Honda Research Institute EU
Honda Research Institute Europe GmbH
https://www.honda-ri.de/

Bystander Privacy Implications of Robots in Everyday Spaces: A Scoping Review

Manuel Dietrich, Alan Sarkisian, Thomas H Weisswange

2026

Preprint:

Copyright ACM 2026. This is the author's version of the work. It is posted here for your personal use. Not for redistribution. The definitive Version of Record was published in 2026 21st ACM/IEEE International Conference on Human-Robot Interaction (HRI), https://doi.org/10.1145/3757279.3785586.

Bystander Privacy Implications of Robots in Everyday Spaces: A Scoping Review

Manuel Dietrich
Honda Research Institute Europe GmbH
Offenbach, Germany
manuel.dietrich@honda-ri.de

Alan Sarkisian
Honda Research Institute Japan Co., Ltd.
Wako, Japan
alan.sarkisian@jp.honda-ri.com

Thomas H. Weisswange
Honda Research Institute Europe GmbH
Offenbach, Germany
thomas.weisswange@honda-ri.de

Abstract

The advancement of AI is driving the integration of robots into everyday environments. The acceptance of these robots not only depends on direct users, but also on others who share these spaces, often referred to as bystanders or non-users. A frequently discussed prerequisite for acceptance is the proper handling of personal information as robots are equipped with means for environmental awareness, data inference, and human interaction. Although bystanders are not the main target of such processing, they can be affected by robot operation. Despite its significance, bystander privacy concerns have received limited attention in prior robotics research.

In this paper, we address bystander privacy in the context of robots operating in everyday environments. We conduct a scoping review of bystander privacy issues associated with related technologies exhibiting agentic qualities comparable to robots. We analyze how agency may reshape conventional attributions of actor roles and transmission principles within the established privacy framework of Contextual Integrity. This allows us to derive transferable insights about privacy expectations as well as unique opportunities and open research issues for robots in public spaces.

CCS Concepts

• **Computer systems organization** → *Robotics*; • **Human-centered computing** → **HCI theory, concepts and models**; • **Security and privacy** → **Usability in security and privacy**.

Keywords

Privacy, Bystanders, Robotics, Review, Public Space, Privacy Enhancing Technologies

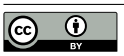
ACM Reference Format:
Manuel Dietrich, Alan Sarkisian, and Thomas H. Weisswange. 2026. Bystander Privacy Implications of Robots in Everyday Spaces: A Scoping Review. In *Proceedings of the 21st ACM/IEEE International Conference on Human-Robot Interaction (HRI '26), March 16–19, 2026, Edinburgh, Scotland, UK*. ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3757279.3785586

1 Introduction

The advancement of AI is accelerating the integration of service and assistant robots into everyday environments. This includes delivery robots moving through public roads [77], drones [48] in public airspace, or guide robots operating in settings with broad accessibility like offices [1] or museums [36]. In such settings, robots typically interact with or affect not only their owners or primary users but also other individuals, such as visitors, workers, or pedestrians ("Incidentally Copresent Persons" [58]). Traditionally, robots have been predominantly designed and evaluated with respect to the needs and expectations of single users. More recently, there have also been attempts to consider implications of deployments with multiple users or user groups [64, 72]. However, such robots might not be ready for the highly complex context of real world situations "in the wild" [37]. In particular, there is a need to take into account the implications and effects of technology deployment on bystanders [28, 33, 34, 51]. There has been some prior work considering bystander interaction in robotics. Fiedler [27] looked into the social impact and ethical implication of humanoid designs with specific features even in absence of any explicit user perspective. Other studies looked at bystander helping behaviors towards robots having problems [66, 76]. Bhat and Zhao [12] evaluated implications of delivery robots for bystanders with visual impairments. In social robot navigation, bystanders are treated as obstacles that robots must route around, while not stopping to engage in direct interactions [40, 69].

One particularly relevant topic in public spaces is privacy. Robots are equipped with many sensors and might be able to process personal information as part of their functionality. Bystanders, who find themselves within a robot's sensing range, might find such data processing problematic, yet they lack established means of intervention. There exist many classical data protection means for technology users, for example the use of consent forms, opt-in dialogues, or simply the decision to not interact with a device [26]. Potential privacy concerns of users in interaction with social robots have been discussed previously for private spaces [24, 30, 46, 60, 61], but also for semi-public environments such as elder care centers [31, 32]. Some aspects such as oversharing sensitive information due to established social bonds to the robot [49] are unique to robots and the user perspective. It has also been shown that the perceived impact on user privacy might be reduced if data is collected by an embodied agent as compared to an abstract sensor [15, 68]. Many of the privacy implications that come with the use of artificial intelligence [44] will likely also apply to robots. However, bystanders might have different problems and expectations and might require novel types of privacy enhancing technologies.

In the following, we will refer to this challenge as "bystander privacy". Bystander privacy is not a novel concern; it has emerged alongside other smart technologies embedded in everyday spaces,



This work is licensed under a Creative Commons Attribution 4.0 International License.
HRI '26, Edinburgh, Scotland, UK
© 2026 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-2128-1/2026/03
https://doi.org/10.1145/3757279.3785586

such as smart homes, remote-controlled drones, or smart glasses [24, 56]. However, the increasing deployment of robots in public and semi-public environments makes it relevant to assess bystander privacy implications for technology with higher agency. Robots can for example proactively initiate an interaction or use mobility to change their sensor range. Some of the previously discussed smart technologies nevertheless can be attributed with a subset of the aspects of agency and we therefore believe it to be relevant to assess this work with a robotics perspective to evaluate which insights might be transferable to better understand bystander privacy for robotics. Previous work has tried a similar transfer for regulatory means of sensing technology towards robots [62]. In this work, we want to look at three research questions:

RQ1: How is bystander privacy discussed for smart technology that demonstrate agent qualities similar to robots?

RQ2: Which insights about bystander privacy in smart technologies can be transferred to the new scenario?

RQ3: How can we generally conceptualize robots within informational flows considering their agentic nature?

The central contribution of this paper is **to provide an overview of bystander privacy expectations and design implications for robots, proposing an informational flow model adapted to agentic technologies.** In a recent perspective article, Reinhardt and Misra [59] examined the privacy implications of service robots, highlighting several open technical challenges related to bystanders. However, a principled overview and structured analysis of the broader space of bystander privacy in robotics has so far been lacking.

The paper is structured as follows: We begin by introducing Nissenbaum's framework of contextual integrity [53] alongside key concepts of technological agency. Next, we present our literature review of studies addressing bystander privacy in the context of smart and intelligent technologies. The findings are organized according to the parameters defined in Nissenbaum's information flow model, highlighting privacy concerns that specifically arise from the agentic nature of emerging technologies. Building on this analysis, we propose an extended interpretation of Nissenbaum's framework that incorporates agentic technologies in both sender and recipient roles, as well as a differentiation between agentic sensing, interpretation, and sharing. This extended model then helps us draw connections to the robot context, showing what we can learn from other technologies about people's expectations and how they deal with privacy concerns.

2 Concepts

2.1 Information Flow Model

To model and better understand data-handling practices involving technologies in everyday life, we draw on Helen Nissenbaum's concept of information flows within the framework of Contextual Integrity [53]. According to Nissenbaum, all practices involving the use of personal information can be described in terms of five parameters of an information flow:

1 Data subject (the person the information is about),
2 Sender (the entity transmitting the information),
3 Recipient (the entity receiving the information),
4 Data type, and
5 Transmission principle (the conditions under which the information is shared).

