Increasing User Confidence in Privacy-Sensitive Robots

Raniah Bamagain and Marius Silaghi

Florida Institute of Technology

150 W University Blvd

Melbourne, FL 32901

rbamagain2017@my.fit.edu, msilaghi@fit.edu

ABSTRACT

As the deployment and availability of robots grow rapidly, and spreads everywhere to reach places where they can communicate with humans, numerous new benefits and services can be provided, but at the same time, various types of privacy issues appear. Indeed, the use of robots that process data remotely causes privacy concerns. There are some main factors that could increase the capability of violating users' privacy. Here we analyze these factors and propose solutions that assist in mitigating the problem of privacy violation while using social robots. These solutions assist in solving the limitations of current robots and in producing privacy-sensitive robots. The result consists in usable, trusted, and comfortable techniques to bring security in the context of social robot utilization, to protect users' privacy in the presence of social robots, to increase users' awareness towards associated privacy risks, and to find trade-offs between privacy loss and utility achieved. The aim is to increase the user confidence in the privacy guarantees made available by the robots. The results are verified with surveys and experiments.

1. INTRODUCTION

According to Pranav Mistry, "Whatever science fiction movies we watch now, we can make the technology real in two days. What we can do is not important. What we should do is more important" [1]. This means developing a new technology is not impossible even if this technology appears for the first time in the fiction world.

Recently, various types of advanced and intelligent technologies have been rapidly developed to become popular and common. Indeed, robots are one of the fictional technologies that have emerged in the real world to become one of the cutting-edge technologies that will play a significant role in our society.

In fact, there are various opportunities to increase the number of robots used [2]. There are various types and classifications of robots that are used in many different sectors and areas, such as industries, hospitals, homes, and companies. Additionally, nowadays, robots are equipped with a wide variety of sensors. Because robots have become more intelligent, mobile, and interactive, communication protocols and channels have become required by most of the robots' applications in order to perform some process [2].

Robots are becoming increasingly popular everywhere. Based on statistics, between 2017 and 2025, the growth of both industrial and non-industrial robotics is still expanding [3,4]. This means the future of using robots everywhere is in progress and is promising. Thus, finding robots in every workstation, home, and everywhere else could be possible.

However, because the popularity of the presence of robots that interact and communicate with humans is growing, the robots are becoming able to constantly sense, watch, hear, process, and record all the environment around them (video and audio), such as all the humans' activities, actions, and data. This means huge amounts of information could be transferred continually in and out of a robot's system [5]. Thus, these abilities of those social robots that interact with humans anywhere and the amounts of data that are processed by the robots could lead to violating users' privacy and affecting humans' behaviors. Indeed, the abilities of these social robots are not limited to only those capabilities, but these robots are also able to move, to enter many different places that people cannot enter or could have a variety of private data, and do even more [6].

The incidents and facts that are involving robots have attracted high attention in the media and have gained the researchers' attention as well. In addition, due to the privacy issues that have appeared as a result of using social robots, many researchers have become interested in this topic that could occupy a large place in the research area. Additionally, many users have become concerned about their privacy from using these robots in their daily lives or from seeing those robots in the environment around them_[12]. However, it is important to keep working on this research area in order to provide solutions that assist in producing a vast number of privacy-sensitive robotics solutions that people are comfortable with. In order to achieve beneficial progress in the privacy-sensitive robotics research area, researchers need to study the current progress of this technology, discover the gaps in research, and solve the limitations that are related to privacy-sensitive robotics.

There are many different problems related to robots, such as there are no privacy standards or techniques that could be applied to different social robots when designing privacy-sensitive social robots [7]. In addition, there is a lack of research that examine the social robots' appearance privacy. Furthermore, there are limitations and issues regarding the techniques that are used to constrain the capabilities of robots, such as perception and movement, which are the main sources of privacy violation. Moreover, techniques and warning systems that could assist in increasing the users' awareness about privacy risks that could arise from the existence of robots around them, and that could assist in understanding the robots' actions, work, and the capabilities are absent. Furthermore, there are limitations in existing techniques that could be used to disclose different new concerns of privacy while using the robots and then providing the best solutions that could assist in trading off between the utility of and privacy concerns related to the robot. Besides, there is a lack of viable adaptive authentication methods that are trusted and require little effort from users, and that could be used by the robot to authenticate different users in order to protect their privacy when many different users use this one robot. Finally, the limitations of applications characteristics that could be used to aid users to manage their robots regarding their privacy preferences are apparent.

Thus, there is a need for solutions that could help in solving and improving the aforementioned issues and limitations in a more appropriate way.

2. LITERATURE REVIEW

Researchers tried to understand humans' privacy concerns when robots are around in order to develop appropriate techniques and solutions that could assist in protecting users' privacy. Thus, researchers conducted experiments that enable participants to discover their concerns [9,14,15,16]. In addition, some other researchers used described or watched scenarios [17,18], used surveys [19], or conducted a discussion [20]. However, there is a need for covering most of the information, objects, situations, and locations about which people could be concerned.

Regarding the first factor, the shape of robots, researchers studied the relationship between the robots' appearance and the users' confidence and trust [21], the relationship between users' behaviors and different appearance of robots [22,23,24,25,26], while others studied users' awareness regarding robots' appearance [9]. However, there is a need to study the effect of robots' appearance on privacy.

Regarding the robots' cameras, researchers proposed techniques to protect private situations, such as nakedness [27,28]. Furthermore, there are some other researchers who used different types of image manipulation techniques to protect privacy [29,30,31]. Moreover, some researchers focused on protecting the users' appearance especially users' faces [32,33], or the trade-off between privacy and utility [34,19,13,11]. Various interfaces were analyzed according to their efficiency and usability for specifying the private objects in an office environment [35]. However, most of the used techniques could draw attention or could be used only to protect users' faces.

Regarding the robots' microphones, privacy violation was studied in [36]. Smart speakers provide an encryption method to address the problem. One can strive to constrain what the robots can hear and to protect audio privacy.

Regarding the robots' movements, in [37] the researchers used the motion-planning algorithm and obstacles. In [38], a semantic map uses both metric measurements and conceptual data. Furthermore [39,40] studied other constraints techniques to protect the personal space.

