Research Article

Anna Chatzimichali, Ross Harrison and Dimitrios Chrysostomou*

Toward privacy-sensitive human–robot interaction: Privacy terms and human–data interaction in the personal robot era

https://doi.org/10.1515/pjbr-2021-0013
received April 14, 2020; accepted October 29, 2020

Abstract: Can we have personal robots without giving away personal data? Besides, what is the role of a robots Privacy Policy in that question? This work explores for the first time privacy in the context of consumer robotics through the lens of information communicated to users through Privacy Policies and Terms and Conditions. Privacy, personal and non-personal data are discussed under the light of the human–robot relationship, while we attempt to draw connections to dimensions related to personalization, trust, and transparency. We introduce a novel methodology to assess how the "Organization for Economic Cooperation and Development Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data" are reflected upon the publicly available Privacy Policies and Terms and Conditions in the consumer robotics field. We draw comparisons between the ways eight consumer robotic companies approach privacy principles. Current findings demonstrate significant deviations in the structure and context of privacy terms. Some practical dimensions in terms of improving the context and the format of privacy terms are discussed. The ultimate goal of this work is to raise awareness regarding the various privacy strategies used by robot companies while ultimately creating a usable way to make this information more relevant and accessible to users.

* **Corresponding author: Dimitrios Chrysostomou,** Robotics and Automation Group, Department of Materials and Production Aalborg University, Fibigerstraede 16, Aalborg East, DK 9220, Denmark, e-mail: dimi@mp.aau.dk
Anna Chatzimichali: Department of Architecture and the Built Environment, University of West of England Frenchay Campus, Coldharbour Ln, Stoke Gifford, Bristol, BS16 1QY, United Kingdom, e-mail: Anna.Chatzimichali@uwe.ac.uk
Ross Harrison: Department of Engineering Mathematics, University of West of England Frenchay Campus, Coldharbour Ln, Stoke Gifford, Bristol, BS16 1QY, United Kingdom

Keywords: privacy-sensitive robotics, user privacy, personal data, human–robot interaction, human–data interaction

1 Introduction

We live in an era where collaborative robots have become an essential element of the industrial shop floor [1], and health-care robots are deployed to fight a global virus outbreak [2]. At the same time, domestic robots enter more modern households, and many users accept them as part of their everyday life [3,4]. As a result, we notice a booming increase in human–robot interactions where humans share workspaces, collaborative tasks, and, eventually, significant parts of their daily living environments with robots [5]. However, these human–robot interactions are as good as the data we feed them. Therefore, detailed records of user interactions may be crucial to uncover user needs, preferences, and expectations and develop systems that add value to the user [6]. Understanding the user's habits and lifestyle widens the opportunities to create a deeper connection with a robot and potentially manage more reliably user expectations. A trustworthy relationship in a human–robot interaction scenario is greatly dependent on the way such expectations are managed. Nevertheless, how could those records be used in a way that respects user privacy?

As Winfield and Jirotka [7] support in their work about how ethical governance enables the build of trust in robotics, it is not enough for organizations to only claim that they are ethical. Organisations have to also show how they are ethical. A great range of ethical principles, codes, guidelines, or frameworks have been introduced very recently [8]. At the same time, privacy and data governance were prioritized as a requirement in the recent Ethics Guidelines for trustworthy AI [9] by the EU Commission. This work moves the discussion from "what" those theoretical principles may be to "how" companies interpret or implement them in a more practical

setting when developing Privacy Statements and Terms and Conditions.

Privacy Policies and Terms and Conditions are developed behind the closed doors of each company. Companies take specific decisions on the information that will be included and the way to present such information to potential customers and users. As an example, some adopt the verbose and complex legal language, while others may present simple bullet points. This publicly available documentation not only provides cues signaling the level of privacy protection offered, but may also reflect part of the data governance policy along with the values of a company. For example, the way the most sensitive aspects of products are communicated to users may reflect a company's attitude toward user empowerment. Allowing users to have clarity and an increased level of choice or control over their data may demonstrate an overall vision related not only to privacy, but also to infer an organizational culture oriented to participatory design or decision-making.

This work presents an overview of issues related to the current legal standing on data governance regarding personal or consumer robots. We explore privacy issues and discuss the definitions of personal and nonpersonal data in the EU jurisdiction and their impact on personal and consumer robots. We integrate our previous work on personal data handling and privacy in human–robot relationships [10] and introduce a rating system for data handling related to human–robot interactions.