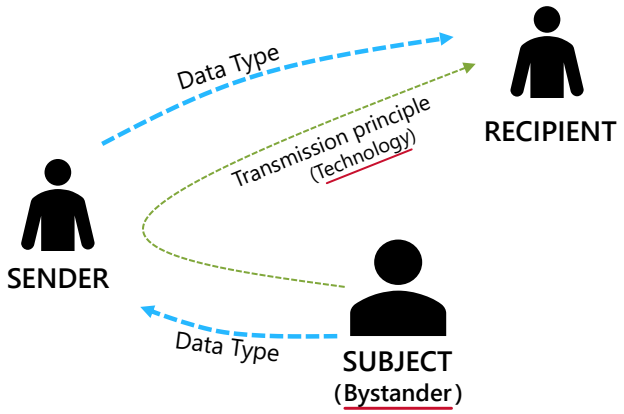


Figure 1: Bystanders and technologies positioned within the five parameters of the Information Flow.

Figure 1 illustrates the five parameters and their relations. The first three parameters—subject, sender, and recipient—form an "actors' triangle", and each must be described in their contextual role [53]. For example, in a medical consultation, the patient is the data subject who discloses symptoms to the doctor, who acts as the recipient. In a one-on-one case, the sender role may be negligible, or could be interpreted as also being assigned to the patient. If the doctor further consults with another doctor about the medical condition of the patient, the first doctor becomes a sender within a new flow. Data types refer to the kind of information collected of or used about a data subject. Finally, transmission principles specify the conditions or constraints under which the information is shared. This includes formal or interpersonal conditions such as "with consent," "required by law," or "in confidence," often in combination.

The concept of Information Flow was developed as a conceptual model to help experts, particularly in the legal domain, fully describe privacy norms and identify privacy violations. The concept should also enable laypersons to capture norms about information practices in semantically rich terms. For a practice to respect privacy, Nissenbaum argues that all five parameters must be considered and aligned with existing privacy norms [53].

Technology Implication on Transmission Principle. One of Nissenbaum's motivations has been to offer an effective framework for analyzing privacy impact arising from the use of emerging technologies [52, 54]. Within her account of information flows, technologies are conceptualized as factors that modify transmission principles [54].

For instance, Nissenbaum [54] discusses a U.S. court decision to publish court records online as a shift in the transmission principle relative to traditional, paper-based access in courthouses. From the perspective of a simplistic public/private dichotomy, one might claim that "nothing changed," because the records had always been public. Contextual Integrity, however, highlights the crucial difference: the ease, scale, and persistence enabled by digital access constitute an additional transmission condition, supplementing

existing ones such as "required by law" [54]. The framework is particularly powerful in identifying such critical transformations in information practices—changes that other approaches are likely to overlook.

Related arguments often arise regarding activities in public spaces: if anyone can observe what happens on the street, why be concerned when certain technologies such as smart glasses record it? Contextual Integrity again reveals a key shift. The transmission principle moves from ephemeral human observation to persistent technological recording, storage, and potential downstream dissemination.

Bystander as Data Subject. According to prior literature, bystander in the context of bystander privacy are characterized by their non-involvement in the primary activity occurring within a given space. A common *definition by negation* describes a bystander as "anyone who is not a primary user" [63, p. 8]. At the level of abstraction assumed by the information flow model, bystanders can be appropriately classified as data subjects, as anyone whose personal information is processed. The fact that the data associated with bystanders may arise only as a by-product of system operation, does not diminish their status as data subjects.

2.2 Agentic Technologies

In contrast to the technologies Nissenbaum discusses in her work so far, robots appear and behave as **agentic technologies**.

Defining agency in absolute terms has historically proven difficult [35]. A more practical approach is to consider whether a technology demonstrates agency relative to the chosen level of abstraction [29, 35]. As we discuss privacy concerns from the perspective of users and bystanders, the relevant level of abstraction is an external, behavior-focused view.

Within this view, Jackson and Williams argue that agency is characterized by autonomy, interactivity, and adaptability [35]. A system exhibits agency when it demonstrates these three qualities with respect to observable behavior at the user level of abstraction. **Autonomy** refers to the capacity of a system to act without being directly controlled or triggered by a human operator. This does not require complete independence, but rather the ability to initiate or sustain activity within defined boundaries. Concrete examples include drones that autonomously explore environments or automated vehicles that navigate traffic without continuous human intervention. Importantly, autonomy is not limited to mobile systems: static technologies, such as advanced smart speakers, may demonstrate autonomy by proactively taking initiative, for example, by issuing verbal interventions [71]. **Interactivity** describes the ability to respond to environmental stimuli. Such contingent behavior relies on perception capabilities, including environmental sensing to trigger a light switch in a smart home, human state estimation to enhance reality augmentation, or natural language understanding by a smart speaker. **Adaptability** captures the system's ability to adjust its future behavior based on experiences. This quality is often equated with learning and includes personalization mechanisms that modify responses or behavior over time as performed by AI assistants.

These forms of agency are all relevant to how we envision robots and to how they already appear in practice. When these dimensions

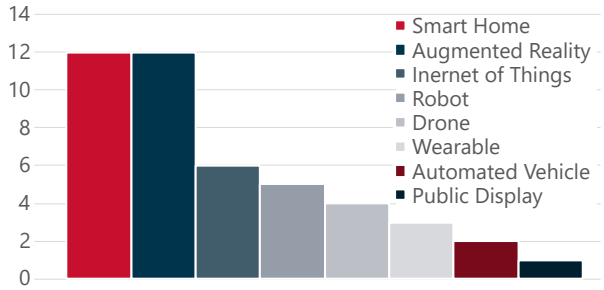


Figure 2: Statistics of technology types covered in the papers used for this review.

are decomposed into their constituent functional dimensions (e.g., mobility, sensing, natural language processing), it becomes evident that we already see many of these capabilities with existing "smart technologies". This indicates that privacy concerns discussed in the broader context of smart technologies could, at least in part, be transferable to robots. This perspective informs the scope of our literature search.

3 Literature Search

We approach RQ1 and RQ2 through a literature review of research articles published before February 2025, discussing bystander privacy in the context of smart or intelligent technologies attributed with agency qualities. As we were interested to include insights from a broad range of areas, we searched in title, abstract and keywords across the ACM Digital Library, IEEE Xplore and ScienceDirect databases using a combination of terms describing the three aspects of [<Bystander> AND <Agent> AND <Privacy>] (a full list of all terms can be found in the supplementary material). In addition, we used the same terms to explicitly search papers published in the International Journal of Social Robotic, International Conference on Social Robotics, Symposium on Usable Privacy and Security, and Proceedings of the Privacy Enhancing Technologies Symposium. Finally, we used combinations of [<Bystander> AND <Agent>] and [<Bystander> AND <Privacy>] for an additional title-only search in Google Scholar and added references from prior reviews [32, 49, 56, 60]. After duplicate filtering, we ended up with 541 papers (detailed numbers across the process can be found in the supplementary material).

In a first screening stage, we evaluated title and abstracts according to three inclusion criteria:

- Discusses a **technical system** pursuing a **dedicated task** in the presence of **people that are not using/in control of the system**.
- **Personal information** is extracted within the scope of its task from a scene and **stored** or **used** in a way that makes it **potentially accessible to others** (through e.g. active/requested disclosure, or through specific behavior/decision of the system).
- Discusses **privacy implications** for people not using/not profiting directly while the system is performing its task.

Furthermore, we explicitly excluded work published as thesis, textbook, (extended) abstract or pre-print. Each paper has been assessed

by two of the authors and potential mismatches have been resolved through discussion. 122 publications have been included and were subject to a second stage of full text filtering (again each paper has been evaluated by two authors). This resulted in 48 studies considered in the analysis (a complete list of these papers can be found in the supplementary material). Figure 2 shows the distribution of different technologies across these papers. This demonstrates that our search criteria covered a diverse application space and allow us to draw generalizable insights.

4 Results

4.1 Human Actors

We first examine how the actors' triangle and their interrelations are represented in the selected studies. As previously argued, bystanders are positioned as subjects within the flow. Human recipients are a central focus in the reviewed literature, as the relationship between subject and recipient plays a decisive role in shaping the subject's concerns.