Regarding the authentications on robots, researchers used the biometric-based method or semi-biometric based methods for authentication [41]. Fingerprint was used as a first step and voice as a second step, in [42] while other researchers used face recognition methods [43,44]. Methods for estimating the gender of a user rely on the morphological shape, were used in [45]. Finally, there are researchers who used external hardware for examining (brainwaves) for authentication, such in [46].

Regarding the robots warning system, [47] studied privacy protection regarding embodied humanoid robot and disembodied robots, while [48] studied the influence of robots' transparency on users' privacy attentions and their awareness. However, it seems like most robots do not use a warning system for security and privacy purposes.

Regarding the robot application's characteristics, [49,50] study controls for robots' functions and general settings.

3. PROPOSED SOLUTIONS AND TECHNIQUES FOR PRIVACY-SENSITIVE ROBOTS

As we mentioned before, there are different factors, such as the robots' appearance, camera, microphone, and movement as well as the lack of users' authentication, the lack of warning system, and the characteristics of applications that assist in controlling the privacy setting on robots, that could result in violating users' privacy.

This section explains the proposed solutions regarding each factor. We evaluate whether those solutions are comfortable and preferred by the social robots' users through conducting surveys and an experiment that are explained later in the paper.

3.1 Shape of Robots

From the previous works, we noticed that there is a relationship between the robots' appearance and users' confidence, trust, behaviors, perception of privacy, and awareness. The researchers asserted that when the robot looks like a human in its appearance, many privacy violations could occur. For example, the studies proved that users could trust the robots in a wrong and risky way [8], so they could forget that they are machines and their abilities surpass humans' abilities. In addition, the studies proved

that when the robots seem like humans, the users could recognize that their senses are placed in the same places as humans and can work as a humans only, such as the camera placed in the eyes, not in the back, the head of robots can move as human only, but not 360 degrees, and the robots' eyes (camera) and ears (microphone) cannot record [9]. On the other hand, the results of some previous surveys asserted that many people did not prefer a social robot that works in their houses, or that acts as their pet or as their friend to look like a machine [10]. Additionally, other studies showed that some robots are equipped with additional sensors that are not needed by social robots.

It would be better if we design the social robots by mixing the outer appearance of machine and humans, such as the NAO, Pepper, ROMEO robots. Moreover, it could be better if we design social robots with appropriate sizes that could make the users more comfortable and that could assist the robots in performing their tasks efficiently. In addition, to provide a better design, we would equip the robots with sensors that the robots need only and place those sensors in appropriate places, such as put the cameras on the robot's eyes, the microphone on the robot's ears, and the speakers on the robot's mouth. However, if there is a need for an extra camera in some other area on robots for certain purposes, such as on the robots' back or near the robots' legs, then the camera should be designed and placed to be clearly noticed by the users.

In addition, it could be more secure if we design automatic covers that are placed on robots' cameras to work as human eyelids, and on the robots' microphone. Therefore, those covers could be used when needed to protect users' privacy during the robots' working period to perform tasks and after the robots have finished their tasks.

Furthermore, the robots can be equipped with a small touch screen that could be hidden inside the robots' body if it is not needed by users, or that can be added as an additional object on robots and removed if users do not need it. The users can use the smart screen for controlling the robots, adjust the setting of robots, or perform many other functions. In addition, the robots can use this screen to display information to their users, provide services to users, or perform other services.

3.2 Constraining Robots' Perception

3.1.1 Constraining Robots' Cameras

We can notice from the previous works that the techniques that were used by the researchers for constraining what the robots can see could draw attention in different levels and lead the watcher to ask questions about the hidden object and information. This could cause another type of risk to the users. Thus, we propose new methods that could prevent this type of problem and that could increase the level of privacy protection.

The first technique, as we mentioned earlier, is to use the automatic covers, as humans' eyelids, during the robots' working period and when the robots finish their work. During the robots' working time, the users can tell the robots to close their eyes (camera) when they want that from the robots by using words, such as "close your eyes (cameras)." In addition, the robots can use those covers when they are programmed to avoid certain objects, areas, or situations, such as when they are detecting a naked person. The robots could cover their eyes (camera) temporarily, as human blinking, until they go far away from the situation or object that they have to avoid or until the users ask them to reopen their eyes (cameras) again by using words, such as "open your eyes (cameras)." The objects, areas, and situations that the robots have to avoid to protect users' privacy will be programmed earlier by allowing robots to use a particular database or network. The covers can also be used when the robots finish their tasks, turned off, and go to rest. In fact, the covers could be the best and the more comfortable solution for users who are obsessed with privacy protection. Since the camera will be covered, if the camera is turned on accidentally, blackness will be the only thing that can be seen and recorded.

The second technique is using our proposed filter, which is the adaptive "delete and replace" filter that works by deleting the target object and replacing it with another nearest object that looks like it. The target objects and the objects that are similar to the target objects could be stored on a database as the simplest way of linking the target objects with the other objects that could be used instead of the original ones. For example, the filter could delete the credit card object and replace it with any business or restaurant card. (See Figure 1).

Figure 1: The left image is the original image and the second image is our proposed adaptive filter "delete and replace"

In addition, this technique could work with a target object that has another object placed above it (see Figure 2).

Figure 2: The left image is the original image and the second image is our proposed adaptive filter "delete and replace"

In Figure 3, the images on the left and the right, from top to bottom, show the original image, abstract, blur, redact, replace, and our proposed filter. Indeed, the images on the right are taken from the previous study except for the last one, which is our proposed filter that we added for comparison [11]. This figure can show how our proposed filter can solve the problem of drawing attention to the protected object.

3.1.2 Constraining Robots' Microphones

Violating personal privacy via hearing private information could cause a problem. Because social robots have the ability to listen to and record, the need for protecting the privacy of audio is considered as a significant step to protect users' privacy. Thus, we proposed different techniques that could be used on the robots' microphone, and that could assist in mitigating the violation of users' privacy.

Figure 3: The images on the left and on the right, from the top to the bottom, show the original image, abstract, blur, redact, replace, and our proposed filter

The first technique is to use the automatic covers, which are similar to the covers that could be used on the robots' camera. The covers can also be used while the robots are working and after they have completed all of their tasks and gone to rest. During the working time, the users can tell the robots to close their ears (microphones) when they want that from the robots, by using words, such as "close your ears (microphones)."