We investigate how the privacy guidelines developed by the Organization for Economic Cooperation and Development (OECD) are reflected upon the publicly available Privacy Statements and Terms and Conditions in the consumer robotics field. These privacy guidelines are the first internationally agreed privacy principles serving as a cross-border commitment to creating a global privacy protection framework. We compare Privacy Policies and Terms and Conditions of eight consumer robotic firms to understand how different practitioners adopt the OECD privacy guidelines in the field.

Currently, there have been no known studies that shed light on understanding how privacy is reflected in publicly available Terms and Conditions or Privacy Policies. This article attempts to bridge this gap by providing a comprehensive analysis of the ways well-established privacy principles (by the OECD) are reflected in the Terms and Conditions and Privacy Policies in the field of consumer robotics. Our goal is to contribute to the academic discourse in the nascent field of privacy-sensitive robots [11,12], increase the awareness regarding the various privacy strategies used by robot companies, and ultimately create a usable way to make this information more relevant and accessible to the public.

2 Privacy, personal data, and nonpersonal data

Is our regulatory framework ready for the adoption of robots in our private lives? Before posing this question, we need to clarify the point of reference for regulation. Regarding regulating robots themselves, the question seems to be difficult to be answered at the moment, especially as robots do not (yet) have consciousness or legal capacity to act. According to the European Civil Law Rules in Robotics [13], "For the time being, many legal sectors are coping well with the current and impending emergence of autonomous robots [...]". However, does this mean additional regulation is superfluous?

Considering the technological-neutrality argument regarding regulation [14], the law serves well when abstracted from specific technologies. In this sense, regulation should provide legal certainty to enable interpretation in new technological settings in robotics as much as in any other field. Despite the fact that the European data protection framework is technology-neutral and does not block technological adoption [15], the original question remains.

Rather than regulating robots *per se*, scholars agree that we need to concentrate on regulating the ways that people develop and interact with robots, while at the same time regulating any potential adverse effects that may arise due to the introduction of robots in our daily lives [16]. It has been noted that requirements regarding transparency, traceability, and human oversight are not covered in the existing legal or regulatory framework [17]. At the same time, the liability of AI and robotics forms a significant part of the policy-making agenda [18–20].

In this work, we specifically focus on issues related to privacy, data protection, and data governance that seem to be at an infant stage in the field of robotics. However, before considering the implications of privacy in robotics, it is worth highlighting the difference between data governance, data protection, and privacy, which are different but tightly linked constructs.

Data governance is a term related to the ways data are managed as a resource. At a company level, a data governance scheme or policy is based on organizational structures and details on how all data are created, collected, shared, protected, archived, and treated at their

end of life. Part of this may relate to customer or user data and is usually publicly communicated to consumers through publicly available Terms and Conditions/Privacy Policies/ Privacy Notices.

2.1 Privacy rights, informational privacy, and data protection

The term privacy, as well as the term rights, can have ambiguous meanings in ordinary language. As Newell [21] points out, "*theorists do not agree* [...] *on whether privacy is a behavior, attitude, process, goal, phenomenal state or what*." Similarly, the term rights can be interpreted in multiple ways: freedom, entitlement, privilege, power, claim, or immunities, while the meaning behind rights is deeply rooted in legal semiotics [22–24]. Recently privacy rights received great attention as an area of research, especially in tracing the origin and capturing the term's nature. The history of the emergence of privacy rights as a social, cultural, and legal idea is presented by Richardson [25], while Koops et al. [26] developed a comprehensive taxonomy and typology of privacy dimensions to clarify the distinction between the concept of privacy and privacy rights.

Judge Cooley provides a simple definition of privacy as the right "to be left alone" [27]. At the same time, privacy is reflected as a fundamental human right in the EU Charter of Fundamental Rights and the European Convention on Human Rights. Alternative definitions of privacy rights can also be found from legislation to a range of academic fields – philosophy, medicine, information system, management, or marketing – highlighting the trans-disciplinary character of the term.

In this work, we adopt terminology as construed in the nascent field of Privacy-Sensitive Robotics [12], where Rueben et al. [28] presented a taxonomy of privacy as an analytical tool for the Privacy-Sensitive Robotics field. According to this taxonomy, we mainly focus on the aspects of "Informational Privacy" covering concepts of Invasion, Collection, Processing, and Dissemination related to personal information – based initially on Soloves privacy hierarchy [29,30].

