2020 IEEE International Conference on Robotics and Automation (ICRA)
31 May - 31 August, 2020. Paris, France

# Enhancing Privacy in Robotics via Judicious Sensor Selection

Stephen Eick & Annie I. Antón

*Abstract*— **Roboticists are grappling with how to address privacy in robot design at a time when regulatory frameworks around the world increasingly require systems to be engineered to preserve and protect privacy. This paper surveys the top robotics journals and conferences over the past four decades to identify contributions with respect to privacy in robot design. Our survey revealed that less than half of one percent of the ~89,120 papers in our study even mention the word privacy. Herein, we propose privacy preserving approaches for roboticists to employ in robot design, including, assessing a robot's purpose and environment; ensuring privacy by design by selecting sensors that do not collect information that is not essential to the core objectives of that robot; embracing both privacy and performance as fundamental design challenges to be addressed early in the robot lifecycle; and performing privacy impact assessments.**

*Index Terms*— **privacy, privacy by design, robotics, robot design, sensor selection, compliance, privacy impact assessments.**

## I. Introduction

Since the founding of the first robotics journal in 1982 [1], robotics has continued to grow as a field, with more journals and conferences supporting the growing number of scholars and advances in this field. Over 89,120 documents have been published in the top robotics conferences and journals since 1982. These documents represent efforts from many different engineering and scientific disciplines, and form the basis for our survey of privacy in robot design.

This paper surveys the top robotics journals and conferences over the past four decades to identify potential contributions with respect to privacy in robot design. We provide initial design recommendations to aid roboticists as they mitigate the risks that emerge when privacy is not a fundamental design consideration. We propose several approaches for roboticists to employ to address privacy, including: carefully assessing a robot's purpose and work environment; cautiously selecting sensors so as to not over collect information that is not essential to the core objectives for a given robot; embracing privacy and performance not as orthogonal considerations, but as fundamental design challenges that should both be addressed early in the robot lifecycle; and performing privacy impact assessments to systematically design privacy in from the onset. Perhaps the most significant contribution of our survey, as captured by the title above, is that *to ensure privacy by design, a robot should be equipped with the least invasive set of sensors needed to accomplish a particular task.*

S. Eick and A. I. Antón are with the School of Interactive Computing, Georgia Institute of Technology, Atlanta, GA, 30308, USA. {stephen.eick, aianton}@gatech.edu.

In the United States, privacy has evolved as a field since 1890 when Warren and Brandeis published their seminal article "Right to Privacy" in the Harvard Law Review [2] in which they discuss how a new technology—the Eastman Kodak "snap camera" that allowed the general public to take candid photos in public places—was eroding privacy. Fast forward to 2020 where stand-alone and connected video cameras are now ubiquitous. In the past, humans were needed to process film photos and video, and non-trivial material costs were associated with their reproduction and dissemination. Today, we enjoy nearly-zero-cost data copying and transmission. Yet, the privacy concerns raised by Warren and Brandeis still exist today and are compounded by the ubiquity of cameras as well as myriad sensors.

Debates about "reasonable expectations of privacy" are now global. In the United States, the Fourth Amendment limits government access to information that has not been disclosed to a third party as well as protections from warrantless searches [3]. The U.S. Supreme Court ruled in *Carpenter v. United States* [4] that the Fourth Amendment can protect individuals from continual, unconsented, and/or unwarranted surveillance in public through GPS and cell phone technology. In Europe, every system—including a robot—that records information about individual Europeans must comply with the General Data Protection Regulation (GDPR) [5]. The GDPR requires organizations to protect personal data once explicit permission has been granted to do so by individuals about whom information is collected. Globally, data protection officials from over 60 countries recently expressed their concern about robotics, artificial intelligence, and machine learning due to the technologies' unpredictable outcomes and the subsequent privacy impacts thereof [6]. As of January 2019, 132 countries now have data privacy laws [7]. Given this global regulatory climate, engineers must design robots with these privacy protections as a fundamental system requirement.

The robotics literature does not address how to translate general privacy principles or codify privacy law into into technical requirements [8], yet the software engineering community recognizes both as part of software design [9][10][11][12][13]. Compliance with privacy regulations and robotic system performance are usually discussed as orthogonal considerations, yet the ability to operationalize relevant regulatory frameworks so as to inform robot system design is increasingly important. We now discuss our efforts to better understand how scientists, engineers, and scholars address privacy in robot design; highlight specific challenges; and propose approaches that can aid roboticists in designing privacy-aware and regulatory-compliant systems.

978-1-7281-7395-5/20/$31.00 ©2020 IEEE

## II. Related Work

Privacy means different things to different people, as evidenced by the various definitions adopted by roboticists. Both Carnivale and Ienca et al. adopt Warren and Brandeis' definition—"the right to be let alone" [14][15]. Lee et al. [16] employ Solove's Taxonomy of Privacy [17] and define privacy as "an individual's right to have control over her own data." Kim et al. [18] employ the Google Dictionary definition of privacy—"the state or condition of being free from being observed or disturbed by other people" [19]. Patompak et al. adopt Reuben et al.'s definition—"the ability of an individual or group to separate themselves and thereby express themselves selectively" [20][21]. Cawthorne et al. view privacy as "the ability to determine what information about one's self can be communicated to others" [22]. Wellman et al. view privacy as "the degree that information known specifically to individual agents is not revealed to the others" [23]. It is also important to consider how the humans, for which we design robots, define privacy.

Ethics, safety, and concerns about privacy and security are increasingly vital considerations in robot design. Roboethics as a field contends with the complex economic, ethical, and social issues that arise with the proliferation of advanced robotics [24]. Morante et al. proposed "cryptobotics" as a new field to address the need for incorporating safety and security in robots [25]. In 2017, Reuben et al. held a workshop at the ACM/IEEE International Conference on Human-Robot Interaction (HRI) to identify future directions for a proposed research area called "privacy-sensitive robotics" [21].

Limited research in the robotics literature addresses privacy and/or security. Kim et al. propose a privacy-focused architecture for an unmanned aerial system (UAS). Video and metadata from the UAS is encrypted and sent to a cloud-based "privacy server," which decrypts the transmitted information and filters the data according to both pre-defined and user-adjustable privacy policies [18]. Butler et al. ran an empirical study measuring human subjects' performance when teleoperating a robot using privacy-filtered images. Practicing a task allowed these subjects to mitigate the loss in information from the privacy-filtered images, demonstrating that both performance and privacy can be achieved [26].

Exploring privacy in robotics from a philosophical standpoint, Carnivale argues the coming generations of robots will affect the structure of societies, and privacy should be a "means to achieving" the creation of robots that affect society to the benefit of humans [14]. Sedenberg et al. apply the Fair Information Practice (FIP) principles [27] in design for commercial therapeutic robots; they suggest privacy and ethics be implemented in system design with data access and review, dynamic user consent models, general privacy controls, awareness of existing laws, responsible data sharing, and anticipation of unintended consequences [28].

Our survey revealed no existing set of fundamental design principles for robot design at large. However, design principles exist for specific robotics subdomains. Adamides et al. created a taxonomy of design guidelines for teleoperated robots [29]. Beer et al. created design guidelines for mobile manipulator robots to enable aging at home [30]. Leenes et al. discuss guidelines for dealing with four legal and ethical issues in the field of robotics: keeping up with innovation, balancing innovation with human rights, preserving social norms, and balancing effectiveness and legitimacy of regulation [31]. Elara et al. discuss design principles for robot-inclusive spaces [32]. Most relevant to our own work, Reuben et al. developed a design taxonomy for privacy-sensitive robotics that does not address sensor selection, which is a critical design consideration for enhancing privacy in robot design [33].

