Exploring the Privacy Horizons: A Survey on HCI & HRI

Antonio Saporito, Parinaz Tabari(✉), Mattia De Rosa, Vittorio Fuccella, and Gennaro Costagliola

Department of Informatics, University of Salerno, Via Giovanni Paolo II, 84084 Fisciano (SA), Italy
ptabari@unisa.it

Abstract. With the constant evolution of technology and the rise of Human-Computer Interaction (HCI) and Human-Robot Interaction (HRI), Human-Technology Interaction (HTI) is becoming more important in everyday life, covering several routines closely linked to technology. In this survey, we aim to examine the important domain of user privacy in the contexts of HCI and HRI. Additionally, we analyze privacy issues, ranging from data collection to ethical and legal implications. Through a detailed analysis, we also highlight challenges and strategies for designing interactive systems that prioritize end-user privacy. This survey aims to provide a clear and comprehensive overview of the challenges and opportunities of integrating privacy into interactive systems. Finally, we will present the different strategies and techniques to be used, such as encryption and anonymization, to improve the level of privacy protection.

Keywords: Human-Computer Interaction · HCI · Human-Robot Interaction · HRI · Human-Technology Interaction · HTI · User Privacy · Ethics · Artificial Intelligence

1 Introduction

With the constant evolution of technology and the rise of Human-Computer Interaction (HCI) and Human-Robot Interaction (HRI), Human-Technology Interaction (HTI) is gaining more and more importance in everyday life, covering several routines closely linked to technology [19]. With the advent of new interactive and always-connected devices, innovative means of interaction between humans and technology have opened up, such as voice assistants, smart home devices, self-driving vehicles, and more. However, these devices have also raised new questions, concerns, and issues regarding the protection of personal data and user privacy [26]. According to the literature, data-driven technologies such as Big Data, Machine Learning, Cloud computing, and the Internet of Things can provide relevant benefits not only for improving production performance but also improve the working environment of humans. However, since these technologies

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2024
O. Gervasi et al. (Eds.): ICCSA 2024 Workshops, LNCS 14822, pp. 113–125, 2024.
https://doi.org/10.1007/978-3-031-65318-6_8

require the acquisition, communication, storage, and processing of personalized and potentially sensitive data of human workers, privacy concerns are becoming more relevant [8]. In the context of HCI, for instance, particular attention is paid to the widespread routine of unconscious data collection, which violates users' privacy, autonomy, and self-determination. These problems are exposed in many recent studies, where users are not informed or are unaware that data is being collected without their consent [18]. In addition, high-tech sectors, such as the automotive industry, are adopting new criteria for evaluating cybersecurity related to human-technology interaction; this represents a growing awareness of the importance of security and privacy considerations in the domain of human-robot interaction.

We aim to examine how these considerations apply to HCI and HRI in general by setting out the issues and strategies to minimize privacy risks. In this context, this survey undertakes an in-depth analysis of the complex world of privacy from various perspectives, considering the challenges posed by technological evolution, innovative design strategies, and the related methodologies required to preserve end-user privacy.

2 Methods

In this section, we analyze the proposed methodology that led to the drafting of this survey. It is necessary to use a suitable search methodology to investigate and analyze a research problem and explain which design strategies and techniques can be used to protect the privacy of end-users in HCIs and HRIs.

2.1 Keywords, Databases, and Search Strategy

The first step was to select the relevant keywords and scientific databases to extract information regarding our objectives. For this phase, we selected keywords such as "privacy", "HCI", "Human-Computer Interaction", "Human-Robot Interaction", "HRI","Human-Technology Interaction", and "HTI" with the Boolean operators "AND" and "OR" where necessary. Google Scholar, ACM Digital Library, Semantic Scholar, and IEEE Xplore were used as the academic databases for searching the documents.

2.2 Data Extraction

For this research, we used the most recent and relevant documents concerning our objectives. After the extraction of articles, a further check was performed by an initial scanning of the title and abstract of the papers. This was done to analyze the relevance of the paper to the problem and to check whether it was a potential candidate for further investigation. Subsequently, the full texts of selected articles in the previous phase were thoroughly read and the final articles were selected. As a final step, we extracted relevant information related to our objectives. In particular, each selected paper was annotated, by noting the

bibliographical data and its salient points (proposal/device), results, limitations, future work, and privacy considerations. The key documents for drafting this paper were original journal articles and conference papers. Some review papers were chosen for their useful basic concepts of privacy for end users.