In addition, the robots can use those covers when they are programmed to avoid certain situations, such as when they are detecting a person calling via phone or talking with others. The covers can also be used after the robots have completed their tasks, turned off, and gone to rest. As we mentioned before, this method could provide more comfort to the users who are obsessed with protecting their privacy.

In fact, because many studies asserted that most robots used unencrypted audio, this audio could have private data that could be collected and recorded, which would violate users' privacy. For this problem, we suggested the second technique, which is to use an encryption mechanism that is similar to those that are used with smart speakers to protect users' privacy. The encryption mechanism is to encrypt all the words that a robot can hear until the robot hears its wake-up word, such as its name. Then the robot would respond to the voice. If the users stop saying anything, the robot could wait for several seconds and then start to use encryption again.

3.3 Constraining Robots' Navigation (Movement)

Different techniques are used to constrain the robots' movements, and most of them are promising. Indeed, because it seems like many people are using many various sensors in their environments, such as at their houses and workplaces for many different purposes, such as facility, safety, and security, we proposed other techniques for constraining the robots' movements. The first technique is to connect the robots' sensors with the sensors in the robots' environment. For example, the robot's sensor could be connected with the movement sensor and infrared sensor, so if a user does not want the robot to enter a place where he/she is, the robot then will check the movement sensor with the infrared sensors, and if the robot detects that there is a person inside that place, the robot will not enter.

Furthermore, the robots can be programmed to respond to requests and commands, such as "do not enter," and "go away," and the robots can also be programmed to use words, such as "may I enter?"

Indeed, using multiple techniques would be the solution that the users would prefer to constrain the robots' movements.

3.4 Users' Authentications on Robots

The authentication system is significant in order to provide security, preserve privacy, and provide services for each user according to their preferences. The preferences for each user are stored on their profiles and could be used after authenticating.

In fact, using multi-factor authentication methods that combine the voice, face, and password could be appropriate for all users. The users could enter the password via the robots' program or via using their voices to activate the robots, and then the robots will use the voice or face for the continuous authentication process. In addition, the robots can build a unique profile for each user that stores all the user's preferences and services, and the robots can change that regarding each user's voice.

3.5 Robots Warning System

As we mentioned earlier, the robots have abilities that exceed the users' expectations, and the robots can do actions that could not be recognizable by users. Thus, using a warning system that assists in reflecting the actions of robots and making those robots more transparent is significant and could be required by the social robots' users. This system could increase the users' awareness about the robots' actions to be aware and cautious about the risk of privacy violations.

The warning system that we propose could use more than one method to make users aware of their robots. Thus, we suggested that the robots' factory must provide a booklet that contains guidance and instructions regarding each robot's capabilities and features in order to give the users complete and detailed knowledge about their robots, how they work, and what they can do. That information could be, for example, the robot's ability to record information, to see from their backs, to save information, the robots' sensors, and so on. That information and those instructions could also be saved and displayed on the robot's small screen, on the robot's program, on its application, on the device that comes with the robot, or could be said verbally by the robot itself.

In addition, as another warning system method, we can use different colors of lights for each capability of the robot. Those colors of lights could be used to make the users more aware of their robots and more cautious to protect their privacy. For example, we can use a color of light that appears statically around the robots' eyes (cameras) without moving when robots turn the camera on and use a color of light that appears and moves circularly when the robots record video with their cameras. Moreover, we can use a color of light that appears statically around the robots' ears (microphones) when the robots turn the microphone on and that appears and moves circularly when the robots record sound with their microphones. In addition, we can use a light when someone enters a room where there are robots. Moreover, we can use a color of light on the robot's head when the robot is connected to the Internet. Finally, we can use a color of light when the robots are on or off. Indeed, we can use a color of light when any sensors of robots are turned on.

The other method of warning system is allowing the robots who could be far away from their users to alert them by using a sound, which means informing their users' verbally (loudly).

3.6 Robot Application

To the best of our knowledge, there are some applications that are used only for controlling the robots, their functions, and their general settings, such as controlling the audio volume, speech volume, speech-language, system reboot, and moving the robots. Thus, it could be more effective, comfortable, and secure if we can use those applications to control, manage, and adjust the security and privacy setting on a robot's system.

As we mentioned, the robots could provide a profile via voice authentication. With the privacy setting, the users could adjust the unique privacy techniques that they prefer. For example, some users prefer using different types of filter techniques or warning system techniques. The users could be able to adjust all of that according to their preferences

4. METHODOLOGY

As we mentioned before, the research aims to provide different types of techniques that are used to produce privacy-sensitive robots and that are comfortable and preferred by the social robots' users. In order to learn more about users' privacy concerns and examine our proposed techniques to determine if they are comfortable, trusted, and preferred by the social robots' users or not, we conducted three different surveys and one experiment. The goals of those surveys and the experiment were to gather information about the users' privacy concerns, users' opinions toward the techniques for protecting privacy, users' opinions towards features of robots relevant to privacy, and users' opinions towards techniques of robots for increasing people's awareness regarding privacy.

By using the methodologies, the total number of participants who were recruited in this user study reached 150, of which 82 participated in the main survey, 40 of them in the Cameras' Covers survey, 20 of them in the Filters' Effects survey, and eight of them in the experiment. The participants were employees at FIT or FIT students whose ages above 18 and were from both genders. In addition, the participants were from different nationalities.

5. STUDY ANALYSIS AND RESULTS

Regarding the "Cameras' Covers" Survey, we distributed the survey to figure out if participants use any different types of covers to cover their cameras, and 40 participants responded to this question. The result illustrated that there were 26 participants (65%) who use a cover for protecting their privacy.

Regarding the "Filters' Effects" Survey, we distributed the survey discover if the proposed filter, which is "delete and replace," can solve the problem of drawing attention and that could be preferred by users to protect their privacy. We informed the participants that in all the pictures, there is an object that we were trying to hide, and we asked them which pictures shows that there is no manipulation and makes sense. The results indicated that most participants chose picture number 5, that used "delete and replace" filter, as the picture that shows that there is no manipulation and that seem real. In addition, we asked the participants what are the filters that they prefer their robots to use in order to protect their privacy are. The results showed that most participants preferred the "delete and replace" filter (see Figure 4). The first two Figures from the left show the results of the questions that aimed to discover if the

proposed filter, which is "delete and replace," can solve the problem of drawing attention. The last Figure shows the preferred filter. Picture1 shows abstraction, picture 2 shows replace, picture 3 shows redact, picture 4 shows blur, and picture 5 shows "delete and replace."