Legal scholars are concerned about the potential privacy harms that robots may introduce. Calo believes the social dimension of robotics opens at least three potential privacy harms: the presence of robots in certain spaces may reduce opportunities for self-reflection; social robots may have abilities to extract sensitive information from people in unforeseen ways; and descriptions of human-robot interactions may provide a new type of sensitive personal information [34]. Kerr argues that, because robots operating independently of human intervention definitively implicate privacy, legal systems will need to reexamine established privacy relationships between humans and robotics [35]. In our global and ever-increasing regulatory ecosystem in which engineers are expected to design "reasonable privacy" into the products, devices, and appliances they create, it behooves us to mitigate the risks of privacy harm as we design robots.

## III. Survey of Privacy Principles in Robot Design

In our survey, we followed the principles of systematic review as detailed by Kitchenham [36]. Our research question for the survey is, "What efforts have been made to address privacy in the design of robots?" Due to space limitations, our methodology is not fully disclosed in this paper.

Our survey focused on the top peer-reviewed robotics journals and conference proceedings, according to the Google Scholar h5-index ranking [37] and the InCites Journal Citation Reports [38]. We consulted well-established robotics researchers to gauge their views about which publications should be included in our study. Ultimately, thirty-four publications were included. Of the ~89,120 available robotics documents published from 1982 through August 28th, 2019, 520 in total mentioned privacy. Of those, 461 were peer-reviewed papers from which we extracted statements about privacy. These statements comprised a dataset of over 900 unique privacy considerations from the robotics literature. Approximately half of one percent of the documents in the surveyed robotics literature even mention privacy.

We uncovered three general perspectives of privacy in the robotics literature. The first perspective emphasizes seclusion by an individual, indicating ability to delineate a personal space [2][14][15][18]. The second perspective emphasizes communicating information and delineating information flows [16][17][22][23]. The third perspective recognizes both a secluded, personal space as well as the outflow of information from that space [20][21]. The key takeaway here

is that a robotic system creates privacy vulnerabilities when an information flow from an individual's personal space is induced that ignores preferences of that individual's self-expression. We must responsibly address these privacy values and preferences in robot design.

## IV. Privacy-Enhancing Sensors for Robot Design

Sensors are essential robot components. Architecting a robot's sensor complex requires a thorough understanding of the robot's envisaged tasks and goals as well as an appreciation for available sensing options to ensure privacy is enhanced rather than made vulnerable. We now overview design considerations associated with particular sensors that roboticists currently employ due to their privacy-enhancing properties. Note that the privacy-enhancing design modifications highlighted here were often made to increase performance; formal privacy guarantees were not provided.

Simple depth sensors project signals into free space and detect the signal amount returned back to measure distance. These sensors allow a robot to only determine the existence or presence of an individual rather than identity. (We limit our study to simple depth sensors; future work will further consider depth sensor-based smartphone unlocking via facial mapping [39]). By obtaining 3D imagery in a space, distance/depth sensors provide information that aid in goal/task completion while preserving privacy. For example, laser range finders (LRFs) detect a human's presence rather than their identity thereby preserving privacy [40][41]. Depth imagers such as the Microsoft Kinect recognize human activity while enhancing privacy by only capturing a human's depth profile [42]. One building occupancy profiling system uses depth sensors to only sense a human's presence rather than their identity, thereby protecting privacy while maintaining high accuracy rates [43]. Depth sensors can detect a fallen elderly person in medical and living environments while protecting privacy more than visible-light cameras do because they sense a human's presence rather than their identity [44]. Should a depth sensor be combined with any other sensor (such as a location sensor), the identity of the person in a bed is potentially vulnerable to privacy invasions. These examples provide compelling evidence of ways in which distance/depth sensors aid in goal/task achievement while seeking to enhance privacy. Sometimes goal/task achievement merely requires that something at a specific distance be recognized rather than identified thereby preserving privacy.

Infrared light sensors enhance privacy because they can detect existence and presence while protecting the identity of a sensed individual [45]. Instead, light from passive infrared reflectors or active infrared emitters is sensed to determine position. One position-tracking system used passive infrared reflectors to identify an elderly person's position in a smart home without sensing their identity to protect their privacy [46]. An elderly adult monitoring system tracked the position of a robotic walker by detecting infrared LEDs on the walker using a camera affixed with an infrared band-pass filter, thereby protecting privacy by sensing the individual's position rather than their identity [47]. By choosing to only sense infrared light from reflectors and emitters, one can focus on determining position to support tracking while also minimizing the potential for privacy vulnerabilities.

Binary sensors are useful for activity discovery in detection systems; for example, door barrier sensors and motion detectors simply detect whether an event has happened rather than what has happened [48]. Consider an occupancy detection system that uses binary door open/close sensors to estimate occupancy; it enhances privacy by not introducing unnecessary additional information that would otherwise have been collected by cameras or RFID sensors [49]. Roboticists employed directional, binary sensor beams to track two agents moving in a multi-room environment as a way to protect privacy [50]. Binary detection beams have also proven useful in assistive living environments for their privacy-preserving nature [51]. Having said this, it is important to stress that using binary sensors in conjunction with or as a trigger for a camera undermines the very privacy-preserving properties of a binary sensor that we wish to leverage. As a rule of thumb, engineers should deliberately select the least privacy-invasive sensor that will still allow the robot under design to accomplish a given task or goal.

Force sensors translate a load or weight into a quantifiable output. Roboticists have applied findings from human gait analysis to track robots in a home environment with force sensors, believing that force sensors introduce fewer privacy vulnerabilities than visible-light cameras [52]. Studies show humans can, in fact, be identified by gait using images from visible-light cameras [53]. One commercial example of a contact force measurement system is the Nintendo Wii Balance Board, which enables motion recognition solely using force data [54]. We were unable to find evidence, however, that an individual's identity has ever been determined using a Nintendo Wii Balance Board. Understanding context-specific goal and task requirements is important when selecting sensors, and force sensors warrant consideration to reduce privacy vulnerabilities in a sensing system.

Finally, a compass senses the earth's magnetic field and points to magnetic north with strong accuracy. Robots can use a magnetic field strength map to localize in a manner that preserves privacy, since magnetic field-based localization relies on data not considered private or sensitive [55][56]. In summary, *to ensure privacy by design, a robot should be equipped with the least invasive set of sensors needed to accomplish a particular task.*

## V. Sensors That May Introduce Privacy Vulnerabilities in Robot Design

This section overviews sensors that despite their perhaps cheaper cost may over-collect and invade privacy.