3 Privacy: A Preliminary Analysis

The term privacy is a complex and multidimensional concept that plays a fundamental role in today's society. It influences various aspects of our daily lives, from the personal to the social and economic spheres. When we mention privacy, we refer to the ability of individuals to control access to their personal information and data while minimizing interference from unauthorized third parties. As privacy is a very complex concept, we can categorize it into different groups:

1. **Physical Privacy**: Physical privacy refers to the right of individuals to maintain control and privacy over their bodies, personal spaces, and physical personal information by restricting access to outsiders. This type of privacy encompasses both the home and work environment and includes the integrity of the body, preserving physical safety, and preventing unintended actions such as unauthorized photographs. Finally, there is the issue of freedom of movement which concerns the ability to move without being constantly monitored in both the physical and digital worlds [16].
2. **Data Privacy**: Data privacy concerns all digital interactions that people may have during their daily lives [31]. This type of privacy can in turn be divided into different spheres:
   - **Personal privacy** concerns with the protection of individual's identifying information such as name, address, and any information that organizations or services may collect [9];
   - **Financial privacy** deals with the sharing and protection of sensitive information related to personal finances such as banking transactions and investments while maintaining the integrity of financial transactions [6];
   - **Health privacy** refers to maintaining patients' sensitive medical data such as patient's name, date of birth, address, photos, ID card number, telephone number, and medical record number. This should be done while preserving privacy and data availability by anonymization and de-identification techniques. This type of privacy can also be referred to as personal privacy of patients [27]; The Health Insurance Portability and Accountability Act (HIPAA) act for privacy safeguards Protected Health Information (PHI) or identifiable health information of the individuals [7].
3. **Communications Privacy**: As technology continues to evolve, communications privacy plays a more fundamental role. It covers different communication aspects, from the protection of interpersonal communications that can take place via messages, and calls, to the confidentiality of digital interactions on social media. This important aspect concerns communications in the work environment, as business emails and conversations with colleagues should be private and secure [25].

4. **Information privacy**: Information privacy concerns the control over the disclosure of personal information such as the protection of an individual's beliefs and opinions, preventing them from being misused. Information privacy therefore relates to the right of individuals to determine the method, time, and scope of information to be disclosed to others [35]. Another aspect is creative expression, in that a person's artistic and creative works must be preserved.

It is important to emphasize that the different categories of privacy are not clearly distinguished and often interact with each other. Moreover, technological developments continue to redefine these notions, raising new challenges and doubts about privacy management.

4 Privacy Issues in HCI and HRI

The evolution of Human-Technology Interaction has generated a fusion of digital interfaces and interactive robots and created a new ecosystem rich in opportunities. However, there are challenges and issues regarding user privacy. As indicated in the literature, Privacy is a complex and multifaceted issue that has been studied in a variety of fields, including law, sociology, psychology, and computer science. In the context of HCI and HRI, privacy concerns arise when users interact with systems that collect, use, and share personal information [24]. In this section, we will explore how and what privacy implications for the user are generated by the intersection of interfaces and robots in different contexts and situations.

4.1 Privacy Issues in Voice Assistants and Connected Devices

Voice assistants and connected devices have become increasingly popular in recent years, which has taken human-technology interaction to very advanced levels. As HTI has evolved, new privacy issues have emerged, and "there are also several concerns including deception, infantilization, and privacy" [17]. One of the main problems with these devices is the collection and storage of users' sensitive data. Voice assistants such as Alexa and Google Assistant are designed to recognize and interpret voice commands, but this requires recording and analyzing the conversations users have with them. Furthermore, "the ontological categorization of voice assistants is nuanced with a particular categorization of Alexa as "object like" or "human-like" triggered in relation to the nature of the interaction (e.g., responsiveness) and the user's desire for social connection or companionship" [17]. However, this type of technology raises privacy concerns regarding the private conversations of individuals, as there could be the possibility of unauthorized access and listening to the devices, resulting in the disclosure of captured information. It is also possible for personal information to be inadvertently disclosed through secondary channels as a consequence of what you are doing; such secondary channels can be either connected devices or

voice assistants [22]. Another concern relates to data sharing by organizations that claim to use collected data to improve the user experience. However, there are doubts about the amount and nature of the sharing of collected data, and according to the literature, "personal data is the price people pay for access" [17] the benefits of these technological devices. However, other fundamental questions arise about transparency and user consent regarding how their data is used and shared. Tackling these issues requires a rigorous approach to privacy protection. In this respect, companies should ensure that collected data is encrypted during transmission and storage, thus reducing the risk of unauthorized access.