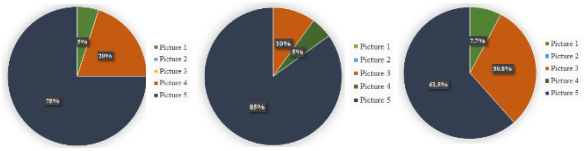

Figure 4: The results of the questions of the "Filters' Effects" Survey

Regarding the main Survey, there were six parts in this survey: the demographic questions, questions about general background, questions about users' concerns, questions about constraint techniques, questions about the robots' additional features for privacy protection, and questions regarding a warning system.

Regarding the general questions, we asked the participants if there is a social robot at their home, workplace, or near them. The results demonstrated that most of the participants (85.4%) did not have a social robot or did not see a social robot around them while (14.6%) of participants have a social robot at their home, workplace, or around them.

For the participants who have a social robot, 12 out of 82, we asked them to identify where they use the social robot. The participants were able to choose more than one option. The results revealed that ten of the participants have a social robot at home while two of them have it at their workplace, and two of them mentioned that they had it at their school when they chose option "other."

For the participants who do not have a social robot, 70 out of 82, we asked them if they wanted to have a social robot or not. The results indicated that most of the participants (40%) said that they might plan to own a robot, and the second large group (37.1%) confirmed their desire to own a robot. However, a few (8.6%) said that they do not know yet if they want to have a social robot or not, and the rest of participants (14.3%) reported that they do not want to have a social robot. In addition, those participants who do not have a social robot and want to have one were also asked when they have a social robot, where do they want to use it? In this question the participants were also able to choose more than one place. However, the results demonstrated that most of the participants (78.6%) want to own a social robot at their home while (42.9%) of participants want to have a social robot at their workplace. However, four out of 70 participants went with the option "other." Although one of those wanted to use the social robot at the kids' places to monitor them, the rest mentioned they did not want to use the social robot anywhere for protection purposes.

Regarding the users' concerns questions, we asked the participants the following: "If you have or could have a social robot in your home, work, or near your environment, what are your most general concerns about the social robot assuming that the social robot could record and store video and audio records or data being streamed in a control center?" The results indicated that most of the participants (59.8%) were concerned most about people who could hack social robots, so the hackers then could do harm to or spy on those users. The second majority concern was the video or audio recording ability of the social robots that could be misused or leak. However, few participants were concerned about targeted advertising and responsibility for damage or harm; the numbers of participants in percentages (25.6%) and (19.5%) are given respectively (see Figure 5).

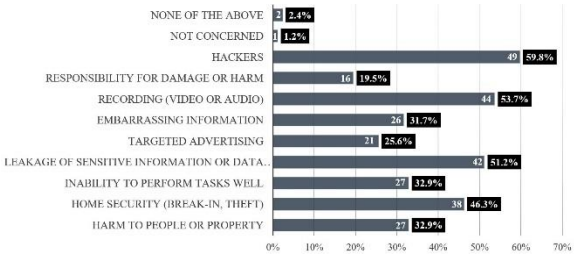

Figure 5: The users' concerns about the social robots

In addition, we sought to know more about the privacy concerns for users regarding certain objects, information, locations, and situations. Thus, we used the scale (Extremely Concerned, Concerned, Neither Concerned nor Unconcerned, Unconcerned, and Extremely Unconcerned), and we asked the participants the following: "How concerned are you about privacy related to the following: Objects, Information, Locations, and Situations?" Indeed, the participants were required to rank every object and location while they had the choice to rank every bit of information or some, and every situation or some. The results could be summarized in Figure 6,7,8, and 9.

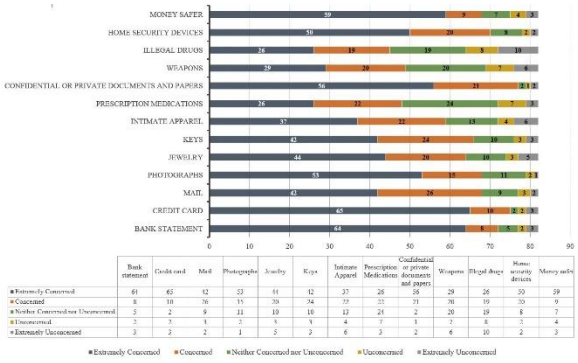

Figure 6: Participants' rating regarding the objects that they are concerned about regarding privacy

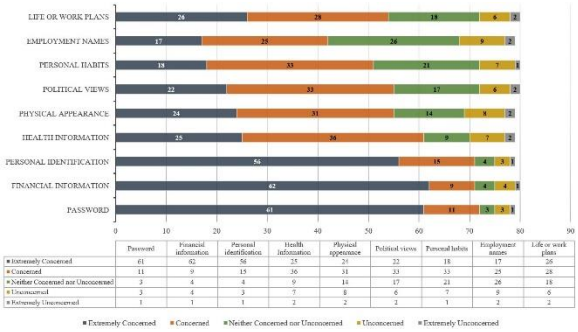

Figure 7: Participants' rating regarding information that they are concerned about regarding privacy

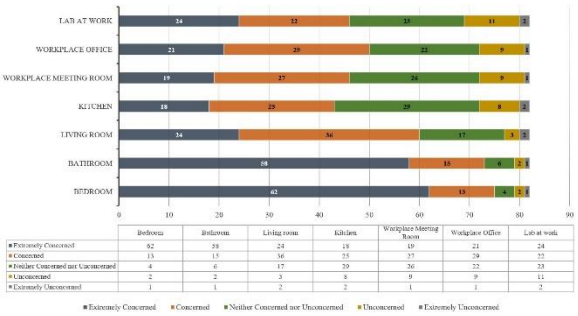

Figure 8: Participants' rating regarding the locations that they are concerned about regarding privacy

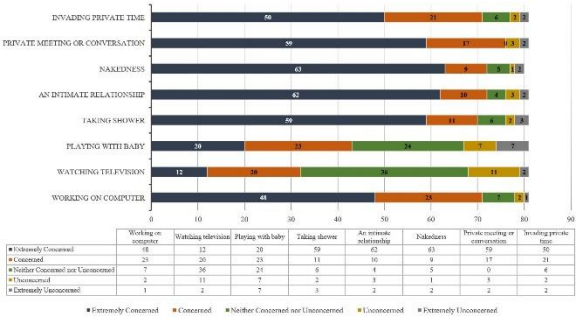

Figure 9: Participants' rating regarding the situations that they are concerned about regarding privacy

Regarding the constraint techniques, we asked the participants to choose the most preferred techniques that they want to use on their social robots in order to have privacy-sensitive social robots. Thus, we asked the participants about the most preferred techniques that could be used on robots' cameras during the robots' working period and when its working time is finished. In addition, we asked the participants about the most preferred techniques that could be used on robots' microphones during their working period and when the working time is finished. Finally, we asked the participants about the most preferred techniques that could be used in order to limit the robot's movements while performing a task.