Visible-light cameras (or, cameras) create privacy vulnerabilities across a range of applications. Sensing human behavior with cameras introduces privacy vulnerabilities because the data from a camera can be used to directly identify an individual's personal and specific attributes. Elder/patient monitoring systems that use cameras create privacy vulnerabilities because cameras can reveal a medical subject's iden-

tity [57][58][59][60][61][62]. Similarly, systems that track people using cameras can not only reveal the identity of an individual, but can also be used to identify a person's location at a specific time [40][41][49][63][64]. Activity recognition systems that rely on cameras as the primary input also introduce additional risk for privacy invasion because because some actions and/or habits of a known person can be highly sensitive [65][66][67][68]. As previously mentioned, gait analysis systems—especially those that use cameras—create privacy vulnerabilities because gait analysis has proven to be an effective way to identify specific individuals [53][69][70]. The literature is full of examples of cameras that were deployed on robots, putting privacy at risk due to the ability to identify individuals within operating environments [71][72][73][74][75][76][77]. Moreover, using cameras to perform simultaneous localization and mapping (SLAM) [56][78] and path planning [79] also put privacy at risk for the same reasons.

Cameras create privacy vulnerabilities for two primary reasons. The first reason is the amount of personal information captured by a camera [28][45][80]. Increasing the resolution of a camera only increases the detail and quantity of the captured information, creating additional privacy vulnerabilities [81]. The second reason is camera usage without providing notice and awareness to the user [41][82] as required by the FIP principles [27]. In our survey, 84% of the extracted privacy statements concerning sensor selection were about visible-light cameras. Although anecdotal at best, this statistic suggests an over-reliance on cameras in robot design, which unnecessarily introduce privacy vulnerabilities when more privacy-enhancing sensors are available. That being said, image pixelization techniques grounded in differential privacy [83] have been explored to reduce the privacy vulnerabilities present in cameras [84].

Microphones transduce sound into electrical signals. As such, they introduce specific privacy vulnerabilities. Roboticists have acknowledged that privacy vulnerabilities from microphones can stem from the perceived lack of privacy in a public space [85] or the unintentional collection of voice information [86]. Unintentional collection of voice information is a serious concern among privacy advocates because of the objective and subjective privacy harms rendered by this practice [34]. Moreover, given that the GDPR requires explicit consent from individuals about whom information is collected and views this requirement as "reasonable privacy," sensor complexes containing microphones that do not provide notice of audio recording to bystanders [82] or fail to obtain user consent to intentionally record voice data [87] would lead to financial penalties for the company that produces such a robot. These risks must be carefully examined before employing microphones to accomplish robot goals and tasks that might otherwise be achievable with a different, more privacy-enhancing sensor. For example, a human behavior-logging system used a bone-conduction microphone to only record the user's voice and avoid recording the voice of another conversation participant [87]. The bone-conduction microphone can only sense the voice of the wearer, enhancing the privacy of any other conversation participant who may not have consented to having their voice recorded.

Biometric sensors use biological information (iris pattern, fingerprint, etc.) to identify a person. These sensors make privacy vulnerable because the information collected is personal and unchangeable. Haptic authentication techniques, which use patterns in user interactions to authenticate users, are a good alternative to biometric authentication techniques because they introduce fewer privacy vulnerabilities than biometrics, since haptic authentication does not rely on individuated, immutable biological data [88]. Biometric sensors introduce privacy vulnerabilities that can be mitigated by choosing less-invasive authentication mechanisms.

Geolocation sensors process a signal transmitted from a satellite for geospatial positioning. A sensor complex using geolocation creates privacy vulnerabilities because location information is inevitably tied to an individual. For example, geolocation information is used to analyze traffic flow rates. Rather than using an individual's personal geolocation information, the position of vacant autonomous vehicles can provide detailed traffic flow rates without introducing privacy vulnerabilities [89]. Geolocation information allows users to be identified in Mobility-on-Demand systems that monitor, for example, pickup and dropoff locations. One way in which this privacy risk can be mitigated without significant impact to performance is to instead report a pickup or dropoff location within a given radius rather than the location itself [90]. Again, it is important to not only consider the privacy risks introduced by certain sensors, but to also seek ways to mitigate those risks, such as by disassociating specific location information from individuals.

Usage sensors identify how much an appliance or service is used. When used in isolation and not combined with personally identifiable information, they may be used as privacy-enhancing sensors. However, consider an activity discovery and detection system that measures home electricity and water usage to identify activities. On the one hand, if there are multiple individuals in a home, the system may be unable to identify the specific individuals who used the water with certainty. However, in the case of a single-occupancy home, such privacy is not guaranteed [48]. An occupancy detection system that measures carbon dioxide concentration and HVAC activation levels in a commercial building may preserve privacy of the individuals working in a commercial building, but in a single occupancy home privacy is not similarly preserved [49]. Although carbon dioxide sensors have been touted as providing privacy because they can measure building occupancy without the potential to identify occupants [45], one cannot ignore the context in which such a sensor is being used and include that context as a critical part of privacy impact assessment.

Finally, as was previously discussed, depth sensors protect privacy because they sense presence or existence rather than identity. However, high-resolution depth images, though they do not sense information which allows for direct identification of a person, can be combined with machine

learning techniques to identify a person by their unique gait [91]. Though a sensor may reduce the presence of privacy vulnerabilities, it is important to understand the full extent of the privacy vulnerabilities introduced by a particular sensor.

## VI. Recommendations

Our recommendations provide engineers with concrete guidance about how to address privacy in robot design. These initial recommendations are by no means exclusive, but do form the basis for this initial work.

**Assess a robot's purpose and environment to determine and thwart privacy vulnerabilities**. Before we can choose appropriate sensors, we must first understand the robot's purpose and the environment in which the robot will operate. Integrating robots into society will require continued technical advancements as well as concerted attention to the many contexts for which robots are designed, each context posing unique yet important privacy implications. Our first recommendation is to assess the envisaged robot's purpose and the tasks it must achieve, as well as the environment in which the robot must operate. Understanding a robot's purpose and tasks focuses the designer's attention on what is critical for the robot's successful operation and acceptance. Considering the environment in which the robot must operate enables robot designers to identify the ways in which the environment may undermine the very privacy preserving properties we seek to achieve. For example, by actively considering the differences between objects and people we can better leverage the self-determination that humans possess and that objects do not.

**Judicious sensor selection in robot design is essential for reducing privacy vulnerabilities.** Robot designers must increasingly consider the indirect and direct effects that particular technologies, such as sensors, may have on individuals. Intelligently selecting sensors so as to not overcollect information that is not essential for a specific robot task or objective is critical to designing privacy-aware and privacy-preserving robots. Kőiva et al. modified their mechatronic fingernail design from using a microphone to using an accelerometer for sensing vibrations because voices were being unintentionally collected [86]. Frassl et al. built a magnetic field map of an indoor environment and used compass-based localization to an accuracy within nine centimeters from ground truth thereby enhancing privacy [55]. Rio et al. tracked a Turtlebot 2 using a load-sensing floor to within four centimeters of ground truth rather than using a more privacy invasive camera [52]. Rather than deploying a motion capture system, Yabuki et al. were able to recognize seven types of exercise motions in a care center using a Nintendo Wii balance board with an accuracy rate of 75% [54]. Wu et al. combined joint angles and depth maps to perform human activity recognition with state-of-the-art performance while also enhancing privacy [42]. Do et al. performed human position tracking with accuracy rates of 86% by fusing information from passive infrared sensors and a thigh-mounted inertial measurement unit instead of using cameras [46]. These examples demonstrate that it is possible to accomplish a required task or goal while enhancing privacy. These examples also comprise a standard of care for what "reasonable privacy" means within the robotics industry. Regulators will come to expect such due diligence from engineers in robot design.

