●	●		
Escher et al. [51]	●	●	●		●	●	●	●	
Geeng and Roesner [56]	●	●	●			●	●		
Huang et al. [64]	●	●	●			●	●		●
Islam and Kundu [65]	●				●			●	
Jakkamsetti et al. [66]	●				●			●	
Johnson et al. [67]	●	●	●			●			
Ju et al. [68]	●	●	●			●			

(Continued)

Table A1. Continued

Citation	Paper Type		Methods Employed			Content of Interest for Review			
	Orig	Byst	Qual	Quant	Design	Concern	TechRec	TechTest	OtherRec
Koshy et al. [70]	●	●	●	●			●		
Kozubaev et al. [71]	●	●	●		●	●			
Lau et al. [75]	●	●	●			●	●		●
Leitão [76]	●	●	●		●	●	●		●
Liu [81]	●	●	●			●			
Mare et al. [84]	●	●	●	●		●	●		●
Marky et al. [85]	●	●	●	●	●	●		●	●
Marky et al. [86]	●	●	●			●	●		●
Marky et al. [87]	●	●	●			●	●		●
Marky et al. [88]	●	●		●	●	●	●	●	
Marky et al. [89]	●	●	●			●	●		●
Meng et al. [93]	●	●	●			●	●		●
Meng-Schneider et al. [94]			●			●			
Park et al. [98]	●		●						●
Pierce et al. [105]	●	○	●		●	●		●	
Shalawadi et al. [121]	●	●	●	●	●			●	
Słupska et al. [124]	●	●	●			●	●		●
Stephenson et al. [125]	●	●	●			●	●		●
Stephenson et al. [126]	●		●			●	●		●
Tabassum and Lipford [130]	●		●				●		●
Tan et al. [131]	●		●				●		●
Thakkar et al. [132]	●	●	●	●	●	●	●	●	●
Ur et al. [133]	●	●	●	●	●	●	●	●	
Wang et al. [134]	●	●	●	●		●			●
Windl et al. [135]	●	●	●	●	●		●	●	
Windl and Mayer [136]	●	●		●		●			
Windl et al. [137]	●	○	●		●		●	●	
Wong et al. [138]	●	○	●			●			
Yao et al. [139]	●	●	●		●	●	●		●
Zeng et al. [142]	●	●	●			●	●		
Zeng and Roesner [143]	●	●	●		●		●	●	●
Zhang et al. 144]	●				●			●	
Zhao et al. [145]	●	●	●	●		●	●		●
Zhou et al. [148]	●	●	●	●	●			●	

Received 15 May 2024; revised 6 March 2025; accepted 14 March 2025