Many of the reviewed studies in the home context examined cases where domestic workers were positioned as bystanders; such workers are present in the household as part of their professional duties. While smart systems are primarily designed to support the home owner, they inevitably affect domestic workers, even though they are not the intended users. These workers include nannies [2, 10] or pet- and babysitters [57].

Further research has shown that smart cameras influence employee–employer relationships, affecting perceptions of trust and respect. The presence of such devices, combined with power dynamics, often constrains workers' ability to voice concerns or preferences regarding data collection [9]. However, in some cases, sharing information with a direct manager can be considered desirable, if it could create positive implications at work [4]. Another category of bystanders in the domestic setting are private visitors, such as friends. These individuals emphasized that their relationship to the home owner influences their acceptance, given the homeowner's responsibility to inform them about data processing practices or to justify the necessity of such processing [7]. For a general acceptance of data sharing, it can be relevant, that a basic relationship between subject and recipient has been established, by a first explicit interaction, before initiating a data flow [4]. If the recipient is a stranger, this can generally raise privacy concerns [55].

Several papers address bystander concerns in contexts where police investigators are the recipients of data [25, 39]. TargetFinder, for example, leverages crowdsourced videos from IoT (Internet-of-Things) devices—including vehicle-mounted cameras and Google Glasses—to locate targets, potentially affecting bystanders captured in the tracking pipeline [39]. Similarly, Dolata et al. [25] describe drones that autonomously scan large areas in search of a target, again raising concerns for uninvolved individuals. However, certain use by public institutions might be acceptable within legal bounds [25, 38]. Other studies highlight bystanders' fears that technologies—particularly Augmented Reality (AR) glasses—may stream or share images with third-party applications [20, 21, 55]. In some cases, bystander concerns are raised without identifying a clear recipient. Either the recipient is left vague (a potential human who might access bystander data), or the privacy concern stems from the general awareness that data is collected and "going somewhere," evoking a panoptic effect. One paper discusses public displays designed to visually highlight unexpected social links between passers-by—for instance, projecting these links onto sidewalks to promote social cohesion [14]. Here, pedestrians act simultaneously as subjects and recipients of personal information.

4.2 Transmission Principle

The conditions under which information is transmitted play a significant role in determining bystander acceptance. A frequently mentioned principle is "with notice", which is relevant for bystander expectations [4, 50, 55], but also often considered when designing devices (in particular those, where some transmission is also passive for a primary user, e.g. smart homes) [3, 57, 67]. It is also found that this principle might not be easy to successfully implement, as it requires clear perceptibility of the signal [11, 12], and to have an intuitive meaning [3, 73]. Thakkar et al. [67] propose notification of information flow in smart home technologies through an additional technical component, such as a mobile phone app. The design of the technological device can also influence the perception of this principle, for example mobile phone AR was found to be perceived less critical than AR glasses the use of the latter is less explicit [55]. Similarly, physical shutters are better at fulfilling bystanders' expectations of notice than digital mechanisms and electronic indicators [3, 73]. Cameras were generally considered acceptable when their use was transparent and justified through an employer-employee relationship [2].

Another frequent principle is being "in control" of the the information flow at all times [3, 50, 73]. Whereas this is usually true for classical technologies and direct users, as the flow is actively initiated, bystanders might need specific consideration to guarantee control. This might involve varying degrees of control from being able to turn off a device [14] to controlling the data types transmitted [4]. In [70], many participants reported the expectation for a negotiation with the technology owner in an Airbnb context as a means of control. Ahmad et al. [3] propose tangible privacy as a design concept for smart home devices to tackle both the issues of providing control and notice for bystanders.

We also find discussions about a very prominent transmission principle in traditional human-technology interaction: "consented". Discussions about AR glasses report that a majority of participants would like to be asked for consent and able to rescind it before data is being used [4, 55]. A majority also responded in favor of using pre-registered consent for general AR use [55] (see [13] for similar results concerning automated vehicles). However, some participants also mention increased difficulties of obtaining consent from bystanders due to missing direct interaction opportunities. Das et al. [19] propose a mobile application and management framework mediating consent across different individual information flows triggered by different technologies. Koelle et al. [41] showed that simple gestures could be used to signal opt-in or opt-out of a bystander.

Another transmission principle that bystanders expect in AR context is information access restriction to trusted individuals ("in confidence") [50, 55]. Participants also reported more willingness

to accept a data flow when it is used for people with accessibility needs [4, 45, 55] or to serve an important police investigation [25]. Monitoring was considered acceptable as part of protecting the rights of the space owner, so long it was not excessive [2]. In contrast, concerns raised if it was unclear, how data would be used [55].

4.3 Data Types

Which information of a subject is transmitted in the process is also influencing bystander acceptance. Many papers consider the implications of raw video and audio data transfer. The main bystander concerns discussed when looking at such raw data were towards a feeling of being observed [2, 3, 6, 57, 75, 78]. This is perceived as particularly critical for sensitive spaces such as bathrooms [2]. A more specific fear has been found towards the implications of minor non-compliance behaviors (such as a phone call while on duty), in particular when the recipient held a certain power [9, 17]. One paper explicitly researched the negative perception of bystanders caused by uncertainty about a potential aggregation of data [13]. However, storing raw video and audio data has generally been triggering high privacy sensitivity ratings [8].

For systems that interpret observable information, both bystanders and device users considered some categories, such as body weight, to be inappropriate for disclosure [5]. Bystanders were also less comfortable providing information to the AR glasses wearer when it was captured by backward-facing cameras, i.e., from outside the user's field of view. Similarly, Ahmed et al. [4] examined bystanders' preferences for sharing visually available personal data, including inferences about age, activity, and facial expressions, with visually impaired people. Their findings suggest that access to visual information should remain aligned with the limits of natural human vision. Forms of "super vision", such as extending perception beyond the usual 120-degree peripheral field of view, were not accepted by participants. The same paper also reports on users accepting additional information types beyond current visibility if it is publicly available, for example educational background that can be assessed through social networks [4].

Data filtering by use of blurring subjects within raw videos was exhibited in several papers concerning AR glasses. Within [20], it is proposed that bystanders that do not give consent to being recorded by AR glasses, have their facial images occluded by a virtual sticker or label. This idea is further expanded upon by [17], which considers the practical implications of this kind of data processing, namely the difficulty of active face detection in keeping pace with the actual frame rate of live raw video capture. As part of their solution, reducing the sampling rate of video frames for face detection in combination with using depth frames, provides sufficient information for actively blurring and obscuring faces.

4.4 Agentic Technology as Actors

In this section, we will present perspectives in which technologies are treated as active participants in interactions, either explicitly through the authors' conceptualizations or implicitly through participants' responses.

One study explored how the robot's degree of freedom in locomotion within a domestic environment influences the perceptions of privacy of all people in the space [73]. The findings showed that as a robot's ability to freely navigate increased, participants reported a heightened sense that "the robot can follow me everywhere," leaving them with no safe private space. This, in turn, led to a desire among participants to impose strict limitations on robot movement, including discussions of physical restrictions for highly capable robots [73]. Another paper examined robot mobility through the lens of boundary management theory of privacy [38]. According to this perspective, the right to privacy is defined as the ability to effectively manage interpersonal boundaries by regulating the permeability of personal information. This right is challenged when surveillance is initiated by the robot rather than when people enter an area where surveillance is in operation [38]. Another paper investigated public attitudes toward police drones in Switzerland. The drone's mobility was associated with "permanent recording" in public spaces, leading to calls for a mandatory short retention period. One of the most pressing concerns was the lack of transparency, for instance, regarding the drones' agenda and intended purposes. Questions of transparency also extended to the drones' agency and their status as senders in the information flow, particularly whether a drone operates autonomously or is remotely controlled by a human [25].