To our knowledge, no case law has yet emerged due to robot sensors that may have over collected and thereby introduced privacy concerns; however, important legal considerations do exist with respect to intelligent systems. My Friend Cayla, released in 2015, is a children's doll that uses speech recognition technology and leverages Internet connectivity. When the doll is asked a question, the query is sent via Bluetooth to a smartphone for decoding, and an answer is retrieved from the Internet. This doll garnered regulatory actions in Germany when a government watchdog determined the doll to be a "concealed transmitting device," the possession of which violates the German Telecommunications Act [92]. Similarly, the Alexa virtual assistant, upon detection of a wake word, captures and transmits audio to Amazon's cloud. Alexa's sensing regime provides no avenue for a person to grant or revoke consent to record. This approach may be found by courts in future litigation to violate two-party consent law, particularly in the U.S. state of Washington [93]. Although these considerations are focused on intelligent systems more generally, they illustrate an important robot design consideration: to understand how a sensor impacts privacy is critical in the robot design process—the very act of considering these impacts enables engineers to prove due diligence in a court of law when a regulator questions whether "reasonable privacy" is afforded by a particular robot.

Our intent in providing this recommendation is to provide roboticists with a new tool for reducing privacy vulnerabilities. Designing to address issues of consent and control are vitally important, and we do not seek to draw away from the importance of these complementary techniques. *Again, to ensure privacy by design, a robot should be equipped with the least invasive set of sensors needed to accomplish a particular task.*

**Roboticists must embrace both privacy and performance as fundamental design challenges to be addressed early in the robot lifecycle.**

Our literature review revealed that robot designers are very concerned with performance. In software engineering, both performance and privacy requirements are classified as non-functional requirements [94]. Non-functional system requirements specify criteria that can be used to judge overall system operation rather than just specific behaviors. Privacy requirements must also be incorporated into the analysis of non-functional robot design requirements to ensure that all non-functional requirements are adequately addressed.

**Empirical studies are important and needed to develop a deeper understanding of how privacy values are influenced by context and how that context must inform the robot design process.** Carefully assessing a robot's purpose and work environment is critical. Our literature review included many empirical studies that underscore the fact that

people's opinions are split with respect to whether or not assistive robots preserve privacy. For example, an eldercare robotics study with 300 robotics experts and non-experts participating sought to understand perceptions about different eldercare robots [95]. Study participants noted that a bathing robot would grant more privacy than a human assistant. In contrast, participants from the same study felt a teddy-bear robot used for in-room monitoring was "a full-time invasion of privacy" [95]. Although both robots were designed to assist the elderly, *the robot designed to bathe the elderly was considered more acceptable than the robot designed to monitor.* This highlights the importance of empirical studies to develop an understanding about individuals' perceptions about privacy as well as how context plays a role in whether or not something is considered a privacy invasion.

Empirical studies also demonstrated privacy's contextual nature. Consider a study that surveyed twelve adults (average age of 25) to examine user preferences regarding an in-home social robot. Most participants said they would not use the robot if it used a camera [77]. In contrast, consider another study that surveyed ten adults in a workplace environment equipped with a social workplace robot; in this study, the participants did not express any privacy concerns about the robot collecting their personal information even though this robot also had a camera [16]. A third study surveyed twelve older adults in care facilities equipped with mobile remote presence systems. The older adults in this study raised privacy concerns primarily when discussing etiquette and managing visitors to their facility, but were still willing to use the robot if its benefits were made clear [96].

It is important to note that the quality of scientific design and analysis in many empirical studies in the robotics literature are lagging in formality and rigor in comparison to other engineering, computing, or scientific fields. For example, one cannot broadly generalize from a study with 12 humans as to how privacy should be addressed across domains or robots. To this end, we advocate for more empirical studies to help illuminate individuals' privacy values in various contexts, and also advocate for more empirical rigor in the design and execution of these studies as well.

**Personal privacy expectations vary across individuals, and robots must be designed to adapt to differing expectations.** Studies highlight the fact that context and user preference have a significant effect on privacy concerns stemming from interactions with a robot [77][97][98][99]. Individual preferences to welcome particular or limited information outflows can be objectively addressed by selecting sensors that minimize data acquisition. The subjective aspect of such preferences must be considered during robot design. How an individual perceives potential privacy harms is just as important as the actual harms that can be rendered by a robot. Similarly, building privacy into a robot requires considering both the physical capacity of a robot to induce unwelcome information flows from an individual as well as the contextual, preferential aspects of what an individual considers to be unwelcome.

**Privacy Impact Assessments (PIAs) can help engineers ensure robot sensors are selected to enhance privacy.** PIAs provide an analysis framework to understand how personally identifiable information (PII) is used over a system's life cycle [100]. PIAs typically force engineers to consider: what information is being collected; why is the information being collected; what is the intended use of the information; with whom will the information be shared; what opportunities do individuals or businesses have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information and how can they grant such consent; and how will the information be secured [101]? The questions asked during a PIA (and the subsequent analysis undertaken to answer them) can assist roboticists in designing robots that mitigate real and/or perceived privacy risks.

## VII. Summary & Future Work

Our paper was motivated by an honest curiosity to learn how roboticists address privacy in the systems they build. We conducted our survey spanning 37 years of robotics literature and found evidence that roboticists are grappling with how to address privacy in robot design. This literature review surveys the top robotics journals and conferences over the past four decades to identify potential contributions with respect to privacy in robot design. We provide initial design recommendations to aid roboticists as they mitigate the risks that emerge when privacy is not a fundamental design consideration. We propose several approaches for roboticists to employ to address privacy, including: carefully assessing a robot's purpose and work environment; cautiously selecting sensors so as to not overcollect information that is not essential to the core objectives for a given robot; embracing privacy and performance not as orthogonal considerations, but as fundamental design challenges to be addressed early in the robot lifecycle; and performing Privacy Impact Assessments to systematically design privacy in from the onset.

There exist additional sources for privacy requirements that must be met in robot design; for example, those enshrined in technical standards. Given the size and richness of our data set, such additional analysis was beyond the scope of our project. However, standards are an important source of requirements that would also benefit from a similar survey.

Our immediate plans for future work include: developing a sensor evaluation tool with heuristics to aid robot designers in considering privacy preserving options for sensor selection; and creating a robot-specific PIA tool to guide roboticists beyond sensor selection in considering the context, the environment, and constraints within which a robot must operate as we seek to preserve privacy. Additional work may include a systematic investigation of the PII that can be collected by given sensor classes to more easily map to specific regulatory frameworks, thereby enabling engineers to demonstrate due diligence in their robot designs to regulatory overseers. Finally, we are designing an empirical study to investigate how roboticists think about and approach sensor selection with respect to a sensor's potential to introduce privacy vulnerabilities or protect privacy.

## REFERENCES


[1] The International Journal of Robotics Research, *All issues*, 2019. [Online]. Available: https://journals.sagepub.com/loi/ijr (visited on 09/15/2019).

[2] S. Warren and L. Brandeis, "The right to privacy," *Harvard Law Review*, vol. 4, no. 5, pp. 193–220, 1890. DOI: 10.2307/1321160.

[3] American Bar Association, *Privacy in an interconnected world*, 2011. [Online]. Available: https://www.americanbar.org/groups/gpsolo/publications/gp_solo/2011/june/privacy_in_an_interconnectedworld/ (visited on 09/15/2019).