4.2 Privacy and Security Issues in Drone Use

Another technology that has become very popular in recent years is the use of drones in a wide range of fields, from the exploration of inaccessible territories to industry and recreational use.

However, their ability to collect data and fly over sensitive spaces has raised concerns about the protection of individual and collective privacy. As previous studies have shown, drones can violate users' privacy through unwanted intrusions into private spaces and observing these places [5]. The ability of drones to fly at low altitudes and the ability to record video and take photos could violate people's privacy in their homes or private spaces, triggering additional issues "such as fear of damage or injury and unwillingness to disclose personal information under drone surveillance" [5]. Another issue related to drones is that they may be equipped with technologies and sensors that can collect detailed information about the surrounding environment; this includes geographical, visual, and even biometric data. The collection and analysis of this data by third parties raise questions about data ownership and unwitting profiling of individuals. Furthermore, the transmissions used to control the drones and receive the collected data trigger another concern: the security of the transferred data. Such transmissions can be vulnerable to unauthorized access or cyber-attacks, compromising the confidentiality of the data collected and the privacy of the people involved. It is therefore important that drone users, both at the individual and organizational levels, address these concerns by implementing measures to ensure that people's privacy is respected; this includes regulating the use and encryption of data collected by drones.

4.3 Privacy Considerations and Issues About Social Robots in Public and Private Environments

"More affordable social robots are being commercially released and to implement viable applications of HRI, a combination of HCI, and user experience methodologies could play a pivotal role in assessing new scenarios and evaluating new investigations" [13]. This type of technology has considerable potential to improve people's daily lives. However, it collects sensitive information in new and different ways such as smartphones. The mobility and autonomy of these devices can threaten the privacy of end-users in unique and as yet unexplored

ways [15]. However, the constant exchange of information between people and robots and the increasing interconnectivity of these devices give rise to "scalability problems that make traditional security countermeasures inapplicable". Security flaws can cause damage to vehicles, financial losses, disclosure of sensitive personal data, and traffic accidents introducing additional privacy concerns for users [3]. In HRI, privacy concerns can arise when robots collect personal information about users, such as their location, activities, and preferences. Robots may also capture images and videos of users and their surroundings, raising concerns about surveillance and data security [24]. Social robots are designed to interact and assist people and they offer various applications in both public and private contexts.

In public settings, such as shopping malls, museums, entertainment venues, or healthcare, these robots can be designed to facilitate the public experience or simplify some work, while collecting a wide range of information. However, it is pointed out in the literature that the collection of biometric data, e.g. in healthcare, by robots may cause a violation of users' privacy, as this data is considered personal and confidential. In particular, it is emphasized that the collection of biometric and sensitive data requires the use of numerous sensors. The use of multiple sensors can be considered invasive and pose a threat to users' privacy. Furthermore, the collection of sensitive data by robots is inevitable during the entire human-robot interaction process, which makes the protection of privacy even more important for the effective use of this technology [32].

An experiment from the literature examines people's behavior towards a robot that exploits data collected from customers during interactions. Specifically, the aim of the experiment concerns the ability of robots to interpret privacy expectations in ambiguous social contexts, such as bars or spaces that could be considered both public and private spaces [10]. In private contexts, on the other hand, robots may collect and use users' personal information, such as conversations, consumption habits, and movements within the house. This may pose risks to users' privacy, such as unauthorized disclosure of personal information or non-consensual surveillance [35]. The use of these devices and the privacy issues associated with them will not be discussed in detail below as they have already been examined in Sect. 3. Social robots are also increasingly being made with anthropomorphic forms and, as a result, the use of voices and faces may be more familiar to the user. However, "an important factor to consider is that an anthropomorphic form may mislead or distort users' understanding of the robot's recording capabilities" [14].