The more recent framework on privacy by Koops et al. [26] adds even more aspects to "Informational Privacy" which overlays eight types of privacy: bodily privacy, spatial privacy, communication privacy, proprietary privacy, intellectual privacy, decisional privacy, associational privacy, and behavioral privacy. While another dimension of Informational Privacy, according to Leenes and De Conca [31], is data protection. In this sense, data protection and privacy have different but also overlapping meanings. The latter work also highlights how data protection and privacy have different but overlapping meanings and how compliance with a data protection regime does not necessarily mean that privacy is a given.

2.2 Data governance in robotics

Privacy is generally considered a prevalent issue concerning most technology areas requiring any personal data exchange to operate. However, why robotics may be different from other technologies? What seems to be overlooked is that users build an emotional and social connection with personal and consumer robots, which is richer than other technological artifacts, e.g., other smart appliances or smart meters. It appears that there is an expectation to trust personal robots with the most sensitive information of our lives without actually understanding the policies that govern the control of this information [32]. In this sense, the impact of data governance policies has to be investigated and tailored especially for the field of personal robots, where both the legal and the social norms play a crucial role in creating public trust. In combination with the lack of investment and skills, this lack of trust holds back a broader uptake of AI [18] and, therefore, the adoption of robots in our lives.

In fields of activity beyond robotics, for example, smart energy, the current lack of laws and regulations around the collection of consumer data has been addressed extensively by legal scholars [33–36]. In smart energy, consumer privacy is an afterthought by most companies [33], and the pervasive lack of transparency of existing systems is a real threat [37]. Legal scholars are just picking up these issues and stress test the scope of current standards and regulations [38]. In addition, currently no comprehensive study focused on the privacy needs and the perceptions of the users. Companies and organizations implement the minimum requirements of state-imposed regulations without users being part of the decision-making process.

Some legal scholars [39–42] have recently made important contributions to the discussion around the legal tensions arising in privacy due to the presence of robots around us. Notably, most academic contributions were made in the US legal context. In the EU context, the Robolaw project [16,43,44], a Commission-funded academic project, investigated how the existing laws and

regulations dealt with robots and concluded in May 2014. On the legal front, the implementation of the General Data Protection Regulation (GDPR), the legal framework that governs personal data protection, came into force after the conclusion of this project in May 2018.

2.3 Personal data

In the European regime, part of the interaction records with smart technology potentially falls under the GDPR *personal data* definition: *any information related to an identified or identifiable natural person*. However, what does *any information* mean in the context of personal and consumer robots? How do we draw a line between what is personal or nonpersonal data? Information like images of human faces is undoubtedly classified as personal, but what about data related to the times of the day a user is active or needs a reminder for a specific medicine?

2.4 Nonpersonal data

Another recently introduced legislative concept is nonpersonal data. The EU Communication on Building a European Data Economy [45] and the new Regulation on the free flow of nonpersonal data [46] initiated its application in May 2019. Machine-generated, nonpersonal data in the context of Industry 4.0 and Internet of Things were defined as *data created without the direct intervention of a human by computer processes, applications, or services, or by sensors processing information received from equipment, software or machinery, whether virtual or real*. But what does *direct intervention of a human* mean in the context of an autonomous machine? For example, data collected by a robot vacuum cleaner may be classified by default as nonpersonal. However, inferences could still be drawn about the habits or other socioeconomic factors related to an individual user. Therefore, it is unclear whether or how this definition complements the personal data definition and where the line between personal and nonpersonal should or could be drawn, especially for robots designed to serve a user.

Legal scholars agree that AI and Big Data challenge the scope of data protection law, especially the extent to which the data subject can be identifiable [47–49]. In particular, Putrova [48] argues that everything is being increasingly datified, and any data can be plausibly argued to be personal, from the weather to water waste. In this sense, the capacity to turn data into personal data depends on processing power and data availability [38]. Anonymized data can be de-anonymized when combined or correlated with other data sets and enable inferences to be drawn about specific aspects of an individual's life. As a result, there is no guarantee that nonpersonal data would remain nonpersonal in the future.

From a practical point of view, the cost to distinguish personal from nonpersonal data is high. Consequently, companies increasingly treat nonpersonal data as personal data [50], a practice that seems to be working for this current period. It is yet questionable for how long companies can sustain this practice. A large amount of accumulated data appear to be purposely mislabeled as personal. Therefore, the new services and technologies that could otherwise utilize these nonpersonal data cannot be implemented due to the limitations applicable to personal data. As a result, this may have a negative impact on the implementation of such technologies or services, which greatly depend on large amounts of interconnected data for their success.