[4] Carpenter v. United States, U.S. Supreme Court, 585 U.S. 16-402, 2018. [Online]. Available: https://supreme.justia.com/cases/federal/us/585/16-402/case.html.

[5] Regulation (EU) 2016/679 (General Data Protection Regulation), 2016. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679.

[6] S. Gardner, *Artificial intelligence poses data privacy challenges*, Bloomberg BNA, Oct. 26, 2016. [Online]. Available: http://web.archive.org/web/20190430013115/https://www.bna.com/artificial-intelligence-poses-n57982079158/.

[7] G. Greenleaf, "Global data privacy laws 2019: 132 national laws and many bills," *Privacy Laws & Business International Report*, vol. 157, pp. 14–18, 2019. [Online]. Available: https://ssrn.com/abstract=3381593.

[8] E. Fosch-Villaronga and B. Özcan, "The progressive intertwinement between design, human needs and the regulation of care technology: The case of lower-limb exoskeletons," *International Journal of Social Robotics*, 2019. DOI: 10.1007/s12369-019-00537-8.

[9] P. Engiel, J. C. S. do Prado Leite, and J. Mylopoulos, "A tool-supported compliance process for software systems," in *Proc. 11th International Conference on Research Challenges in Information Science (RCIS)*, Brighton, May 10, 2017, pp. 66–76. DOI: 10.1109/RCIS.2017.7956519.

[10] J. Maxwell and A. I. Antón, "The production rule framework: Developing a canonical set of software requirements for compliance with law," in *Proc. 1st ACM International Health Informatics Symposium (IHI '10)*, Arlington, VA, pp. 629–636. DOI: 10.1145/1882992.1883092.

[11] J. C. Maxwell, A. I. Antón, P. Swire, M. Riaz, and C. M. McCraw, "A legal cross-references taxonomy for reasoning about compliance," *Requirements Engineering Journal*, vol. 17, no. 2, pp. 99–115, Jun. 2012. DOI: 10.1007/s00766-012-0152-5.

[12] A. Massey, P. Otto, and A. I. Antón, "Evaluating legal implementation readiness decision-making," *IEEE Transactions on Software Engineering*, vol. 41, no. 6, pp. 545–564, Jun. 2015. DOI: 10.1109/TSE.2014.2383374.

[13] P. Otto and A. I. Antón, "Addressing legal requirements in requirements engineering," in *Proc. 15th IEEE International Requirements Engineering Conference (RE'07)*, Delhi, India, pp. 5–14. DOI: 10.1109/RE.2007.65.

[14] A. Carnevale, "Will robots know us better than we know ourselves?" *Robotics and Autonomous Systems*, vol. 86, pp. 144–151, Dec. 2016. DOI: 10.1016/j.robot.2016.08.027.

[15] M. Ienca, F. Jotterand, C. Vică, and B. Elger, "Social and assistive robotics in dementia care: Ethical recommendations for research and practice," *International Journal of Social Robotics*, vol. 8, no. 4, pp. 565–573, Aug. 2016. DOI: 10.1007/s12369-016-0366-7.

[16] M. K. Lee, K. P. Tang, J. Forlizzi, and S. Kiesler, "Understanding users' perception of privacy in human-robot interaction," in *Proc. 6th International Conference on Human-Robot Interaction*, Lausanne, Switzerland, 2011, pp. 181–182. DOI: 10.1145/1957656.1957721.

[17] D. Solove, "A taxonomy of privacy," *University of Pennsylvania Law Review*, vol. 154, no. 3, p. 447, Jan. 2006, GWU Law School Public Law Research Paper No. 129. [Online]. Available: https://ssrn.com/abstract=667622.

[18] Y. Kim, J. Jo, and S. Shrestha, "A server-based real-time privacy protection scheme against video surveillance by unmanned aerial systems," in *Proc. 2014 International Conference on Unmanned Aircraft Systems (ICUAS)*, Orlando, FL, pp. 684–691. DOI: 10.1109/ICUAS.2014.6842313.

[19] Google Dictionary. [Online]. Available: https://www.google.com/search?q=define+privacy&oq=define+privacy&aqs=chrome..69i57j0l2j69i60j0l2.3091j0j7&sourceid=chrome&espv=210&es_sm=122&ie=UTF-8 (visited on 02/17/2014).

[20] P. Patompak, S. Jeong, I. Nilkhamhang, and N. Y. Chong, "Learning proxemics for personalized human–robot social interaction," *International Journal of Social Robotics*, May 25, 2019. DOI: 10.1007/s12369-019-00560-9.

[21] M. Reuben et al., "Themes and research directions in privacy-sensitive robotics," presented at the IEEE Workshop on Advanced Robotics and its Social Impacts (ARSO), Genova, Italy, 2018. DOI: 10.1109/ARSO.2018.8625758.

[22] D. Cawthorne and A. Cenci, "Value sensitive design of a humanitarian cargo drone," in *Proc. 2019 International Conference on Unmanned Aircraft Systems (ICUAS)*, Atlanta, GA, pp. 1117–1125. DOI: 10.1109/ICUAS.2019.8797940.

[23] M. P. Wellman and P. R. Wurman, "Market-aware agents for a multiagent world," *Robotics and Autonomous Systems*, vol. 24, no. 3, pp. 115–125, Feb. 1998. DOI: 10.1016/S0921-8890(98)00026-8.

[24] G. Veruggio, "The birth of roboethics," presented at the Workshop on Roboethics, IEEE International Conference on Robotics and Automation, Barcelona, 2005. [Online]. Available: http://www.roboethics.org/icra2005/veruggio.pdf.

[25] S. Morante, J. G. Victores, and C. Balaguer, "Cryptobotics: Why robots need cyber safety," *Frontiers in Robotics and AI*, vol. 2, no. 23, p. 23, Sep. 2015. DOI: 10.3389/frobt.2015.00023.

[26] D. J. Butler, J. Huang, F. Roesner, and M. Cakmak, "The privacy-utility tradeoff for remotely teleoperated robots," in *Proc. Tenth Annual ACM/IEEE International Conference on Human-Robot Interaction*, Portland, Oregon, USA, 2015, pp. 27–34. DOI: 10.1145/2696454.2696484.

[27] Secretary's Advisory Committee on Automated Personal Data Systems, "Records, computers and the rights of citizens," U.S. Department of Health, Education and Welfare, Washington, D.C., Jul. 1, 1973. [Online]. Available: https://aspe.hhs.gov/report/records-computers-and-rights-citizens.

[28] E. Sedenberg, J. Chuang, and D. Mulligan, "Designing commercial therapeutic robots for privacy preserving systems and ethical research practices withing the home," *International Journal of Social Robotics*, vol. 8, no. 4, pp. 575–587, Aug. 2016. DOI: 10.1007/s12369-016-0362-y.

[29] G. Adamides, G. Christou, C. Katsanos, M. Xenos, and T. Hadzilacos, "Usability guidelines for the design of robot teleoperation: A taxonomy," *IEEE Transactions on Human-Machine Systems*, vol. 45, no. 2, pp. 256–262, Apr. 2015. DOI: 10.1109/THMS.2014.2371048.