4.4 Privacy Considerations about the Use of Apps

With the arrival of the digital era, a wide range of apps have also been introduced that are used in daily activities, giving people instant access to information, services, and entertainment. This has also led to an abuse of data collection by these apps and caused several privacy issues in this area as well. In this section, we will analyze the factors that tend to influence users on whether or not they want to continue using privacy-invasive apps and that could lead to emotional

distress. Nowadays, apps collect various information about users, from browsing preferences to geographical information. Even though they collect more and more data and information that is misused, users tend to continue to use these apps; this is due to factors such as convenience, ease of use, and attraction of these innovative features. As indicated in the literature, "the privacy paradox suggests that people may express concerns about privacy but continue to use privacy-invasive apps" [23]. This highlights how intrusiveness in the collection of personal information by apps can generate feelings of distrust in the digital environment. Despite this concept, the integration of these apps into everyday life tends to minimize emotional distress if they are needed for gaining practical benefits. The data collected by these apps, however, can be exploited to manipulate users' choices and behaviors. Therefore, there is a need for greater awareness among users about the risks of using these apps.

4.5 Privacy Considerations - Ethical and Legal Implications

The increasingly intense interaction between humans and technology entails several complex ethical and legal implications. Therefore, the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) in the United States are crucial in drafting regulations and practices related to these interactions. The GDPR is a European Union regulation that was enacted to strengthen data protection laws within the EU, giving people more control over the information being collected, processed, and stored by organizations. The CCPA is a privacy law in the United States and was drafted based in part on the GDPR; its purpose is equivalent to the GDPR with some differences in provisions. According to the literature, "Privacy is a fundamental human right that is protected by law in many countries. However, the design of ubiquitous computing systems often fails to take into account the privacy needs and expectations of users, leading to a range of privacy violations and negative user experiences." "Privacy concerns in HCI and HRI can be categorized into several dimensions, including data collection, data use, data sharing, and user control" [24].

From an ethical point of view, human-technology interaction raises important questions about privacy and the protection of personal data. In fact, the collection, processing, and storage of sensitive data often take place in a non-transparent or unclear manner; this can make users feel 'violated'. The GDPR stipulates that to collect and process data, informed user consent must be obtained and should ensure that the data collected is only used for legitimate and specific purposes. The GDPR has several provisions, including the 'Right to Data Portability', which is the right that people have to move their data from one system to another and it is important when a user wants to switch from one device to another. From a legal perspective, however, the CCPA in the US and its GDPR analog in the EU emphasize transparency, accountability, and individual control over personal data [11]. The CCPA also has several provisions, including the 'Right to Know', meaning individuals have the right to know what data is being collected and shared with companies, allowing them to have active

control over their privacy. This is a key point in human-technology interaction as data collection can influence personal decisions such as consumer or financial choices [21]. Technological evolution leads to some crucial questions:

- How can technological evolution be balanced with users' privacy protection?
- How can it be ensured that interactions between humans and technology respect people's rights?

In the next sections, we will investigate which design strategies and techniques attempt to answer these questions and discuss the approaches that seek to enable the preservation of individuals' privacy in the various contexts of human-technology interaction.

5 Techniques and Design Strategies for Privacy Preservation

The evolution of privacy-oriented design strategies has resulted in many techniques that preserve the confidentiality of data collected by systems and bring about a balance between the functionality of systems and respect for privacy. These strategies can address different privacy concerns and help define a more secure and trustworthy digital ecosystem. There are several strategies to preserve privacy in HCI and HRI contexts. These strategies can be considered as design guidelines for interactive systems [30]. Different strategies for privacy preservation are outlined below:

- **Data anonymization:** This strategy is the 'irreversible' and 'permanent' de-identification operation aimed at turning personal data into anonymous data before it is processed or shared. Anonymizing personal data means being able to make use of that information without obligations and responsibilities imposed by data protection regulations. Therefore, through the anonymization process, the risk of recognizing a user will be decreased [20,29].
- **Minimization of data collection:** This strategy involves collecting only the information that is strictly necessary for the proper operation of the system or application. Thus, it can reduce the exposure of personal data.
- **Pseudonymization:** This strategy, on the other hand, is the 'reversible' de-identification operation that can reduce the 'privacy risk'. This strategy replaces personal information with pseudonyms or unique identifiers, making direct association between data and individuals more difficult. The pseudonymized data can be attributed to a specific subject only by providing separately kept additional information [20]
- **Access Control:** With this strategy, suitable controls are implemented to determine who has access to the data and to what extent. This ensures that only people with the right authorizations can access the collected data [1].
- **End-to-end encryption:** This strategy guarantees, through encryption, the confidentiality of information by allowing access only to authorized people. Anyone who does not have the matching private key when transmitting and storing data will not be able to read it. This can prevent unauthorized third parties from accessing or compromising the collected data [2].