O'Hagan et al. [55] discuss AR headsets and their growing capacity to process captured data to create unanticipated insights about people in everyday environments. The authors find strong bystander expectations towards possibilities to opt-out and be aware of such data extractions. Individual responses also raised acceptable exceptions such as sharing physiological states with a doctor or identification characteristics with the police.

A public display that revealed unexpected links between pedestrians, explicitly considered bystanders [14]. This system decides what information is disclosed to whom, which directly raises bystander privacy concerns.

Calo [16] discuss an effect that can be interpreted as technology as recipient: the mere presence of a social machine can threaten solitude, a classic value that privacy rights are meant to protect. Through their agency, robots can create a situation of "having company" on their own initiative, rather than at the discretion of users or bystanders. Such presence, or even the mere possibility of presence and observation, may inhibit creativity and self-disclosure.

5 Discussion

The results illustrate how bystander privacy is elaborated in the reviewed papers by mapping discussions to key parameters of the information flow. Across all parameters, bystanders' expectations can frequently be traced to different forms of agentic qualities—for example, how agency capabilities reshape data types and agent relationships. We propose three stages in which agency in information processing matters (Figure 3):

- **Agentic Sensing.** This refers to the capability of a technology to decide or influence when and where to initiate collection, which data types to involve, and even who becomes a subject. Such behavior is particularly relevant when bystander concerns arise from a technology's ability to navigate freely within an environment—for example, as autonomous drones or robots do [25, 73].

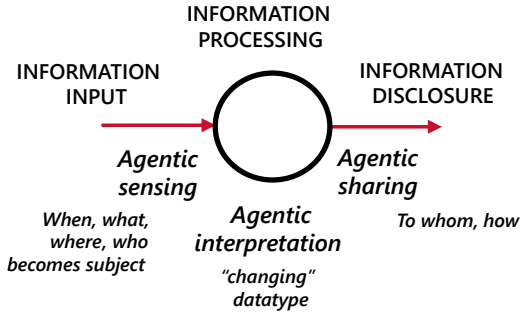


Figure 3: Robots can demonstrate agentic processing across three stages: sensing, interpretation, and sharing.

- **Agentic Interpretation**. This refers to system capabilities that autonomously interpret and so extend the meaning of collected data beyond its originally intended scope. Because the inferred data are not equivalent to the source data, this process constitutes a change in datatype. This has been observed in cases where captured data are autonomously interpreted by the system—for instance, in AR devices that generate inferences unanticipated by users [55]. Nissenbaum herself looked at information flows in the context of AI technologies and identifies this novel concern on what she describes as potentially limitless inferences of personal information [54].
- **Agentic Sharing**. A smaller subset of studies discusses technologies with autonomous capabilities that determine when and with whom to share information—thus controlling the transmission principles of information usage. One example is a public display system that autonomously decides which information to disclose and to which audience [14].

Robots usually have all three of those *behavioral freedoms* which allows us to consider the transfer of insight across all the technologies we found. Next, we will discuss how the insights suggest a new perspective on Nissenbaum's information flow model. When examined through the lens of the three agency capabilities, smart technologies are frequently characterized in ways that align them with the role of a sender. In the classic framing of informational norms, the sender is assumed to be a human actor. However, smart technologies increasingly make decisions about with whom information is shared, and in doing so, they assume a similarly active role. Decisions about when, what, and where to sense, as well as how to interpret collected data, can all be understood as forms of sender activity. Prior work has also considered robots as recipients of information. Several papers highlight that the mere presence of a robot, even in the absence of a clearly identifiable human recipient (i.e., someone to whom the robot "reports"), can raise concerns. Conceptualizing robots as recipients allows such cases to be systematically accounted for within the information flow model.

For this reason, we argue that modeling technologies solely as factors that modify transmission principles is insufficient for agentic technologies, as this approach fails to adequately reflect how people perceive and reason about them. These arguments lead us to an extended view of the information flow, as illustrated in Figure 4.

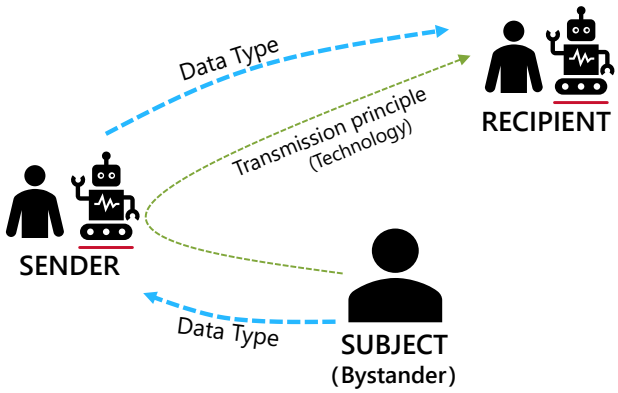


Figure 4: New perspective on the Information Flow that also positions robots as senders and recipients.

5.1 Transferring Bystander Privacy Expectations to the Robotic Context

We discuss insights with respect to the reinterpreted actor roles, and with respect to the three agentic qualities.

5.1.1 Actor Relations. Compared to most smart technologies, robots are more likely to be perceived as agents that autonomously decide when and how to sense, and when to communicate with external actors such as an owner or service provider. In the smart-home context, bystander concerns and expectations were primarily shaped by the personal power relation between the device owner and the bystander (e.g., [2]). AR technologies created an explicit relation between bystander and recipient through an in-presence transmission of information. We argue that the role of the recipient relation will be less prominent in robot applications as the recipient will be less explicit or sometimes even unknown when the information flow is initiated. This impact of a missing concrete human recipient with respect to the general feeling of being surveilled is not easy to assess from existing work. However, the fact that the recipient is not transparent might itself be a cause of bystander concerns that needs to be addressed [55]. Making ownership transparent might relax this uncertainty if an owner is trusted or has transparent intentions, for example when it is the police [25].

5.1.2 Robots as Recipients. Robots can transform a situation of being alone into one of having company, which constitutes a unique privacy concern for autonomous technologies [73]. Importantly, this concern is independent of whether data is being sensed or transmitted to third parties such as owners. Within the Information Flow framework, the robot is conceptualized as the recipient. This perspective has practical implications: it helps to understand why privacy expectations and perceived violations can arise even without a human observer. This aligns with discussion regarding physical privacy implications invading personal space [49, 59]. Theoretical discussions highlight this concern [16], but empirical evidence remains scarce. We assume that the effect scales with the degree of anthropomorphism: the more human-like the robot appears and behaves, the more people may feel observed and judged.

5.1.3 Agentic Sharing. Agentic sharing activities have not been discussed much in prior work. Similar to public display technologies [14], robots in public spaces could act as intermediaries between pedestrians. In the public display case, disclosures were both mutual and occur in the presence of the people whose information is shared. Pedestrians generally accepted such practices to some extent [14], which suggests that robots might similarly be accepted as sender in a public facilitator function.

We argued above that the role of the device owner—who could, at least to some extent, control data flows including sharing with third parties, and act as a privacy negotiation partner—may be less relevant for autonomous robots than for other smart technologies. Moreover, research on smart environments shows that visitors already frequently questioned the extent of owners' responsibility for managing data flows, noting that owners themselves might have only limited understanding of data handling practices [8]. By contrast, in the context of robots, people may expect to exercise more direct control over privacy through their own interactions.

5.1.4 Agentic Sensing and Interpretation. Results concerning raw video and audio data will likely transfer to the robotic scenario for bystander issues of aggregation, as robots can be expected to make use of data beyond the immediate interaction with the subject. AR devices are mobile, but their mobility depends on human agency, which limits the transferability of findings to robots. However, insights on the conditions for environmental sensing and human state interpretations remain relevant. From the literature we know that bystanders have rejected AR sensing capabilities that extend beyond natural human perception [5]. By analogy, we propose that robots—due to their agentic appearance—evoke expectations of a "natural" field of perception. Exceeding this (e.g., through super-vision or super-hearing) risks violating bystander expectations. This principle may also extend to interpretation. Just as robots should not exceed natural human sensory capabilities, they may also be expected to limit themselves to "reasonable" human-like interpretations.