[30] J. Beer et al., "The domesticated robot: Design guidelines for assisting older adults to age in place," in *Proc. Seventh Annual ACM/IEEE International Conference on Human-Robot Interaction*, Boston, MA, 2012, pp. 335–342. DOI: 10.1145/2157689.2157806.

[31] R. E. Leenes, E. Palmerini, B.-J. Koops, A. Bertolini, P. Salvini, and F. Lucivero, "Regulatory challenges of robotics; some guidelines for addressing legal and ethical issues," *Law, Innovation and Technology*, vol. 9, no. 1, pp. 1–44, Mar. 2017. DOI: 10.1080/17579961.2017.1304921.

[32] M. R. Elara, N. Rojas, and A. Chua, "Design principles for robot inclusive spaces: A case study with roomba," in *Proc. 2014 IEEE International Conference on Robotics and Automation (ICRA)*, Hong Kong, 2014, pp. 5593–5599. DOI: 5593-5599.

[33] M. Rueben, F. J. Bernieri, C. M. Grimm, and W. D. Smart, "Framing effects on privacy concerns about a home telepresence robot," in *Proc. Twelfth Annual ACM/IEEE International Conference on Human-Robot Interaction*, Vienna, Austria, 2017, pp. 435–444. DOI: 10.1145/2909824.3020218.

[34] R. Calo, "The boundaries of privacy harm," *Indiana Law Journal*, vol. 86, no. 3, 2011. [Online]. Available: https://www.repository.law.indiana.edu/ilj/vol86/iss3/8.

[35] I. Kerr, "Schrödinger's robot: Privacy in uncertain states," *20 Theoretical Inquiries L.*, Apr. 2018, Ottawa Faculty of Law Working Paper No. 2018-14. [Online]. Available: https://ssrn.com/abstract=3158790.

[36] B. Kitchenham, "Procedures for performing systematic reviews," Keele University and National ICT Australia Ltd. (Joint), Tech. Rep. TR/SE-0401 (KU) and 0400011T.1 (NICTA), Jul. 2004. [Online]. Available: http://www.inf.ufsc.br/~aldo.vw/kitchenham.pdf.

[37] Google Scholar, *Top publications*. [Online]. Available: https://scholar.google.com/citations?view_op=top_venues&hl=en&vq=eng_robotics (visited on 01/15/2019).

[38] InCites Journal Citation Reports. [Online]. Available: https://jcr.incites.thomsonreuters.com/JCRJournalHomeAction.action?pg=JRNLHOME&categoryName=ROBOTICS&categories=RB (visited on 01/15/2019).

[39] Apple, Inc., *About Face ID advanced technology*, Jan. 14, 2020. [Online]. Available: https://support.apple.com/en-us/HT208108.

[40] T. Ikeda, Y. Chigodo, T. Miyashita, F. Kishino, and N. Hagita, "A method to recognize 3d shapes of moving targets based on integration of inclined 2d range scans," in *Proc. 2011 IEEE International Conference on Robotics and Automation (ICRA)*, Shanghai, China, May 2011, pp. 3575–3580. DOI: 10.1109/ICRA.2011.5980540.

[41] T.-E. Tseng, A.-S. Liu, P.-H. Hsiao, C.-M. Huang, and L.-C. Fu, "Real-time people detection and tracking for indoor surveillance using multiple top-view depth cameras," in *Proc. 2014 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, Chicago, IL, Sep. 2014, pp. 4077–4082. DOI: 10.1109/IROS.2014.6943136.

[42] M.-Y. Wu, T.-Y. Chen, K.-Y. Chen, and L.-C. Fu, "Daily activity recognition using the informative features from skeletal and depth data," in *Proc. 2016 IEEE International Conference on Robotics and Automation (ICRA)*, Stockholm, Sweden, May 2016, pp. 1628–1633. DOI: 10.1109/ICRA.2016.7487303.

[43] M. Jin, N. Bekiaris-Liberis, K. Weekly, C. J. Spanos, and A. M. Bayen, "Occupancy detection via environmental sensing," *IEEE Transactions on Automation Science and Engineering*, vol. 15, no. 2, pp. 443–455, Apr. 2018. DOI: 10.1109/TASE.2016.2619720.

[44] F. Zhao, Z. Cao, Y. Xiao, J. Mao, and J. Yuan, "Real-time detection of fall from bed using a single depth camera," *IEEE Transactions on Automation Science and Engineering*, vol. 16, no. 3, pp. 1018–1032, Jul. 2019. DOI: 10.1109/TASE.2018.2861382.

[45] Q.-S. Jia, H. Wang, Y. Lei, Q. Zhao, and X. Guan, "A decentralized stay-time based occupant distribution estimation method for buildings," *IEEE Transactions on Automation Science and Engineering*, vol. 12, no. 4, pp. 1482–1491, Oct. 2015. DOI: 10.1109/TASE.2014.2361122.

[46] H. M. Do, M. Pham, W. Sheng, D. Yang, and M. Liu, "RiSH: A robot-integrated smart home for elderly care," *Robotics and Autonomous Systems*, vol. 101, pp. 74–92, Mar. 2018. DOI: 10.1016/j.robot.2017.12.008.

[47] D. Chugo, T. Asawa, T. Kitamura, J. Songmin, and K. Takase, "A motion control of a robotic walker for continuous assistance during standing, walking and seating operation," in *Proc. 2009 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, St. Louis, MO, Oct. 2009, pp. 4487–4492. DOI: 10.1109/IROS.2009.5354523.

[48] J. Saives, C. Pianon, and G. Faraut, "Activity discovery and detection of behavioral deviations of an inhabitatnt from binary sensors," *IEEE Transactions on Automation Science and Engineering*, vol. 12, no. 4, pp. 1211–1224, Oct. 2015. DOI: 10.1109/TASE.2015.2471842.

[49] A. Ebadat, G. Bottegal, D. Varagnolo, B. Wahlberg, and K. H. Johansson, "Regularized deconvolution-based approaches for estimating room occupancies," *IEEE Transactions on Automation Science and Engineering*, vol. 12, no. 4, pp. 1157–1168, Oct. 2015. DOI: 10.1109/TASE.2015.2471305.

[50] L. Bobadilla, O. Sanchez, J. Czarnowski, and S. M. LaValle, "Minimalist multiple target tracking using directional sensor beams," in *Proc. 2011 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, San Francisco, CA, Sep. 2011, pp. 3101–3107. DOI: 10.1109/IROS.2011.6095104.

[51] Y. Tian, K. Khosoussi, and J. P. How, "Resource-aware algorithms for distributed loop closure detection with provable performance guarantees," presented at the Workshop on the Algorithmic Foundations of Robotics (WAFR), Mérida, México, Dec. 2018. [Online]. Available: https://arxiv.org/pdf/1901.05925.pdf.

[52] M. Rio, F. Colas, M. Andries, and F. Charpillet, "Probabilistic sensor data processing for robot localization on load-sensing floors," in *Proc. 2016 International Conference on Robotics and Automation (ICRA)*, Stockholm, Sweden, May 2016, pp. 4544–4550. DOI: 10.1109/ICRA.2016.7487654.

[53] J. Chen, "Gait correlation analysis based human identification," *Scientific World Journal*, vol. 2014, no. 168275, Jan. 2014. DOI: 10.1155/2014/168275.