In the future, the broadening scope of the definition of what constitutes personal data could make the GDPR hard to maintain [48]. At the same time, some authors believe the law may fall behind new technological advantages [51], despite its current technologically neutral nature. While it is hard to foresee how the relationship between technology and regulation will evolve in the future, creating personal data from nonpersonal databases is a real risk [17].

The authors feel that the social context, conditions of operation, and user interaction modes with a device are crucial elements that need to be thoroughly considered before making a distinction between personal and nonpersonal data. Considering there is a need for future adaptations of the legal framework to be led by evidence-based approaches, this work looks in that direction. This article is, therefore, a first attempt to gain concrete evidence on the ways robotic companies approach similar issues through Privacy Policies and related publicly available documentation.

3 Is privacy important? The privacy — personalization paradox

Personal robots are highly personalized products adapted to fit user needs, behaviors, and preferences. For example,

in the context of therapy, robots can uniquely adapt their personality to create deep engagement with the individual while being both predictive and repetitive [52–54].

In essence, personalization is impossible without sharing personal data at some level. However, disclosing private data and information raises privacy concerns. On the one hand, there is a higher perceived quality of a personalized product or service and, on the other, the loss of privacy. This dilemma, known as the privacy-personalization paradox, is a special subcategory of what is widely referred to as the privacy paradox [55]. According to the privacy paradox, on the one hand, individuals perceive their privacy and personal data – in theory – as very important while responding to surveys (e.g., the Eurobarometer [56][1]). On the other hand, individuals demonstrate privacy-compromising behavior and easily trade privacy for short-term benefits in practice. The privacy-personalization paradox refers explicitly to this discrepancy when the willingness to give away personal information refers to benefits related to personalized goods or services [57–61].

4 Building trust in human–robot interactions

The cooperative nature of humans appears to originate from the unique motivation to form a shared mental model of mutual goals and intentions with other users [62,63]. To achieve a task, we need to (i) share a common goal (e.g., assemble a part), (ii) agree on the task distribution (who will do what), (iii) be capable of identifying which task the colleague will do next (e.g., they now plan to screw two parts together), and (iv) be able to anticipate where they will move next (so we can hand over a screwdriver). Without such mutual intention understanding, genuine collaboration cannot be achieved, e.g., we would collide with our colleague and we would place an object in a poor position for them to pick it up.

Lewis et al. [64] mention system intelligibility and transparency as one of the core factors affecting trust in automation. At the same time, Hancock et al. [65] demonstrated in his meta-analysis that one of the critical factors related to the robots' general performance in human–robot interaction scenarios included transparency of interaction and, consequently, establishing trust with the robot.

In cases where the user of a personal or a consumer robot is not aware of what kind of data is shared and for what specific purpose, the intentions of the interaction could be misleading. Therefore, the trust between the user and the robot suffers [66–69]. In human–robot interaction, the whole is greater than the sum of its parts. The social interaction adds an extra layer to the quality of the relationship between the human and the machine. It is crucial to understand how users built such trust and whether it is trust in the software, the robot itself, the manufacturer, the service provided, or the robot's brand. The recently established field of privacy-sensitive robotics started to investigate these matters in greater detail [11].

In our work, we look into the context of trust and transparency in human–robot interaction. More specifically, we examine the clarity level and communication of intentions regarding privacy formed as part of the Privacy Policy. It is a well-known idea that the vast majority of users rarely read digital contractual agreements, Terms and Conditions, or Privacy Policy documents [70]. In the past, it has also been observed that firms might take steps to make such documents less comprehensible [71] deliberately. Trust is certainly an issue when "take-it or leave-it" approach or boilerplate contractual agreements is the norm.

Here we concentrate on the role and impact of Privacy Policies in defining the transparency of the human–robot interaction in terms of the data collected or utilized by the robot. In this sense, we are interested in how they may affect the trust that the user builds with the robot through the ways the company has communicated them.

5 OECD privacy guidelines

The OECD is an intergovernmental economic organization founded to stimulate economic progress and world trade. To assist the development of a global privacy protection framework and support digital trade, in 2013, the OECD released the Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data [72] also known as the OECD Privacy Framework,[2] which was based on the original version initially released in 1980.