- **User consent management:** This strategy involves requesting explicit consent from users to be able to collect, process, or share data that is collected. It also allows the withdrawal of consent at any time the user wishes [12].
- **Privacy by Design:** This strategy aims to ensure a proper level of privacy and protection of personal data from the design phase of any system, service, product, or process as well as during their life cycle. This means that a proper level of data protection is ensured in all activities that involve the handling and processing of data within an organization [4].
- **Data retention limitation:** With this strategy, a specific period is defined for the retention of collected data. At the end of this period, the data will be automatically deleted or anonymized which can reduce the risk of retaining sensitive information for a long and unnecessary time.
- **Transparency and communication:** This strategy involves communicating clearly and explicitly to users about the application of collected data, thus building a base of trust and awareness [33].

Of the strategies and practices mentioned above, some of the most common methods for data protection and privacy protection are: data anonymization, encryption, and privacy by design. In the following we will examine these strategies and discuss why they are important and why they should be used in the design of interactive systems.

5.1 Data Anonymization

This strategy represents one of the first strategies adopted and is divided into four different techniques: masking, randomization, generalization, and layered anonymization.

- **Masking** removes all data that can directly identify the user (e.g. name and address), thus acting on the level of detail without altering the original data.
- **Randomization** alters the original data by separating the user from it and making it less accurate. As the altered data is no longer accurate, it makes it impossible to relate it to a specific individual [36].
- **The generalization of data** involves replacing more specific data entries with broader ones to prevent individual identification. This method is generally used in k-anonymity infrastructures and maintains data usefulness for analysis while preserving privacy [28].
- **Stratified anonymization** is also called re-anonymization. It focuses on anonymizing data already anonymized in a previous phase.

The choice of method to be used depends on the organization's needs; therefore, it must be done by carefully evaluating the database and the objectives to be achieved.

5.2 Encryption

Encryption, on the other hand, is the basis of data protection and is the most important way of ensuring that information cannot be stolen and read by unauthorized third parties. It is essential that a cryptographic algorithm offers:

- **authentication:** the process of attesting to the identity of each participant in a communication;
- **secrecy:** ensuring that no one can read a message, except the legitimate recipient;
- **integrity:** ensuring that no unauthorized alterations are allowed on a transmission, i.e. a message being sent to a recipient must not be altered before delivery;
- **non-repudiation:** providing the certainty that the sender of a message cannot deny having sent it.

Encryption, therefore, serves both to protect transmitted data from being altered or stolen by attackers and to authenticate a user. In encryption, there is a conversion of data from a readable format into an encrypted format that can only be read or processed after it has been decrypted. Only the authorized user can decrypt the data and access the information in its original format. There are plenty of methods to encrypt and decrypt data, but the key to success does not lie in the algorithm. The most important thing is to keep the encryption key (password) secret, or rather to make sure that only authorized persons know it.

5.3 Privacy by Design

Finally, the implementation of the 'Privacy by Design' concept is essential in the design of systems, applications, and technologies involving sensitive data. Indeed, according to the literature, "Design can play a critical role in addressing privacy challenges by incorporating privacy into the design of technologies and systems" [34]. The Privacy by Design approach implies the integration of privacy protection from the earliest stages of a system's development, ensuring:

- **Initial Respect for Privacy:** Privacy by design ensures that data protection is an integral part of the design, reducing risks and breaches.
- **Risk Prevention:** vulnerabilities are identified and addressed from the outset, minimizing security threats and intrusions.
- **User Confidence:** Demonstrates a strong commitment to privacy, increasing user confidence in the secure use of services.
- **Simplified Compliance:** Privacy by design simplifies compliance with privacy laws, thereby reducing legal risks.
- **Reduced Costs:** Providing reduced costs for privacy issues to be handled from the outset for future expenses associated with handling breaches or retroactive changes.

The combined use of these strategies thus makes it possible to minimize privacy risks due to HCI and HRI, but this is not always applicable in all contexts since technological evolution constantly proposes new privacy challenges. The different strategies listed above can also be considered as guidelines to be followed when implementing an interactive system that allows users' privacy to be preserved.