Regarding the robots' cameras, we asked the participants the following: "What are the most trusted and comfortable ways that could be used with the robot's camera while performing a task to provide privacy (e.g., credit card)." The results showed that half of the participants, 41 out of 82, preferred using both the adaptive filters and the automatic hardware covers. However, a few participants, nine out of 82, preferred using a type of filter, such as blurring, pixelation, redacting, or replacing that changes the appearance of only the private part of the image/scene (only the credit card) that is seen by the robot (see Figure 10).

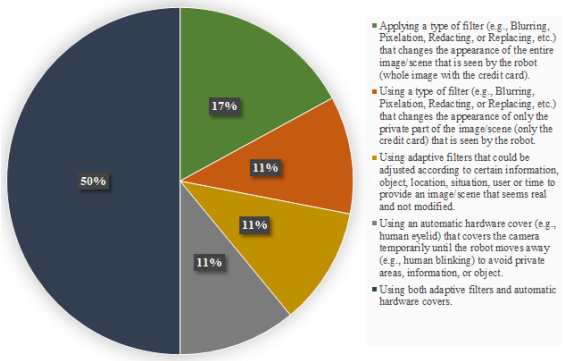

Figure 10: Participants' preferences regarding the ways that could be used with the robot's camera while performing a task to provide privacy

In addition, we asked the participants the following: "What are the most trusted and comfortable ways that could be used with the robot's camera while performing a task to protect private situations (e.g., changing clothes)?" The results demonstrated that most of the participants (51.2%) preferred using multiple techniques, which were mentioned on the other choices. A few participants (2.4%) wanted their robots to automatically turn and walk away when detecting a private-sensitive situation. Indeed, the second preferred technique was using adaptive filters. This method was attractive to (15.9%) of the participants, followed by the technique of using an automatic cover, such as a human eyelid that covers the camera temporarily until the robot moves away. This is like a human blinking in order to avoid private-sensitive situations. This method was chosen by (13.4%) of the participants (see Figure 11).

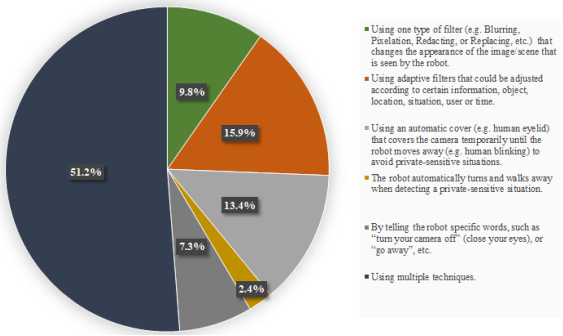

Figure 11: Participants' preferences regarding the ways that could be used with the robot's camera while performing a task to protect private situations

Furthermore, regarding the robots' cameras, we asked the participants this last question, which was "what are the most trusted and comfortable ways that could be used to disable the camera (turn the camera off) after finishing?" The results indicated that most participants (35.4%) preferred using the automatic cover that covers the robot's camera completely after finishing tasks. However, a few participants (14.6%) chose to turn the Internet connection off in order to protect their privacy (see Figure 12).

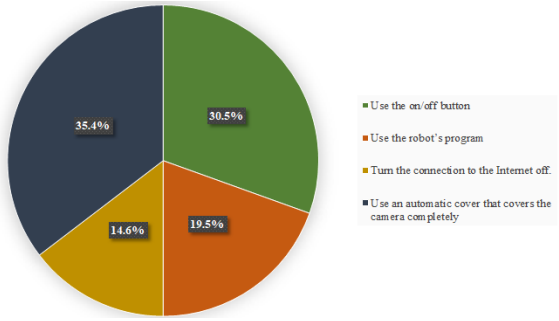

Figure 12: Participants' preferences regarding the ways that could be used with the robot's camera to disable the camera after finishing tasks

Regarding the robots' microphones, we asked the participants the following: "What are the most trusted and comfortable ways that could be used to disable the microphone while performing a task?" The results illustrated that most participants (37.8%) preferred turning the microphone off by using the on/off button for the microphone to protect privacy. However, the second large group of participants (31.7%) preferred using the automatic cover that covers the microphone completely when the robot does not require the microphone to complete the task (see Figure 13).

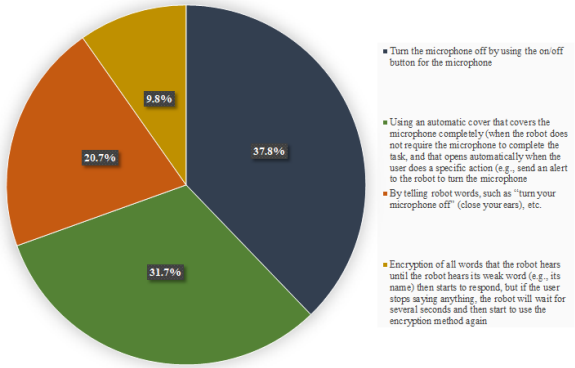

Figure 13: Participants' preferences regarding the ways that could be used with the robot's microphone while performing a task to protect privacy

In addition, we asked the participants the following: "What are the most trusted and comfortable ways that could be used to secure the microphone after finishing tasks?" The results showed that most of the participants (34.1%) preferred using the automatic cover that covers the microphone completely; however, a few participants (15.9%) preferred turning the connection to the Internet off (see Figure 14).