1 In the latest Eurobarometer study (e-Privacy 2016) "The privacy of their personal information, online communications and online behavior is very important to the majority of respondents" and "nine in ten respondents say it is important that personal information on their computer, smartphone or tablet can only be accessed with their permission."

2 https://www.oecd.org/sti/ieconomy/privacy-guidelines.htm [accessed on 10/4/2020].

This work utilizes the OECD principles as it is considered a globally accepted standard that formed the basis for privacy regulation in a number of jurisdictions [73]. Therefore, our analysis takes a universal perspective and is not tied to one jurisdiction. The EU approach to privacy (and the GDPR) may be considered one of the most comprehensive ones [31]. Nevertheless, global (regulatory) convergence around the GDPR standards for all jurisdictions is unlikely [74]. We adopt the OECD principles as a global standard for our analysis, rather than other domestic laws or standards, to create a more inclusive methodology independent of trading relationships with the European Economic Area. As a result, the analysis in this study is relevant not only in a European context but in a more global context. In the future, this work can be expanded to a discussion more tailored to the EU context by drawing closer attention to the overlap and differences between the OECD principles and the GDPR, as discussed by legal scholars [73,75].

The OECD privacy framework involves eight principles: (P1) the Collection Limitation Principle, (P2) the Data Quality Principle, (P3) the Purpose Specification Principle, (P4) the Use Limitation Principle, (P5) the Security Safeguards Principle, (P6) the Openness Principle, (P7) the Individual Participation Principle, and (P8) the Accountability Principle. According to the framework, the principles are defined as follows:

(*P1*) *Collection Limitation Principle*: There should be limits to the collection of personal data, and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

(*P2*) *Data Quality Principle*: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete, and kept up to date.

(*P3*) *Purpose Specification Principle*: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

(*P4*) *Use Limitation Principle:* Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified in accordance with (the Purpose Specification Principle) except: (a) with the consent of the data subject or (b) by the authority of law.

(*P5*) *Security Safeguards Principle:* Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data.

(*P6*) *Openness Principle:* There should be a general policy of openness about developments, practices, and policies concerning personal data. Means should be readily available for establishing the existence and nature of personal data and the primary purposes of their use, and the identity and usual residence of the data controller.

(*P7*) *Individual Participation Principle*: Individuals should have the right to (a) obtain from a data controller, or otherwise, confirmation of whether the data controller has data relating to them; (b) have communicated to them, data relating to them within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; (c) be given reasons if a request made under subparagraphs (a) and (b) is denied and be able to challenge such denial; and (d) challenge data relating to him and if the challenge is successful in having the data erased, rectified, completed, or amended.

(*P8*) *Accountability Principle*: A data controller should be accountable for complying with measures that give effect to the principles stated above.

In the present study, we directly utilized the above principles to assess the Privacy Policy documentation of personal and consumer robotic companies. The interpretation of these principles and the rating scheme is described in Section 6.

6 Methodology

Here we shed some light on how privacy terms are formed and utilize the OECD principles as a unifying framework and a tool to draw comparisons between approaches of different companies in the field of consumer robotics. The goal is to determine the part of the policy that captures the essence of each principle.

The methodology background rests on prior literature examining Privacy Policies based on objective or subjective standards in fields other than robotics. For example, Khalil et al. [76] review Massive Open Online Courses (MOOC) and explore how consent to collect and use data is described to potential users. Nokhbeh Zaeem and Barber [77] study Privacy Policies of 600 companies across industries to reveal trends in user data collection, while Das et al. [78] and O'Loughlin et al. [79] examine the Privacy Policies of mobile apps.

To assess the extent to which the OECD privacy principles are considered in a Privacy Policy of personal and consumer robotic products (see Table 1), each Privacy

Policy was reviewed four times by the researchers, and each review had a distinct scope;

Review 1 – Determine the supporting text guidelines for each principle: The first of the four reviews required every policy to be read and common themes of text to be recorded. Once the review was completed, these themes were then assigned to the most relevant principle.

Review 2 – Extraction of relevant text: Having identified the text that would support a principle, each policy was then reviewed a second time for all relevant text to be extracted and recorded against the relevant principle.