6 Conclusion

The analysis carried out on privacy considerations and issues in HCI and HRI contexts highlights the importance of carefully addressing emerging challenges related to the protection of user data. The constant integration of technology into everyday life has made it imperative to understand the risks and benefits inherent to privacy in human-technology interactions. In an increasingly connected technological world, ethical and legal dilemmas arise and there is a need to balance technological innovations with respect for people's rights by ensuring the protection of their data. Consequently, privacy considerations should start from the initial stages of designing a system, using as many data protection strategies as possible, including the "privacy by design" approach, to minimize the risk of breaches. User-centered system design thus becomes crucial, with a focus on creating innovative and satisfying experiences while respecting the users' privacy preferences. Users' awareness of privacy and the risks associated with HCI and HRI interactions is crucial. Educational campaigns that can help inform individuals about security practices, personal data management, and possible threats should be conducted to achieve greater empowerment. Furthermore, privacy regulations, such as GDPR and CCPA, indicate the increasing focus on the protection of personal data. Consequently, organizations should comply with these regulations while facing new challenges due to technological evolution. Legal compliance is indeed crucial, but it should be complemented by an ethical approach that goes beyond the legal obligation to ensure comprehensive privacy protection. In conclusion, facing new challenges due to technological evolution requires interdisciplinary collaboration and ongoing commitment to create interactive systems that respect the rights of individuals.

References

1. Anderson, R.: Access control. Wiley Data and Cybersecurity (2020)
2. Bai, W., Pearson, M., Kelley, P.G., Mazurek, M.L.: Improving non-experts' understanding of end-to-end encryption: An exploratory study. In: 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pp. 210–219. IEEE (2020)
3. Bakhtina, M., Matulevicius, R.: Information security analysis in the passenger-autonomous vehicle interaction. In: Proceedings of the 16th International Conference on Availability, Reliability and Security. ARES 21, Association for Computing Machinery, New York, NY, USA (2021). https://doi.org/10.1145/3465481.3470045
4. Cavoukian, A.: Understanding how to implement privacy by design, one step at a time. IEEE Consum. Electron. Mag. **9**(2), 78–82 (2020)

5. Chang, V., Chundury, P., Chetty, M.: Spiders in the sky: user perceptions of drones, privacy, and security. In: Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems. p. 6765-6776. CHI '17, Association for Computing Machinery, New York, NY, USA (2017). https://doi.org/10.1145/3025453.3025632
6. Chatzigiannis, P., Gu, W.C., Raghuraman, S., Rindal, P., Zamani, M.: Privacy-enhancing technologies for financial data sharing. arXiv preprint arXiv:2306.10200 (2023)
7. for Civil Rights, O.: Summary of the hipaa privacy rule (2003)
8. Coronado, E., Kiyokawa, T., Ricardez, G.A.G., Ramirez-Alpizar, I.G., Venture, G., Yamanobe, N.: Evaluating quality in human-robot interaction: a systematic search and classification of performance and human-centered factors, measures and metrics towards an industry 5.0. J. Manuf. Syst. **63**, 392–410 (2022). https://doi.org/10.1016/j.jmsy.2022.04.007, https://www.sciencedirect.com/science/article/pii/S0278612522000577
9. Dionne, X.: Collection of personal information in canadian law. Global Priv. Law Rev. **4**(2) (2023)
10. Hedaoo, S., Williams, A., Wadgaonkar, C., Knight, H.: A robot barista comments on its clients: social attitudes toward robot data use. In: 2019 14th ACM/IEEE International Conference on Human-Robot Interaction (HRI), pp. 66–74. IEEE (2019)
11. Hijmans, H., Raab, C.: Ethical dimensions of the GDPR, AI regulation, and beyond. Direito Público **18**(100) (2021)
12. Human, S., et al.: Data protection and consenting communication mechanisms: current open proposals and challenges. In: 2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pp. 231–239. IEEE (2022)
13. Khan, S., Germak, C.: Reframing HRI design opportunities for social robots: lessons learnt from a service robotics case study approach using UX for HRI. Future Internet **10**(10) (2018). https://doi.org/10.3390/fi10100101
14. Lee, M.K., Tang, K.P., Forlizzi, J., Kiesler, S.: Understanding users' perception of privacy in human-robot interaction. In: Proceedings of the 6th International Conference on Human-Robot Interaction, pp. 181–182. HRI '11, Association for Computing Machinery, New York, NY, USA (2011). https://doi.org/10.1145/1957656.1957721
15. Lutz, C., Schöttler, M., Hoffmann, C.P.: The privacy implications of social robots: scoping review and expert interviews. Mobile Media Commun. **7**(3), 412–434 (2019)
16. Mehta, V., Bandara, A.K., Price, B.A., Nuseibeh, B.: Wearables for physical privacy. In: Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct, pp. 942–945 (2016)
17. Pradhan, A., Findlater, L., Lazar, A.: "phantom friend" or "just a box with information": personification and ontological categorization of smart speaker-based voice assistants by older adults. Proc. ACM Hum.-Comput. Interact. **3**(CSCW) (2019). https://doi.org/10.1145/3359316
18. Punchoojit, L., Hongwarittorrn, N.: Research ethics in human-computer interaction: a review of ethical concerns in the past five years. In: 2015 2nd National Foundation for Science and Technology Development Conference on Information and Computer Science (NICS), pp. 180–185 (2015). https://doi.org/10.1109/NICS.2015.7302187
19. Rapp, A.: Human-Computer Interaction. Oxford University Press (2023). https://doi.org/10.1093/acrefore/9780190236557.013.47