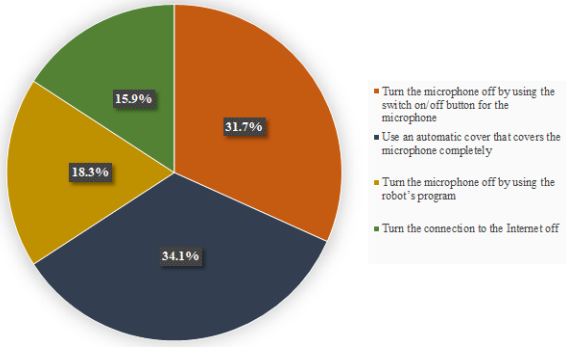

Figure 14: Participants' preferences regarding the ways that could be used with the robot's microphone after finishing tasks to protect their privacy

Regarding the robots' movements, we asked the participants the following: "What are the most trusted and comfortable ways that could be used to limit the robot's movement while performing a task to protect private areas?" The results revealed that most participants (45.1%) preferred using multiple techniques, which were mentioned on the other choices. The second large group of participants (22%) preferred to tell the robot specific words, such as "go away," or "do not enter" in order to limit their movements. However, a few participants (13.4%) preferred that the robots use navigation (see Figure 15).

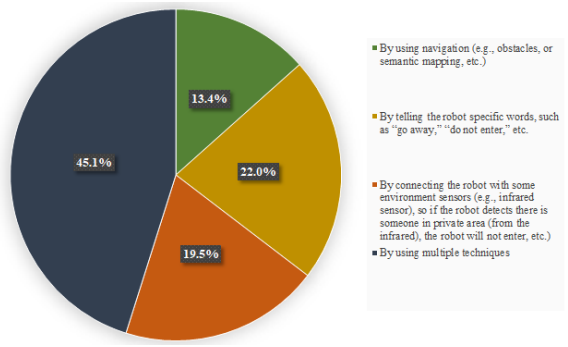

Figure 15: Participants' preferences regarding the ways that could be used to limit the robot's movement while performing a task to protect private areas

Regarding the additional features of the social robot for privacy protection, we asked the participants the following: "If you have a social robot at home or workplace, do you want to allow every household member or workplace member to use the robot?" Additionally, we asked them "if

other members use your social robot, do you prefer to add an authentication feature on it?" The results of both questions could be seen in Figure 16 and 17.

For the question: "What are the most appropriate authentication methods that the social robot can use to authenticate the authorized user?" we gave them the ability to choose more than one method. The results demonstrated that most of the participants (62.2%) wanted to use the face recognition method, followed by the password (58.5%), and lastly, the voice recognition method (56.1%). However, a few of the participants mentioned other types of authentication methods, such as fingerprint, multi-factors methods, and NFC. The numbers of participants in percentages were (4.8%), (6%), and (1.2%), respectively.

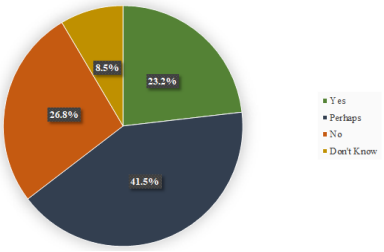

Figure 16: Users' desire to allow sharing the use of their social robots

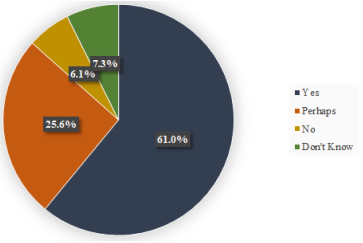

Figure 17: Users' desire to add an authentication method on the social robots that are used by different members

Additionally, in order to know if the users prefer managing and controlling the policies of their social robots by themselves, we asked the participants the following: "Do you think having policies to control the social robots' permissions and limitations, such as controlling the permission policies to access the contacts, locations, or photos could assist in mitigating the problem of privacy violation?" The results illustrated that the majority of participants (58.5%) believed that having policies to control the social robots' permissions and limitations could assist in mitigating the problem of privacy violation. However, a few participants (2.4%) did not believe this feature could assist in mitigating the privacy violation. The second group of participants (32.9%) said having policies to control the social robots' permissions and limitations may assist in protecting their privacy while (6.1%) of them do not know if this feature could solve the problem of violating the users' privacy or not.

Regarding the last part, the awareness/ warning system, we started this part with the following question: "Do you believe that having a warning system that reflects the robot transparency could assist in mitigating a privacy violation?" The results demonstrated that the majority of participants (51.2%) believed that having a warning system on their social robots could assist in mitigating the privacy violation while a few participants (4.9%) did not believe that. See Figure 18.

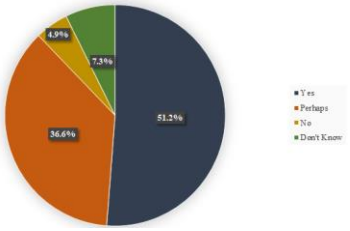

Figure 18: Participants' opinions regarding whether or not the warning system could help in mitigating a privacy violation

In order to know more about the warning system that users would prefer, we asked them several questions. We started with the following: "Do you prefer that the social robot send you alerts when it moves toward you?" The results revealed that (41.5%) of the participants preferred that their social robot send them alerts when they are moving toward them while (13.4%) did not want to receive any alerts from their social robots when those robots move toward them. The second large group of participants (40.2%) were not sure and they clarified that they might prefer their social robots to send them alerts, while (4.9%) of those participants did not know if they wanted that or not.

In addition, we asked the participants if they could have that warning method and their social robots have to send them alerts when they are moving toward them, how do they prefer the robot send them the alerts? We let them choose more than one answer. The results indicated that most of the participants (45.1%) preferred that their robots inform them about moving toward them verbally (loudly). However, the second large group of participants (40.2%) preferred that their robots send a message to their smartphones to inform them. Others (19.5%) also preferred their robots to send them a message, but to the device that comes with the robot. However, (20.7%) of the participants chose none of the above as their answer.

Furthermore, we asked the participants how they prefer the social robot alert users who do not notice its existence, such as if the robot is hidden behind a sofa so the user cannot see it? We let them choose more than one answer. The results could be seen in Figure 19.