Review 3 – Scoring of the extracted text according to each OECD principle: The third review enabled a rating from 0 to 3 based on the degree to which the extracted text within the policy supported the specific principle. The decision to use a 0–3 scale allowed a scoring mechanism that can demonstrate the level of detail in each of the Privacy Policies while providing a simplified measure that focuses on the main points of each principle (see Table 2). Privacy Policies that did not cover a certain principle scored 0 for the specific principle; policies that refer to issues associated with a principle vaguely scored 1 for that principle; policies that support the principle in reasonable detail related to a principle scored 2; while policies that support a principle in a detailed and explicit manner scored 3 in that principle.

Review 4 – Comparative review of scores and text: This final review was to directly compare the text of policies with matching scores for a specific principle to identify and remove any anomalies and ensure consistent, noncontradicting scores across the results set.

One of the coauthors identified the Privacy Policies and the Terms and Conditions by searching for the most popular consumer robotic firms and their publicly available documentation in their proprietary web pages. All the policies and Terms and Conditions were then independently reviewed by two of the authors, and the scores assigned by each author were compared. There was a lack of substantial deviation in the rating, and it was easy to reach a consensus on the final ranking. The third author was also consulted in terms of the rating strategy to ensure the rating strategy's robustness.

Table 2: Rating scale and description of the principles of rating Privacy Policy extracts

Rating	Description
0	No text in support of this principle or in direct contrast
1	Text supporting this principle is limited in detail and vague in statement
2	Text supporting this principle has a reasonable amount of detail and specificity
3	Text supporting this principle is detailed and explicit

Our initial sampling strategy was to include the most popular consumer robotic firms in the field in this review. However, due to the small number of active companies in the field, we broadened the scope of research to include companies that offer products directly available to consumers. As a result, we reviewed the Privacy Policies of eight robotic companies in this study. The Privacy Policies were publicly available, and there was no requirement to purchase the product to access them. Initially, 15 consumer robotic companies were identified as potentially subject to the study (SoftBank, Ubtech, ANKI, Bluefrog, Dyson, Ecovacs, Intuition Robotics, Qihan Sanbot, iRobot, Reach Robotics, Wonder Workshop, Promobot, Aeleous, Avatarmind, and iLife). However, five of those companies did not have publicly available Privacy Policies (Bluefrog,

Table 1: OECD Privacy Principles and relevance to Privacy Policy statements of personal and consumer robotic products

OECD Privacy Principle	Related Privacy Policy extract
Collection Limitation Principle	Statements regarding limiting the collection of personal data. Statements explaining the process of consent
Data Quality Principle	Statements specifying the data types are to be collected. Statements regarding mechanisms to maintain accurate and complete data
Purpose Specification Principle	Statements specifying how the data collected will be used. Statements about retention periods
Use Limitation Principle	Statements regarding limiting the use of the data to the ones specified. Statements regarding sharing of data to third parties
Security Safeguards Principle	Statements regarding any security measures taken to safeguard data. Statements regarding safeguarding data if transferred across country borders
Openness Principle	Statements explaining how consumers are updated of changes to the Privacy Policy
Individual Participation Principle	Statements specifying the data subject's rights and how they can exercise them
Accountability Principle	Statements regarding efforts to comply with rules, regulations, and ethical guidelines

Table 3: Operational information of the consumer robotic companies that were the subject of the study

Company name	Size	Company's headquarter location
Dyson	Large	UK
ANKI	Medium	US
iRobot	Medium	US
UBtech	Medium	China
Ecovacs	Medium	China
Wonder Workshop	Small	US
Reach Robotics	Small	UK
SoftBank	Small	France, Japan

Qihan Sanbot, Aeleous, Avatarmind, and iLife) while two of them (Intuition Robotics and Promobot) had publicly available Privacy Policies that were only related to the use of their website, which was independent of the product or the service the robot provided.

At this point, it is worthwhile noting that some of the largest humanoid companies do not have publicly available Privacy Policies related to the service or the robotic device. The reason may be that consumers are not expected to order a humanoid without prior communication with the company. A humanoid may be considered a product for a more specialized audience, and, therefore, detailed privacy information is not publicly available.

Table 3 presents the companies selected for this study, along with the size and the country in which each company's headquarters are located. Some of those companies specialize in robots, while others, for example, Dyson, develop various products, including consumer robots. The size was estimated according to the turnover. The size of the company based on the turnover was categorized as follows – small (<10M USD), medium (<1B USD), and large (<10B USD). We provide a brief description of each company in Section 7. Due to copyright restrictions, we refrain from referring to extracts from each policy here.