[54] T. Yabuki and G. Venture, "Human motion classification and recognition using wholebody contact force," in *Proc. 2015 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, Hamburg, Germany, Sep. 2015, pp. 4251–4256. DOI: 10.1109/IROS.2015.7353979.

[55] M. Frassl, M. Angermann, M. Lichtenstern, P. Robertson, B. J. Julian, and M. Doniec, "Magnetic maps of indoor environments for precise localization legged and non-legged

locomotion," in *Proc. 2013 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, Tokyo, Japan, Nov. 2013, pp. 913–920. DOI: 10.1109/IROS.2013.6696459.

[56] C. Gao and R. Harle, "MSGD: Scalable back-end for indoor magnetic field-based GraphSLAM," in *Proc. 2017 IEEE International Conference on Robotics and Automation (ICRA)*, Singapore, May 2017, pp. 3855–3862. DOI: 10.1109/ICRA.2017.7989444.

[57] C. Zhu, W. Sheng, and M. Liu, "Wearable sensor-based behavioral anomaly detection in smart assisted living systems," *IEEE Transactions on Automation Science and Engineering*, vol. 12, no. 4, pp. 1225–1234, Oct. 2015. DOI: 10.1109/TASE.2015.2474743.

[58] T. Liu and J. Liu, "Mobile robot aided silhouette imaging and robust body pose recognition for elderly-fall detection," *International Journal of Advanced Robotic Systems*, vol. 11, no. 42, Mar. 2014. DOI: 10.5772/57318.

[59] N. Kubota, T. Narita, and B. H. Lee, "3D topological reconstruction based on Hough transform and growing neural gas for informationally structured space," in *Proc. 2010 IEEE/RSJ International Conference on Intelligent Robots and Systems*, Taipei, Taiwan, Oct. 2010, pp. 3459–3464. DOI: 10.1109/IROS.2010.5653538.

[60] T. Hori, Y. Nishida, and S. Murakami, "Pervasive sensor system for evidence-based nursing care support," in *Proc. 2006 IEEE International Conference on Robotics and Automation (ICRA)*, Orlando, FL, May 2006, pp. 1680–1685. DOI: 10.1109/ROBOT.2006.1641948.

[61] T. Harada, T. Sato, and T. Mori, "Pressure distribution image based human motion tracking system using skeleton and surface integration model," in *Proc. 2001 IEEE International Conference on Robotics and Automation (ICRA)*, Seoul, May 2001, pp. 3201–3207. DOI: 10.1109/ROBOT.2001.933111.

[62] N. Miyake, S. Shibukawa, H. Masaki, and M. Otake-Matsuura, "User-oriented design of active monitoring bedside agent for older adults to prevent falls," *Journal of Intelligent Robotic Systems*, Jul. 2019. DOI: 10.1007/s10846-019-01050-w.

[63] R. C. Luo, O. Chen, and C. W. Lin, "Indoor human monitoring system using wireless and pyroelectric sensory fusion system," in *Proc. 2010 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, Taipei, Taiwan, Oct. 2010, pp. 1507–1512. DOI: 10.1109/IROS.2010.5651345.

[64] M. Pham, D. Yang, and W. Sheng, "A sensor fusion approach to indoor human localization based on environmental and wearable sensors," *IEEE Transactions on Automation Science and Engineering*, vol. 16, no. 1, pp. 339–350, Jan. 2019. DOI: 10.1109/TASE.2018.2874487.

[65] A. Moschetti, L. Fiorini, D. Esposito, P. Dario, and F. Cavallo, "Daily activity recognition with inertial ring and bracelet: And unsupervised approach," in *Proc. 2017 IEEE International Conference on Robotics and Automation (ICRA)*, Singapore, May 2017, pp. 3250–3255. DOI: 10.1109/ICRA.2017.7989370.

[66] N. Melo, J. Lee, and R. Suzuki, "Identification of the user's habits based on activity information," in *Proc. 2018 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, Madrid, Spain, Oct. 2018, pp. 2014–2019. DOI: 10.1109/IROS.2018.8593873.

[67] Y.-T. Chiang, K.-C. Hsu, C.-H. Lu, L.-C. Fu, and J. Y.-J. Hsu, "Interaction models for multiple-resident activity recognition in a smart home," in *Proc. 2010 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, Taipei, Taiwan, Oct. 2010, pp. 3753–3758. DOI: 10.1109/IROS.2010.5650340.

[68] Y.-H. Chen, C.-H. Lu, K.-C. Hsu, L.-C. Fu, Y.-J. Yeh, and L.-C. Kuo, "Preference model assisted activity recognition learning in a smart home environment," in *Proc. 2009 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, St. Louis, MO, Oct. 2009, pp. 4657–4662. DOI: 10.1109/IROS.2009.5353937.

[69] T. Liu, Y. Inoue, K. Shibata, and K. Shiojima, "Three-dimensional lower limb kinematic and kinetic analysis based on a wireless sensor system," in *Proc. 2011 IEEE International Conference on Robotics and Automation*, Shanghai, China, May 2011, pp. 842–847. DOI: 10.1109/ICRA.2011.5979856.

[70] S. Mohammed, A. Samé, L. Oukhellou, K. Kong, W. Huo, and Y. Amirat, "Recognition of gait cycle phases using wearable sensors," *Robotics and Autonomous Systems*, vol. 75, pp. 50–59, Jan. 2016. DOI: 10.1016/j.robot.2014.10.012.

[71] F. Martín, E. Soriano, and J. M. Cañas, "Quantitative analysis of security in distributed robotic frameworks," *Robotics and Autonomous Systems*, vol. 100, pp. 95–107, Feb. 2018. DOI: 10.1016/j.robot.2017.11.002.

[72] Y. Pyo, K. Nakashima, S. Kuwahata, R. Kurazume, T. Tsuji, K. Morooka, and T. Hasegawa, "Service robot system with an informationally structured environment," *Robotics and Autonomous Systems*, vol. 74, pp. 148–165, Dec. 2015. DOI: 10.1016/j.robot.2015.07.010.

[73] M. Reuben, "Context-aware assistive interfaces for persons with severe motor disabilities," in *HRI'15 Extended Abstracts: Proc. Tenth Annual ACM/IEEE International Conference on Human-Robot Interaction Extended Abstracts*, ser. HRI '15, Portland, OR, Mar. 2015, pp. 217–218.

[74] F. Michaud et al., "Exploratory design and evaluation of a homecare teleassistive mobile robotics system," *Mechatronics*, vol. 20, no. 7, pp. 751–766, Oct. 2010. DOI: 10.1016/j.mechatronics.2010.01.010.

[75] J. Klow, J. Proby, M. Reuben, R. Sowell, C. Grimm, and W. Smart, "Privacy, utility, and cognitive load in remote presence systems," in *Proc. Companion of the 2017 ACM/IEEE International Conference on Human-Robot Interaction*, ser. HRI '17, Vienna, Austria, Mar. 2017, pp. 167–168.

[76] S. Booth, J. Tompkin, H. Pfister, J. Waldo, K. Gajos, and R. Nagpal, "Piggybacking robots: Human-robot overtrust in university dormitory security," in *Proc. 2017 ACM/IEEE International Conference on Human-Robot Interaction*, ser. HRI '17, Vienna, Austria, Mar. 2017, pp. 426–434.