5.2 Implications for Bystander-Privacy-Aware Robot Design

To address the privacy concerns of bystanders, various solutions have been proposed. We present insights from literature, including limitations and those considered effective, and discuss which are relevant for robots in everyday environments.

5.2.1 Transparency/Notice. When examining solutions to preserve bystander privacy in the context of smart technologies, one recurring discussion point is how to effectively inform people about the state of recording [41, 42, 74]. Similar to IoT devices or smart cameras, robots could use LED indicators to show when a camera or microphone is active. However, studies consistently report such indicators as ineffective, primarily because they are ambiguous and fail to clearly communicate "off" states [74, 19]. Color-coding schemes have also been tested, but these require bystanders to learn the meaning of each color, which poses usability challenges [42]. Moreover, under difficult lighting conditions—such as outdoors or when using AR devices—visual indicators are often hard to perceive. Acoustic signals, such as a startup sounds for cameras, are similarly unreliable due to background noise [42].

Physical mechanisms offer another approach. For instance, a shutter that visibly opens only when a camera is active provides a more intuitive signal. Yet in robotic contexts, cameras are frequently multifunctional—supporting navigation, human state sensing, and recording—making this approach impractical. Furthermore, microphones and other non-visual sensors require alternative methods. Windl et al. [73] discuss awareness mechanisms unique to robots, such as intuitive appearance changes when sensors are active or inactive, visual feedback like light bands or text displays, and even robotic voice cues announcing that the robot is no longer listening. Such multimodal approaches may offer more natural privacy signals compared to static indicators like LEDs.

In the smart-home and IoT domain, privacy dashboards have been explored as a solution. Wall-mounted displays accessible to all visitors increase transparency by eliminating the need for them to ask owners about data use [67]. For robots operating in unconstrained environments, dashboards are less feasible. Mobile applications providing the same information add convenience but introduce additional barriers: they must be installed and often require users to share personal information. Das et al. [19] propose an independent smartphone app infrastructure that automatically detects nearby devices and notifies users about their status.

5.2.2 Privacy Controls. For controlling devices with respect to their data processing, dashboards and companion apps can also provide oversight or control functions [19, 67]. Flammer et al. [28] propose that devices should connect to nearby mobile phones to request configuration before initiating operation. Beyond this, Koelle et al. [42] suggest in-situ control through free-hand gestures or voice commands to disable recording. Ahmad et al. [3] highlight that participants often resorted to tangible workarounds—such as covering smart cameras with blankets or clothing—and thus expressed a strong preference for physical on/off controls. Similarly, Windl et al. [73] found that people expect physical switches for intervening in robot operation, such as halting movement in critical spaces.

However, unlike smart-home devices or cameras that can simply suspend parts of their functionality in the presence of a visitor, robots rely on sensors for their basic operation. Providing bystanders with only a binary choice—either fully shutting the system down or leaving all functions active—risks discouraging use altogether. A modular approach, where specific sensing or processing functions can be selectively controlled, may therefore be more practical. Limiting information sensing for non-users must be intuitive. We suggest exploring strategies that allow partial and in-situ rejection of certain processes, rather than complete deactivation. A concept which might be relevant is that of design for intervenability: Explicitly designing the robot that humans are able to effectively intervene just before or after some undesired data processing happens [22].

5.2.3 Bystander Consent. We identified papers discussing consent negotiations between two parties—typically a device or space owner and bystanders—which may also represent a suitable concept for robots in partly constrained environments [7], [70]. These parties often have different yet interdependent preferences, such as whether

audio recording remains active while a visitor is present. The literature examines how such negotiations can be implemented, both technically and strategically, to establish acceptable compromises on data handling policies [7]. In line with our earlier arguments, a robot could be included in the negotiation process: either by checking bystander preferences in relation to its own functional requirements (e.g., "I need the camera for navigation"), or by acting as an advocate for the space owner (e.g., "I need to scan the environment to ensure no fire emergency doors are blocked").

In unconstrained environments, O'Hagan et al. [55] investigated how AR bystanders prefer to manage consent through opt-in versus opt-out. Participants deemed opt-in acceptable only for friends using AR devices, provided they were informed and retained the option to withdraw consent at any time. For strangers, participants preferred being asked for consent prior to any data processing. However, designing mechanisms that ensure awareness, understanding, and consent remains challenging, particularly due to the absence of a direct interactive channel between bystanders and the device. Koelle et al. [41] have highlighted consent gestures as a potential solution to this issue. Beyond non-verbal gestures, the exploration of verbal consent mechanisms appears equally important and warrants further investigation. In domains such as smart speakers, legal and ethical boundaries for providing consent verbally have already been investigated [65]. Extending these approaches to robots could open promising avenues for more natural consent practices.

5.2.4 Filtering and Privacy-aware Behaviors. As discussed before (Sec. 4.3), several studies have explored mechanisms for automatically detecting bystanders within a frame and subsequently excluding or blurring them in the recording [17]. Corbett et al. [18] further propose that audio recording or interaction should cease if an unfamiliar voice is detected. These are technologies which are suitable for certain application of robots in everyday spaces. Although such process can help to preserve objective privacy, as long as the bystander is not able to assess them, it might not positively affect their perceived privacy. Bhardwaj et al. [11] investigate coping strategies of AR device wearers when the technology itself could not adequately protect bystander privacy. One common strategy was avoiding the use of AR devices in sensitive environments. Another was explicitly reassuring interaction partners or strangers that the glasses were not recording—clarifying that recording occurred only when the indicator light was on. Although these are human coping strategies, they offer transferable insights for robotics. Technical methods already exist to detect sensitive environments or contexts [43, 47]. Building on these, robots could learn from human coping strategies—for example, how individuals manage embarrassing situations—and respond by automatically disabling recording or redirecting sensors. Similarly, robots could detect signs of bystander discomfort and respond with proactive explanations, such as clarifying that data is only temporarily stored or specifying its intended use.

5.3 Conceptual Reflection

To analyze issues of bystander privacy in robotics, we have adapted Nissenbaum's concept of Information Flow to account for technologies with agentic qualities. This adapted perspective has proven to be a productive framework, enabling the transfer of bystander privacy concerns from other agentic technologies into the robotics context. It further illuminates previously overlooked aspects, for instance by reshaping the robot's role as both recipient and sender of information. The framework also provides opportunities for further conceptual reflection and extensions with respect to responsibility and taxonomic aspects. We introduce these directions as follows:

5.3.1 Actors Responsibilities. Conceptualizing artificial agents, particularly robots, as senders or recipients can enrich the understanding of information flows as well as bystander expectations and perceived violations. However, this conceptualization also raises concerns regarding the social responsibility associated with these roles. In data protection law, such as the GDPR, senders may take on roles like controller or processor, categories explicitly reserved for humans or institutions, which also carry legal liability. There are strong reasons to keep both legal and moral responsibility with humans. Consequently, any revised Information Flow models that include artificial actors cannot serve as complete network for distributing responsibility. Future discussions must therefore focus on the accountable roles of designers and deploying entities, such as companies, as has already been debated in the context of other agentic systems like autonomous vehicles [23].

5.3.2 AI Privacy Taxonomy. Within what we describe as agentic interpretation, concerns arise from the interpretive capacities of AI-driven technologies. In the reviewed literature, this has been noted, for example, in systems that infer bystander emotions or activities, or even in discussions of generating novel insights [55]. Nissenbaum herself has acknowledged that the *unlimited* inference capabilities of AI and machine learning technologies pose challenges to her framework [54]. To address this, we suggest that the AI privacy risk taxonomy developed by Lee et al. [44] can provide useful extensions. A key risk introduced there is aggregation—the combination of multiple pieces of personal data to infer information beyond what is explicitly captured.