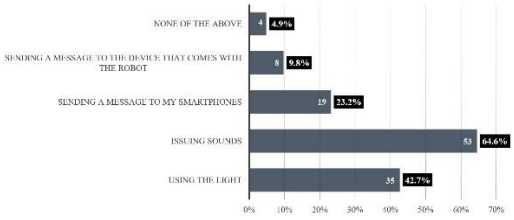

Figure 19: Preferred warning methods to alert users who do not notice the robot's existence

Moreover, we asked the participants the following: "Do you prefer that the social robot turn on a specific color of light around its camera and microphone or other sensors to show when these sensors are on, off, or when they are recording?" The results showed that most of the participants (73.2%) preferred that the social robot turns on a specific color of light around its camera and microphone or other sensors to show when these sensors are on, off, or when they are recording while only a few (2.4%) did not prefer that. However, (20.7%) of the participants were not sure and said they may want their social robot to turn on a specific color of light around its camera and microphone or other sensors for warning while a few of them (3.7%) said they did not know.

Lastly, we asked the participants the following: "How do you prefer the social robot to announce its capability (see, record, listen, etc.)?" We allowed them to choose only one answer. The result indicated that most of the participants (32.9%) preferred that their robots inform them about their capabilities verbally. The second large group (26.8%) preferred their robots to use a specific color of light for each capability while (17.1%) of the participants wanted to be informed about the robot's capabilities via the robot's small screen that is a part of the robot's body. However, other participants preferred to receive a message either to their smartphones or the device that comes with the robots. The percentages of the participants were (19.5%) and (3.7%), respectively.

6. CONCLUSION

Robots have evolved very quickly and have become a form of technology that is equipped with sophisticated features. Nowadays, robots can be found everywhere. Indeed, the social robots that have the ability to communicate with humans to sense, hear, watch, process, and record all of their environments definitely contain a lot of their private information. Thus, they could violate the users' privacy. In fact, there are many different sources that cause this violation, such as the robots' cameras and microphones, the outer shape of the robots, the robots' movements, the lack of the reliable authentication system, the lack of robots' warning system, and the characteristics of the application that can be used for controlling and management.

Thus, using social robots, which have advanced sensors or which lack some essential features which could assist in mitigating the privacy violation, cause privacy concerns. In this research, we reviewed issues and limitations regarding protection of users' privacy. Then we used surveys to analyze solutions that assist in solving the problem of privacy violation and producing privacy-sensitive robots. This identifies the most trusted, comfortable, and usable techniques that could assist in protecting users' privacy while using social robots, increasing users' awareness toward privacy risks, balancing between the utilities achieved and privacy loss.

7. REFERENCES

[1] Pranav Mistry. Brainy quote. https://www.brainyquote.com/search_ results?q=fiction+technology, 2018.

[2] Oleksandr Shyvakov. Developing a security framework for robots. Master's thesis, University of Twente, 2017.

[3] Allied Market Research. Robotics technology market. https://www. alliedmarketresearch.com/robotics-technology-market, 2018.

[4] Statista. Size of the global market for industrial and non-industrial robots between 2017 and 2025. https://www.statista.com/statistics/760190/ worldwide-robotics-market-revenue/, 2018

[5] Ramesh Subramanian. Emergent ai, social robots and the law: Security, privacy and policy issues. Subramanian, Ramesh (2017)" Emergent AI, Social Robots and the Law: Security, Privacy and Policy Issues," Journal of International, Technology and Information Management, 26(3), 2017.

[6] Christoph Lutz and Aurelia Tam`o. Privacy and healthcare robots–an ant analysis. In We Robot 2016: the Fifth Annual Conference on Legal and Policy Issues relating to Robotics. University of Miami School of Law, 2016, Discussant: Matt Beane, University of California Santa Barbara, 2016.

[7] Bill Gates. A robot in every home. https://www.scientificamerican.com/ article/a-robot-in-every-home/, 2018.

[8] Marcus Woo. Robots: can we trust them with our privacy. http://www.bbc. com/future/story/20140605-the-greatest-threat-of-robots, 2018.

[9] Min Kyung Lee, Karen P Tang, Jodi Forlizzi, and Sara Kiesler. Understanding users' perception of privacy in human-robot interaction. In Proceedings of the 6th international conference on Human-robot interaction, pages 181–182. ACM, 2011.

[10] IEEE Organization. Play face-off. https://robots.ieee.org/play/, 2019.

[11] Alexander Hubers, Emily Andrulis, William Smart, Levi Scott, Tanner Stir- rat, Duc Tran, Ruonan Zhang, Ross Sowell, and Cindy Grimm. Video manipulation techniques for the protection of privacy in remote presence systems. volume 2-05-, pages 59–60. ACM, 2015.

[12] Clark Fouraker. Robotic security forces on patrol in nyc prompt privacy concerns for some. https://newyork.cbslocal.com/2018/10/16/ knightscope-robot-security-patrol/, 2018