[77] K. Jeong, J. Sung, H.-S. Lee, A. Kim, H. Kim, C. Park, Y. Jeong, J. Lee, and J. Kim, "Fribo: A social networking robot for increasing social connectedness through sharing daily home activities from living noise data," in *Proc. 2018 ACM/IEEE International Conference on Human-Robot Interaction*, ser. HRI '18, Chicago, IL, USA, 2018, 114–122. DOI: 10.1145/3171221.3171254.

[78] S. Wang, H. Wen, R. Clark, and N. Trigoni, "Keyframe based large-scale indoor localisation using geomagnetic field and motion pattern," in *Proc. 2016 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, Daejeon, South Korea, Oct. 2016, pp. 1910–1917. DOI: 10.1109/IROS.2016.7759302.

[79] R. Allamaraju et al., "Human aware UAS path planning in urban environments using nonstationary MDPs," in *Proc. 2014 IEEE International Conference on Robotics and Automation (ICRA)*, Hong Kong, May 2014, pp. 1161–1167. DOI: 10.1109/ICRA.2014.6907000.

[80] A. Virgona, A. Alempijevic, and T. Vidal-Calleja, "Socially constrained tracking in crowded environments using shoulder pose estimates," in *Proc. 2018 IEEE International Conference on Robotics and Automation (ICRA)*, Brisbane,

Australia, May 2018, pp. 4555–4562. DOI: 10.1109/ICRA.2018.8461030.

[81] L. Lopes, T. Miklovicz, E. Bakker, and Z. Milosevic, "The benefits and challenges of robotics in the mineral raw materials sector - an overview," in *Proc. 2018 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, Madrid, Spain, Oct. 2018, pp. 1507–1512. DOI: 10.1109/IROS.2018.8594218.

[82] E. Cha, T. Trehon, L. Wathieu, C. Wagner, A. Shukla, and M. J. Matarić, "Modlight: Designing a modular light signaling tool for human robot-interaction," in *Proc. 2017 IEEE International Conference on Robotics and Automation (ICRA)*, Singapore, Singapore, May 2017, pp. 1654–1661. DOI: 10.1109/ICRA.2017.7989195.

[83] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy," *Foundations and Trends® in Theoretical Computer Science*, vol. 9, no. 3–4, pp. 211–407, 2014. DOI: 10.1561/0400000042.

[84] L. Fan, "Image pixelization with differential privacy," in *Data and Applications Security and Privacy XXXII*, Springer International Publishing, 2018, pp. 148–162. DOI: 10.1007/978-3-319-95729-6_10.

[85] R. Matsuo and J.-H. Lee, "A novel interaction method based on a mobile device in intelligent space," in *Proc. 2012 IEEE International Conference on Intelligent Robots and Systems (IROS)*, Vilamoura, Portugal, Oct. 2012, pp. 3324–3325. DOI: 10.1109/IROS.2012.6386266.

[86] R. Kõiva, T. Schwank, G. Walck, R. Haschke, and H. J. Ritter, "Mechatronic fingernail with static and dynamic force sensing," in *Proc. 2018 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, Madrid, Spain, Oct. 2018, pp. 2114–2119. DOI: 10.1109/IROS.2018.8594207.

[87] T. Sato, S. Itoh, S. Otani, T. Harada, and T. Mori, "Human behavior logging support system utilizing pose/position sensors and behavior target sensors," in *Proc. 2003 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, Las Vegas, NV, Oct. 2003, pp. 1068–1073. DOI: 10.1109/IROS.2003.1248786.

[88] J. Yan, K. Huang, T. Bonaci, and H. J. Chizeck, "Haptic passwords," in *Proc. 2015 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, Hamburg, Germany, Sep. 2015, pp. 1194–1199. DOI: 10.1109/IROS.2015.7353521.

[89] J. Chen, K. H. Low, Y. Yao, and P. Jaillet, "Gaussian process decentralized data fusion and active sensing for spatiotemporal traffic modeling and prediction in mobility-on-demand systems," *IEEE Transactions on Automation Science and Engineering*, vol. 12, no. 3, pp. 901–921, Jul. 2015. DOI: 10.1109/TASE.2015.2422852.

[90] A. Prorok and V. Kumar, "Privacy-preserving vehicle assignment for mobility-on-demand systems," in *Proc. 2017 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, Vancouver, BC, Sep. 2017, pp. 1869–1876. DOI: 10.1109/IROS.2017.8206003.

[91] A. Haque, A. Alahi, and F.-F. Li, "Recurrent attention models for depth-based person identification," in *Proc. 2016 Conference on Computer Vision and Pattern Recognition (CVPR)*, Las Vegas, NV, Jun. 2016, pp. 1229–1238. DOI: 10.1109/CVPR.2016.138.

[92] BBC News, "German parents told to destroy Cayla dolls over hacking fears," Feb. 17, 2017. [Online]. Available: https://www.bbc.com/news/world-europe-39002142.

[93] R. Kuruvilla, "Between you, me, and Alexa: On the legality of virtual assistant devices in two-party consent states," *Washington Law Review*, vol. 94, no. 4, pp. 2029–2055, 2019. [Online]. Available: https://digitalcommons.law.uw.edu/wlr/vol94/iss4/11.

[94] R. Pressman and B. Maxim, *Software Engineering: A Practitioner's Approach, 9th Edition*. McGraw Hill, 2020, ISBN: 9781259872976.

[95] A. Moon, P. Danielson, and H. F. M. Van der Loos, "Survey-based discussions on morally contentious applications of interactive robotics," *International Journal of Social Robotics*, vol. 4, no. 1, pp. 77–96, Jan. 2012. DOI: 10.1007/s12369-011-0120-0.

[96] J. M. Beer and L. Takayama, "Mobile remote presence systems for older adults: Acceptance, benefits, and concerns," in *Proc. 6th International Conference on Human-Robot Interaction*, ser. HRI '11, Lausanne, Switzerland, 2011, pp. 19–26. DOI: 10.1145/1957656.1957665.

[97] K. Caine, S. Šabanovic, and M. Carter, "The effect of monitoring by cameras and robots on the privacy enhancing behaviors of older adults," in *Proc. Seventh Annual ACM/IEEE International Conference on Human-Robot Interaction*, ser. HRI '12, 2012, pp. 343–350. DOI: 10.1145/2157689.2157807.

[98] M. Niemelä, L. van Aerschot, A. Tammela, I. Aaltonen, and H. Lammi, "Towards ethical guidelines of using telepresence robots in residential care," *International Journal of Social Robotics*, Feb. 22, 2019. DOI: 10.1007/s12369-019-00529-8.

[99] D. Fischinger et. al, "Hobbit, a care robot supporting independent living at home: First prototype and lessons learned," *Robotics and Autonomous Systems*, vol. 75, pp. 60–78, 2016. DOI: https://doi.org/10.1016/j.robot.2014.09.029.

[100] Federal Trade Commission, *Privacy Impact Assessments*. [Online]. Available: https://www.ftc.gov/site-information/privacy-policy/privacy-impact-assessments (visited on 09/08/2019).

[101] NIST Technology Innovation Program, "Privacy Impact Assessment (PIA)," National Institute of Technology, Tech. Rep., May 9, 2017, UPI: 006-55-01-27-02-7040-00. [Online]. Available: https://www.nist.gov/system/files/documents/2017/05/09/NIST-TIP-PIA-Consolidated.pdf.