6 Conclusion

In this paper, we discussed bystander privacy in the context of robots in everyday environments. Insights were developed through a scoping review of bystander privacy with technologies attributed with agentic qualities through the lens of Contextual Integrity. This enabled us to investigate bystander privacy issues and expectations which could be transferable to the robotics domain. We structured our insights around the robot's capabilities for agentic sensing, interpretation, and sharing, as well as their positioning as senders or recipients within the actor's triangle. Open questions were identified, such as how new power relations emerge in the absence of a clearly identifiable human recipient and the extent to which the "naturalness" of robotic sensing shapes bystander perceptions. We also explored how existing privacy design concepts can be applied to the robotics context, identifying directions for future work: physical intervention mechanisms, interactive consent processes via verbal negotiation, or privacy-aware behaviors analogous to AR user's coping strategies. Finally, we adapted the conceptual information flow framework to highlight responsibility issues and propose opportunities for extending the theoretical foundation through the integration of an AI privacy risk taxonomy.

References

[1] Naoko Abe and Tommaso Colombino. 2024. Encounters with indoor delivery robots: a sociological analysis of non-verbal behaviours towards robots. In *22nd European Conference on Computer-Supported Cooperative Work (ECSCW 2024)* (Rimini, Italy). EUSSET. doi:10.48340/ECSCW2024_N01

[2] Ruba Abu-Salma, Junghyun Choy, Alisa Frik, and Julia Bernd. 2024. "They Didn't Buy Their Smart TV to Watch Me with the Kids": Comparing Nannies' and Parents' Privacy Threat Models for Smart Home Devices. *ACM Transactions on Computer-Human Interaction* 32 (2024), 12. Issue 2. doi:10.1145/3702321

[3] 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 (2020), 1–28. Issue CSCW2. doi:10.1145/3415187

[4] Tousif Ahmed, Apu Kapadia, Venkatesh Potluri, and Manohar Swaminathan. 2018. Up to a Limit? Privacy Concerns of Bystanders and Their Willingness to Share Additional Information with Visually Impaired Users of Assistive Technologies. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2 (2018), 1–27. Issue 3. doi:10.1145/3264899

[5] Taslima Akter, Tousif Ahmed, Apu Kapadia, and Manohar Swaminathan. 2022. Shared Privacy Concerns of the Visually Impaired and Sighted Bystanders with Camera-Based Assistive Technologies. *ACM Transactions on Accessible Computing* 15 (2022), 1–33. Issue 2. doi:10.1145/3506857

[6] Wael Albayaydh and Ivan Flechais. 2023. Examining power dynamics and user privacy in smart technology use among jordanian households. In *32nd USENIX Conference on Security Symposium (Security 2023)* (Anaheim, CA, USA). USENIX Association.

[7] 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* (New York, NY, USA). ACM, –. doi:10.1145/3544548.3581360

[8] 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. *Proceedings on Privacy Enhancing Technologies* 2022 (2022), 99–119. Issue 3. doi:10.56553/popets-2022-0064

[9] 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 *18th USENIX Conference on Usable Privacy and Security (SOUPS 2022)* (USA). USENIX Association, 687–706.

[10] J Bernd, R Abu-Salma, and A Frik. 2020. Bystanders' Privacy: The Perspectives of Nannies on Smart Home Surveillance. In *10th USENIX Workshop on Free and Open Communications on the Internet (FOCI 2020)*. –. https://www.usenix.org/conference/foci20/presentation/bernd

[11] Divyanshu Bhardwaj, Alexander Ponticello, Shreya Tomar, Adrian Dabrowski, and Katharina Krombholz. 2024. In Focus, Out of Privacy: The Wearer's Perspective on the Privacy Dilemma of Camera Glasses. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems* (New York, NY, USA). ACM, –. doi:10.1145/3613904.3642242

[12] Prajna Bhat and Yuhang Zhao. 2022. "I was Confused by It; It was Confused by Me:" Exploring the Experiences of People with Visual Impairments around Mobile Service Robots. *Proceedings of the ACM on Human-Computer Interaction* 6 (2022), 481. Issue CSCW2. doi:10.1145/3555582

[13] Cara Bloom, Joshua Tan, Javed Ramjohn, and Lujo Bauer. 2017. Self-driving cars and data collection: Privacy perceptions of networked autonomous vehicles. In *13th USENIX Conference on Usable Privacy and Security (SOUPS 2017)* (Santa Clara, CA, USA). USENIX Association, 357–375.

[14] Matthias Bohmer and Jörg Müller. 2010. Users' Opinions on Public Displays that Aim to Increase Social Cohesion. In *6th International Conference on Intelligent Environments (IE 2010)*. 255–258. doi:10.1109/IE.2010.53

[15] Kelly Caine, Selma Šabanović, and Mary Carter. 2012. The effect of monitoring by cameras and robots on the privacy enhancing behaviors of older adults. In *7th Annual ACM/IEEE International Conference on Human-Robot Interaction (HRI 2012)* (Boston, MA, USA). 343–350. doi:10.1145/2157689.2157807

[16] Ryan Calo. 2010. People Can Be So Fake: A New Dimension to Privacy and Technology Scholarship. *Penn State Law Review* 114 (2010), 809. Issue 3. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1458637

[17] Matthew Corbett, Brendan David-John, Jiacheng Shang, Y Charlie Hu, and Bo Ji. 2023. BystandAR: Protecting Bystander Visual Data in Augmented Reality Systems. In *21st Annual International Conference on Mobile Systems, Applications and Services* (New York, NY, USA). ACM, 370–382. doi:10.1145/3581791.3596830

[18] Matthew Corbett, Brendan David-John, Jiacheng Shang, Y Charlie Hu, and Bo Ji. 2024. Securing Bystander Privacy in Mixed Reality While Protecting the User Experience. *IEEE Security & Privacy* 22 (2024), 33–42. Issue 1. doi:10.1109/MSEC.2023.3331649

[19] Anupam Das, Martin Degeling, Daniel Smullen, and Norman Sadeh. 2018. Personalized Privacy Assistants for the Internet of Things: Providing Users with Notice and Choice. *IEEE Pervasive Computing* 17 (2018), 35–46. Issue 3. doi:10.1109/MPRV.2018.03367733

[20] Brendan David-John, Diane Hosfelt, Kevin Butler, and Eakta Jain. 2021. Let's SOUP up XR: Collected thoughts from an IEEE VR workshop on privacy in mixed reality. In *VR4Sec: Security for VR and VR for Security, SOUPS 2021 Workshop*. –. https://par.nsf.gov/biblio/10354958

[21] Nigel Davies, Adrian Friday, Sarah Clinch, Corina Sas, Marc Langheinrich, Geoff Ward, and Albrecht Schmidt. 2015. Security and Privacy Implications of Pervasive Memory Augmentation. *IEEE Pervasive Computing* 14 (2015), 44–53. Issue 1. doi:10.1109/MPRV.2015.13

[22] Manuel Dietrich and Jörg Pohle. 2024. Robot Design for Social Intervenability. In *Proceedings of the 13th Nordic Conference on Human-Computer Interaction* (Uppsala, Sweden) *(NordiCHI '24)*. ACM, New York, NY, USA, Article 56, 9 pages. doi:10.1145/3679318.3685392

[23] Manuel Dietrich and Thomas H Weisswange. 2019. Distributive justice as an ethical principle for autonomous vehicle behavior beyond hazard scenarios. *Ethics and Information Technology* 21 (9 2019), 227–239. Issue 3. doi:10.1007/s10676-019-09504-3

[24] Manuel Dietrich and Thomas H Weisswange. 2022. Exploring Privacy Implications for Domestic Robot Mediators. In *IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS 2022): Workshop on Robot Trust for Symbiotic Societies (RTSS 2022)* (Kyoto, Japan).