20. Ribeiro, S.L., Nakamura, E.T.: Privacy protection with pseudonymization and anonymization in a health IoT system: results from OCARIoT. In: 2019 IEEE 19th International Conference on Bioinformatics and Bioengineering (BIBE), pp. 904–908. IEEE (2019)
21. Samarin, N., et al.: Lessons in VCR repair: compliance of android app developers with the California consumer privacy act (CCPA). arXiv preprint arXiv:2304.00944 (2023)
22. Schulz, T., Herstad, J., Holone, H.: Privacy at Home: an inquiry into sensors and robots for the stay at home elderly. In: Zhou, J., Salvendy, G. (eds.) ITAP 2018. LNCS, vol. 10927, pp. 377–394. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-92037-5_28
23. Seberger, J.S., Shklovski, I., Swiatek, E., Patil, S.: Still creepy after all these years: the normalization of affective discomfort in app use. In: Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems, pp. 1–19 (2022)
24. Seymour, W., Kraemer, M.J., Binns, R., Van Kleek, M.: Informing the design of privacy-empowering tools for the connected home. In: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, pp. 1–14. CHI '20, Association for Computing Machinery, New York, NY, USA (2020).https://doi.org/10.1145/3313831.3376264
25. Sivunen, A., Laitinen, K.: Digital communication environments in the workplace. Workplace Commun., 41–53 (2019)
26. Solera-Cotanilla, S., Vega-Barbas, M., Pérez, J., López, G., Matanza, J., Álvarez-Campana, M.: Security and privacy analysis of youth-oriented connected devices. Sensors **22**(11), 3967 (2022)
27. Su, J., Cao, Y., Chen, Y., Liu, Y., Song, J.: Privacy protection of medical data in social network. BMC Med. Inform. Decis. Mak. **21**, 1–14 (2021)
28. Sweeney, L.: Achieving k-anonymity privacy protection using generalization and suppression. Internat. J. Uncertain. Fuzziness Knowl.-Based Syst. **10**(05), 571–588 (2002)
29. Tahir, H., Brézillon, P.: A context approach to improve the data anonymization process. In: 2022 International Conference on Engineering and Emerging Technologies (ICEET), pp. 1–6. IEEE (2022)
30. Teresa Baldassarre, M., Santa Barletta, V., Caivano, D., Piccinno, A.: Integrating security and privacy in HCD-scrum. In: Proceedings of the 14th Biannual Conference of the Italian SIGCHI Chapter, pp. 1–5 (2021)
31. Ward, C., Ellis, D., D'Ambrosio, L.A., Coughlin, J.F.: Digital Breadcrumbs: a lack of data privacy and what people are doing about it. In: Kurosu, M. (ed.) HCI 2018. LNCS, vol. 10901, pp. 599–612. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-91238-7_46
32. Weng, Y.H., Hirata, Y., et al.: Design-centered HRI governance for healthcare robots. J. Healthcare Eng. **2022** (2022)
33. Wiencierz, C., Luenich, M.: Trust in open data applications through transparency. New Media Soc. **24**(8), 1751–1770 (2022)
34. Wong, R.Y., Mulligan, D.K.: Bringing design to the privacy table: broadening "design" in "privacy by design" through the lens of HCI. In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, pp. 1–17 (2019)
35. Yang, D., et al.: Effects of social behaviors of robots in privacy-sensitive situations. Int. J. Soc. Robot., 1–14 (2022)
36. Zhu, Y., Liu, L.: Optimal randomization for privacy preserving data mining. In: Proceedings of the Tenth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pp. 761–766 (2004)