[13] Jeffrey Klow, Jordan Proby, Matthew Rueben, Ross Sowell, Cindy Grimm, and William Smart. Privacy, utility, and cognitive load in remote presence systems. volume 126657, pages 167–168. ACM, 2017.
[14] Jenay M Beer and Leila Takayama. Mobile remote presence systems for older adults: acceptance, benefits, and concerns. In 2011 6th ACM/IEEE International Conference on Human-Robot Interaction (HRI), pages 19–26. IEEE, 2011.
[15] Kelly Caine, Selma ˇSabanovic, and Mary Carter. The effect of monitoring by cameras and robots on the privacy enhancing behaviors of older adults. Pages 343–350. ACM, 2012
[16] Dag S. Syrdal, Michael L. Walters, Nuno Otero, Kheng L. Koay, and Kerstin Dautenhahn. "He knows when you are sleeping" - privacy and the personal robot companion. volume WS-07-07, pages 28–33, 2007.
[17] Margaret M Krupp, Matthew Rueben, Cindy M Grimm, and William D Smart. A focus group study of privacy concerns about telepresence robots. In 2017 26th IEEE International Symposium on Robot and Human Interactive Communication (RO-MAN), pages 1451–1458. IEEE, 2017.
[18] Matthew Rueben, Frank Bernieri, Cindy Grimm, and William Smart. Framing effects on privacy concerns about a home telepresence robot. volume 127194, pages 435–444. ACM, 2017
[19] Daniel J Butler, Justin Huang, Franziska Roesner, and Maya Cakmak. The privacy-utility tradeoff for remotely teleoperated robots. In Proceedings of the Tenth Annual ACM/IEEE International Conference on Human-Robot Interaction, pages 27–34. ACM, 2015.
[20] Margaret Krupp, Matthew Rueben, Cindy Grimm, and William Smart. Privacy and telepresence robotics: What do non-scientists think? pages 175–176. ACM, 2017.
[21] Paul Robinette, Alan R Wagner, and Ayanna M Howard. Building and maintaining trust between humans and guidance robots in an emergency. In 2013 AAAI Spring Symposium Series, volume SS-13-07, pages 78–83, 2013
[22] Anja Austermann, Seiji Yamada, Kotaro Funakoshi, and Mikio Nakano. Does the appearance of a robot affect users' ways of giving commands and feedback? In 19th International Symposium in Robot and Human Interactive Communication, pages 234–239. IEEE, 2010.
[23] T. Kanda, T. Miyashita, T. Osada, Y. Haikawa, and H. Ishiguro. Analysis of humanoid appearances in human-robot interaction. IEEE Transactions on Robotics, 24(3):725–735, 2008.
[24] Roy de Kleijn, Lisa van Es, George Kachergis, and Bernhard Hommel. Anthropomorphization of artificial agents leads to fair and strategic, but not altruistic behavior. International Journal of Human - Computer Studies, 122:168–173, 2019.
[25] Michael L Walters, Dag S Syrdal, Kerstin Dautenhahn, Ren´e Te Boekhorst, and Kheng Lee Koay. Avoiding the uncanny valley: robot appearance, personality and consistency of behavior in an attention-seeking home scenario for a robot companion. Autonomous Robots, 24(2):159–178, 2008.
[26] Aaron Powers, Sara Kiesler, and Jennifer Goetz. Matching robot appearance and behavior to tasks to improve human-robot cooperation. Technical report, Figshare, 2018.
[27] Francisco E. Fernandes, Guanci Yang, Ha M. Do, and Weihua Sheng. Detection of privacy-sensitive situations for social robots in smart homes. Volume 2016-, pages 727–732. IEEE, 2016.
[28] Margaret M. Fleck, David A. Forsyth, and Chris Bregler. Finding naked people. volume 1065, pages 594–602, 1996.
[29] Michael S. Ryoo, Brandon Rothrock, Charles Fleming, and Hyun J. Yang. Privacy-preserving human activity recognition from extreme low resolution. 2016.
[30] M. Boyle, C. Edwards, and S. Greenberg. The effects of filtered video on awareness and privacy. pages 1–10, 2000.
[31] Qiang A. Zhao and John T. Stasko. Evaluating image filtering based techniques in media space applications. pages 11–18, 1998.
[32] Yuta Nakashima, Tatsuya Koyama, Naokazu Yokoya, and Noboru Babaguchi. Facial expression preserving privacy protection using image melding. Volume 2015-, pages 1–6. IEEE, 2015.
[33] Pavel Korshunov and Touradj Ebrahimi. Using face morphing to protect privacy. pages 208–213. IEEE, 2013.
[34] S. Jana, A. Narayanan, and V. Shmatikov. A scanner darkly: Protecting user privacy from perceptual applications. pages 349–363. IEEE, 2013.
[35] Matthew Rueben, Frank Bernieri, Cindy Grimm, and William Smart. User feedback on physical marker interfaces for protecting visual privacy from mobile robots. volume 2016-, pages 507–508. IEEE Press, 2016.
[36] Tamara Denning, Cynthia Matuszek, Karl Koscher, Joshua Smith, and Tadayoshi Kohno. A spotlight on security and privacy risks with future household robots: attacks and lessons. pages 105–114. ACM, 2009.
[37] Steven M. Lavalle. Planning Algorithms, volume 9780521862059. Cambridge University Press, GB, 2006.
[38] Cipriano Galindo, Juan-Antonio Fern´andez-Madrigal, Javier Gonz´alez, Alessandro Saffiotti, ¨ Orebro universitet, and Akademin f¨or naturvetenskap och teknik. Robot task planning using semantic maps. Robotics and Autonomous Systems, 56(11):955–966, 2008.
[39] John T. Butler and Arvin Agah. Psychological effects of behavior patterns of a mobile personal robot. Autonomous Robots, 10(2):185–202, 2001.
[40] L. Takayama and C. Pantofaru. Influences on proxemic behaviors in human robot interaction. pages 5495–5502. IEEE, 2009.
[41] DoHyung Kim, Jaeyeon Lee, Ho-Sub Yoon, and Eui-Young Cha. A noncooperative user authentication system in robot environments. IEEE Transactions on Consumer Electronics, 53(2):804–811, 2007.

[42] Komal G Purohit and Raju J Bhiwani. Biometric authenticated voice operated robot.
[43] Woo-han Yun, DoHyung Kim, and Ho-Sub Yoon. Fast group verification system for intelligent robot service. IEEE Transactions on Consumer Electronics, 53(4):1731–1735, 2007.
[44] Keun-Chang Kwak. Face recognition with the use of tensor representation in home robot environments. IEICE Electronics Express, 6(4):187–192, 2009.
[45] Arnaud Ramey and Miguel Salichs. Morphological gender recognition by a social robot and privacy concerns: late breaking reports. pages 272–273. ACM, 2014.
[46] Pinki Kumari and Abhishek Vaish. Brainwave based user identification system: A pilot study in robotics environment. Robotics and Autonomous Systems, 65:15–23, 2015.
[47] Jonathan Vitale, Meg Tonkin, Sarita Herse, Suman Ojha, Jesse Clark, Mary- Anne Williams, Xun Wang, and William Judge. Be more transparent and users will like you: A robot privacy and user experience design experiment. Pages 379–387. ACM, 2018.
[48] Christoph Lutz and Aurelia Tam`o. Robocode-ethicists: Privacy-friendly robots, an ethical responsibility of engineers? pages 27–28. ACM, 2015.
[49] Kimberley Mok. This smartphone app can control robots with augmented reality. https://thenewstack.io/smartphone-app-can-control-robots-augmented-reality/, 2017.
[50] Bob Violino. Robot control: There's an app for that. https://www.zdnet. com/article/robot-control-there's-an-app-for-that/, 2016.