[25] Mateusz Dolata and Gerhard Schwabe. 2023. Moving beyond privacy and airspace safety: Guidelines for just drones in policing. *Government Information Quarterly* 40 (2023), 101874. Issue 4. doi:10.1016/j.giq.2023.101874

[26] 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* (Yokohama, Japan) *(CHI '21)*. ACM, New York, NY, USA, Article 64, 16 pages. doi:10.1145/3411764.3445148

[27] Lena Fiedler. 2024. Ethical Implications of Stereotyping Robots in Public Spaces. In *Robophilosophy Conference 2024* (Aarhus, Denmark). IOS Press, 265–274.

[28] Ivo Flammer. 2016. Genteel Wearables: Bystander-Centered Design. *IEEE Security & Privacy* 14 (9 2016), 73–79. Issue 5. doi:10.1109/MSP.2016.91

[29] Luciano Floridi. 2008. The Method of Levels of Abstraction. *Minds Mach.* 18, 3 (Sept. 2008), 303–329. doi:10.1007/s11023-008-9113-7

[30] Eduard Fosch-Villaronga, Christoph Lutz, and Aurelia Tamò-Larrieux. 2020. Gathering Expert Opinions for Social Robots' Ethical, Legal, and Societal Concerns: Findings from Four International Workshops. *International Journal of Social Robotics* 12 (5 2020), 441–458. Issue 2. doi:10.1007/s12369-019-00605-z

[31] Munkhjargal Gochoo, Fady Alnajjar, Tan Hsu Tan, and Sumayya Khalid. 2021. Towards Privacy-Preserved Aging in Place: A Systematic Review. *Sensors* 21 (4 2021), 3082. Issue 9. doi:10.3390/S21093082

[32] Reinhard Grabler and Sabine Theresia Koeszegi. 2025. Privacy Beyond Data: Assessment and Mitigation of Privacy Risks in Robotic Technology for Elderly Care. *ACM Transactions on Human-Robot Interaction* 14 (3 2025), 6. Issue 1. doi:10.1145/3689216

[33] Elise Christin Lind Hjemly and Ole Andreas Alsos. 2021. Trusting Autonomous Systems – Designing For Bystanders and Secondary Users. In *23rd International Conference on Engineering and Product Design Education (E&PDE 2021)* (Herning, Denmark). The Design Society. doi:10.35199/EPDE.2021.25

[34] Ohad Inbar and Noam Tractinsky. 2009. The incidental user. *Interactions* 16, 4 (July 2009), 56–59. doi:10.1145/1551986.1551998

[35] Ryan Blake Jackson and Tom Williams. 2021. A Theory of Social Agency for Human-Robot Interaction. *Frontiers in Robotics and AI* 8 (8 2021), 687726. doi:10.3389/frobt.2021.687726

[36] Björn Jensen, Nicola Tomatis, Laetitia Mayor, Andrzej Drygajlo, and Roland Siegwart. 2005. Robots meet humans-interaction in public spaces. *IEEE Transactions on Industrial Electronics* 52, 6 (2005), 1530–1546.

[37] Malte Jung and Pamela Hinds. 2018. Robots in the Wild: A Time for More Robust Theories of Human-Robot Interaction. *ACM Transactions on Human-Robot Interaction* 7 (5 2018), 2. Issue 1. doi:10.1145/3208975

[38] Margot E Kaminski. 2015. Regulating Real-World Surveillance. *Washington Law Review* 90 (2015), 1113–1165. Issue 3. doi:10.2139/SSRN.2681128

[39] Youssef Khazbak, Junpeng Qiu, Tianxiang Tan, and Guohong Cao. 2020. TargetFinder: A Privacy Preserving System for Locating Targets through IoT Cameras. *ACM Trans. Internet Things* 1 (2020), –. Issue 3. doi:10.1145/3375878

[40] Heather Knight, Timothy Lee, Brittany Hallawell, and Wendy Ju. 2017. I get it already! the influence of ChairBot motion gestures on bystander response. In *26th IEEE International Symposium on Robot and Human Interactive Communication (RO-MAN 2017)* (Lisbon, Portugal), Vol. 2017-January. IEEE, 443–448. doi:10.1109/ROMAN.2017.8172340

[41] Marion Koelle, Swamy Ananthanarayan, Simon Czupalla, Wilko Heuten, and Susanne Boll. 2018. Your smart glasses' camera bothers me! exploring opt-in and opt-out gestures for privacy mediation. In *10th Nordic Conference on Human-Computer Interaction (NordiCHI 2018)* (New York, NY, USA). ACM, 473–481. doi:10.1145/3240167.3240174

[42] Marion Koelle, Katrin Wolf, and Susanne Boll. 2018. Beyond LED Status Lights - Design Requirements of Privacy Notices for Body-worn Cameras. In *Proceedings*

of the Twelfth International Conference on Tangible, Embedded, and Embodied Interaction (New York, NY, USA). ACM, 177–187. doi:10.1145/3173225.3173234

[43] Lindrit Kqiku and Delphine Reinhardt. 2024. SensitivAlert: Image Sensitivity Prediction in Online Social Networks Using Transformer-Based Deep Learning Models. In *18th International AAAI Conference on Web and Social Media (ICWSM 2024)* (Buffalo, NY, USA), Vol. 18. AAAI, 851–864. doi:10.1609/ICWSM.V18I1.31357

[44] Hao Ping Lee, Yu Ju Yang, Thomas Serban von Davier, Jodi Forlizzi, and Sauvik Das. 2024. Deepfakes, Phrenology, Surveillance, and More! A Taxonomy of AI Privacy Risks. In *Conference on Human Factors in Computing Systems (CHI 2024)* (Honolulu, HI, USA). ACM, 775. doi:10.1145/3613904.3642116

[45] Kyungjun Lee, Daisuke Sato, Saki Asakawa, Hernisa Kacorri, and Chieko Asakawa. 2020. Pedestrian Detection with Wearable Cameras for the Blind: A Two-way Perspective. In *ACM Conference on Human Factors in Computing Systems (CHI 2020)* (Honolulu, HI, USA). ACM, 1–12. doi:10.1145/3313831.3376398

[46] Leigh Levinson, Manuel Dietrich, Alan Sarkisian, Selma Šabanović, and William D. Smart. 2025. Effective Engineering, Stakeholder Involvement, and Regulatory Plurality Within Privacy-Aware Robotics. In *20th ACM/IEEE International Conference on Human-Robot Interaction (HRI 2025)* (Melbourne, Australia). IEEE Computer Society, 1443–1447. doi:10.1109/HRI61500.2025.10974108

[47] Yifang Li, Nishant Vishwamitra, Hongxin Hu, and Kelly Caine. 2020. Towards A Taxonomy of Content Sensitivity and Sharing Preferences for Photos. In *ACM Conference on Human Factors in Computing Systems (CHI 2020)* (Honolulu, HI, USA). ACM. doi:10.1145/3313831.3376498

[48] Shiva Nischal Lingam, Rutger Verstegen, Sebastiaan M Petermeijer, and Marieke Martens. 2025. Human interactions with delivery drones in public spaces: design recommendations from recipient and bystander perspectives. *Frontiers in Robotics and AI* 12 (2025), 1580289. doi:10.3389/frobt.2025.1580289

[49] Christoph Lutz, Maren Schöttler, and Christian Pieter Hoffmann. 2019. The privacy implications of social robots: Scoping review and expert interviews. *Mobile Media and Communication* 7 (9 2019), 412–434. Issue 3. doi:10.1177/2050157919843961

[50] 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 *11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society (NordiCHI 2020)*. ACM, –. doi:10.1145/3419249.3420164

[51] Sara Nielsen, Rodrigo Ordoñez, Karl Damkjær Hansen, Mikael B. Skov, and Elizabeth Jochum. 2021. RODECA: A Canvas for Designing Robots. In *Companion of the 2021 ACM/IEEE International Conference on Human-Robot Interaction* (Boulder, CO, USA) *(HRI '21 Companion)*. ACM, New York, NY, USA, 266–270. doi:10.1145/3434074.3447173

[52] Helen Nissenbaum. 2004. Privacy as contextual integrity. *Wash. L. Rev.* 79 (2004), 119.

[53] Helen Nissenbaum. 2009. *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

[54] Helen Nissenbaum. 2019. Contextual integrity up and down the data food chain. *Theoretical inquiries in law* 20, 1 (2019), 221–256.

[55] Joseph O'Hagan, Pejman Saeghe, Jan Gugenheimer, Daniel Medeiros, Karola Marky, Mohamed Khamis, and Mark McGill. 2023. Privacy-Enhancing Technology and Everyday Augmented Reality: Understanding Bystanders' Varying Needs for Awareness and Consent. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 6 (2023), 1–35. Issue 4. doi:10.1145/3569501

[56] Alfredo J. Perez, Sherali Zeadally, and Scott Griffith. 2017. Bystanders' Privacy. *IT Professional* 19 (2017), 61–65. Issue 3. doi:10.1109/MITP.2017.42

[57] James Pierce, Claire Weizenegger, Parag Nandi, Isha Agarwal, Gwenna Gram, Jade Hurrle, Hannah Liao, Betty Lo, Aaron Park, Aivy Phan, Mark Shumskiy, and Grace Sturlaugson. 2022. Addressing Adjacent Actor Privacy: Designing for Bystanders, Co-Users, and Surveilled Subjects of Smart Home Cameras. In *ACM Designing Interactive Systems Conference (DIS 2022)* (New York, NY, USA). ACM, 26–40. doi:10.1145/3532106.3535195

[58] Astrid Rosenthal-Von Der Pütten, David Sirkin, Anna Abrams, and Laura Platte. 2020. The forgotten in HRI: Incidental encounters with robots in public spaces. In *15th ACM/IEEE International Conference on Human-Robot Interaction (HRI 2020): Companion* (Cambridge, United Kingdom). IEEE Computer Society, 656–657. doi:10.1145/3371382.3374852

[59] Delphine Reinhardt and Archan Misra. 2025. Toward Privacy-Respecting Service Robots. *IEEE Pervasive Computing* (2025). doi:10.1109/MPRV.2025.3555407

[60] Matthew Rueben and William D. Smart. 2016. Privacy in Human-Robot Interaction: Survey and Future Work. In *5th We Robot Conference 2016* (Coral Gables, FL, USA).

[61] Matthew Rueben, William D. Smart, Cindy M. Grimm, and Maya Cakmak. 2017. Privacy-sensitive robotics. In *ACM/IEEE International Conference on Human-Robot Interaction (HRI 2017)* (Vienna, Austria). IEEE Computer Society, 425–426. doi:10.1145/3029798.3029805

[62] Alberto Sanfeliu, Maria Rosa Llácer, Maria Dolors Gramunt, Albert Punsola, and Yuji Yoshimura. 2010. Influence of the Privacy Issue in the Deployment and Design of Networking Robots in European Urban Areas. *Advanced Robotics* 24 (2010), 1873–1899. Issue 13. doi:10.1163/016918610X527202

[63] 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 (Oct. 2025), 43 pages. doi:10.1145/3731755

[64] Sarah Sebo, Brett Stoll, Brian Scassellati, and Malte F Jung. 2020. Robots in Groups and Teams: A Literature Review. *Proceedings of the ACM on Human-Computer Interaction* 4 (10 2020), 1–36. Issue CSCW2. doi:10.1145/3415247

[65] William Seymour, Mark Cote, and Jose Such. 2023. Legal Obligation and Ethical Best Practice: Towards Meaningful Verbal Consent for Voice Assistants. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (Hamburg, Germany) *(CHI '23)*. ACM, New York, NY, USA, Article 166, 16 pages. doi:10.1145/3544548.3580967

[66] Xiang Zhi Tan, Marynel Vázquez, Elizabeth J. Carter, Cecilia G. Morales, and Aaron Steinfeld. 2018. Inducing Bystander Interventions during Robot Abuse with Social Mechanisms. In *13th ACM/IEEE International Conference on Human-Robot Interaction (HRI 2018)* (Chicago, IL, USA). IEEE Computer Society, 169–177. doi:10.1145/3171221.3171247

[67] 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* (New York, NY, USA). ACM, 1–13. doi:10.1145/3491102.3502137

[68] Meg Tonkin, Jonathan Vitale, Suman Ojha, Jesse Clark, Sammy Pfeiffer, William Judge, Xun Wang, and Mary Anne Williams. 2017. Embodiment, Privacy and Social Robots: May I Remember You?. In *9th International Conference on Social Robotics (ICSR 2017)* (Tsukuba, Japan), Vol. 10652 LNAI. Lecture Notes in Computer Science (LNAI 10652). Springer, Cham, 506–515. doi:10.1007/978-3-319-70022-9_50

[69] Katherine M. Tsui, Munjal Desai, and Holly A. Yanco. 2010. Considering the bystander's perspective for indirect human-robot interaction. In *5th ACM/IEEE International Conference on Human-Robot Interaction (HRI 2010)* (Osaka, Japan). IEEE, 129–130. doi:10.1109/HRI.2010.5453230

[70] Zixin Wang, Danny Yuxing Huang, and Yaxing Yao. 2023. Exploring tenants' preferences of privacy negotiation in airbnb. In *32nd USENIX Conference on Security Symposium (SEC 2023)* (Anaheim, CA, USA). USENIX Association.

[71] Jing Wei, Tilman Dingler, and Vassilis Kostakos. 2022. Understanding User Perceptions of Proactive Smart Speakers. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 5, 4, Article 185 (Dec. 2022), 28 pages. doi:10.1145/3494965

[72] Thomas H. Weisswange, Hifza Javed, Manuel Dietrich, Malte F. Jung, and Nawid Jamali. 2025. Design Implications for Robots that Facilitate Groups–A Scoping Review on Improving Group Interactions through Directed Robot Action. *ACM Transactions on Human-Robot Interaction* (11 2025). doi:10.1145/3777455

[73] Maximiliane Windl, Jan Leusmann, Albrecht Schmidt, Sebastian S Feger, and Sven Mayer. 2024. Privacy communication patterns for domestic robots. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*. 121–138. https://www.usenix.org/conference/soups2024/presentation/windl

[74] 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 (2019), 1–24. Issue CSCW. doi:10.1145/3359161

[75] Yaxing Yao, Huichuan Xia, Yun Huang, and Yang Wang. 2017. Privacy Mechanisms for Drones: Perceptions of Drone Controllers and Bystanders. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (New York, NY, USA). ACM, 6777–6788. doi:10.1145/3025453.3025907

[76] Xinyan Yu, Marius Hoggenmüller, and Martin Tomitsch. 2024. Encouraging Bystander Assistance for Urban Robots: Introducing Playful Robot Help-Seeking as a Strategy. In *ACM Designing Interactive Systems Conference (DIS 2024)* (Copenhagen, Denmark). ACM, 2514–2529. doi:10.1145/3643834.3661505

[77] Xinyan Yu, Marius Hoggenmüller, Tram Thi Minh Tran, Yiyuan Wang, and Martin Tomitsch. 2024. Understanding the Interaction between Delivery Robots and Other Road and Sidewalk Users: A Study of User-generated Online Videos. *ACM Transactions on Human-Robot Interaction* 13 (10 2024), 59. Issue 4. doi:10.1145/3677615

[78] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End user security and privacy concerns with smart homes. In *13th Symposium on Usable Privacy and Security (SOUPS 2017)*. 65–80. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/zeng

Received 2025-09-30; accepted 2025-12-01