7 A comparative analysis of Privacy Policies

7.1 Dyson – Dyson 360

Dyson, a company specializing in household appliances, has developed the Dyson 360, a robotic vacuum cleaner. The first robotic vacuum cleaner by Dyson, the Dyson 360 Eye, was launched in 2014. The company recently launched the Dyson 360 Heurist, which has a visual navigation system and can be controlled via a mobile application.

Dyson's Privacy Policy[3] covers all "connected products" and services provided by the company. This Privacy Policy had a relatively larger word count than the rest of the Privacy Policies reviewed, which may be justified due to the company's size and the broad range of products provided. Based on the four-step review process, and according to the OECD privacy principles followed in this work, this was the highest-ranked policy with an overall score of 14.

7.2 ANKI – Cozmo, Vector

Founded in 2010 by three graduates of Carnegie Mellon University, ANKI created small consumer robots such as Cozmo and Vector, defining the category of affordable, entertainment home robots that create emotional connections with the users. Digital Dream Labs later acquired the company to continue the development of the Vector robot.[4]

The company's Privacy Policy[5] is detailed and demonstrates how user data and privacy are treated when the user interacts with the robot. This was the second-highest-ranked policy with an overall score of 12. Compared, for example, to Dyson's Privacy Policy, this is clearly a policy specializing in the interaction with a robot.

7.3 Wonder Workshop

Wonder Workshop specializes in educational robotics to encourage age-appropriate learning and coding skills. Their range of robots is available to individual consumers; however, the company also supplies material to enable educational institutions to form part of a more formal curriculum.

3 https://privacy.dyson.com/globalprivacypolicy.aspx [accessed on 30/12/19].
4 https://tinyurl.com/ANKI-Cozmo [accessed on 30/12/2019].
5 https://anki.com/en-gb/company/privacy.html [accessed on 30/12/19].

The company's Privacy Policy[6] appears to have taken under special consideration issues related to children's privacy and data. In terms of the Accountability Principle, the policy refers specifically to privacy pledges and agreements regarding student data privacy and educational law.

7.4 iRobot Corporation – Roomba

It has been more than a decade since iRobot Corporation introduced its first robot vacuum in the market, the infamous Roomba. After that, it altered the landscape of the consumer robots and autonomous cleaning devices. The latest products from iRobot are using a machine-generated map of the floor plan that the robot is working on, raising multiple personal data security questions to their users' homes [80].

The company's policies[7] refer to the ways personal data are utilized for further processing. There is an explicit statement on handling personal information for user registration purposes and potentially other information if the user chooses to register using an account related to social media. It is worthwhile noting that, like most companies, these terms and conditions are considered as a "blanket" covering the web page, the actual robot, and the mobile application for all the product ranges.

The policy comprises an adequate justification of the Security Safeguards Principle detailing handling, transit, and data storage. There may, however, be a gray area related to the handling of the generated data when the user may choose to opt in and enable "smart-home" features such as connection with Amazon's Alexa and use the generated floor plan as input for controlling the robot.

7.5 Reach Robotics – MekaMon

Reach Robotics released the MekaMon robot in 2017. MekaMon, a spider-legged robot, is used in a robotic battle game that includes Augmented Reality and forms an educational tool. The company recently went into administration. However, according to a public declaration, they are still active in the educational field.

The company's Privacy Policy is part of the Terms and Conditions[8] and includes the services provided by the company. Interestingly no issues regarding the collection or storage of data generated through the device are discussed in the policy.

7.6 UBtech – AlphaMini

UBtech provides a range of robots, from large-scale humanoid and service robots to smaller companion or educational toy robots. The company's large service robots can be used in many sectors, providing guidance and facilitating users in many tasks. UBtech also has an educational branch, including robots and tool kits aimed at tech children coding through the interaction with a robot.

It appears that UBtech has separate Privacy Policies for each robot. We could track down only the AlphaMini product Privacy Policy.[9] The AlphaMini is a personal robot companion that is managed through a mobile application.

7.7 SoftBank Robotics – Pepper, Nao

SoftBank Robotics humanoids Pepper and Nao are famous worldwide for their capabilities as social assistants in education, health-care centers, and public spaces to welcome, entertain, and facilitate users and visitors.

SoftBank Robotics Privacy Policy[10] covers the use of the services provided by the company, including services and data related to the robots.

The policy refers to the practice of collecting dialog data to surpass the limitations of the software related to voice recognition. The sharing of spoken words, which can potentially include personal or other sensitive information with third parties, may result in personal information being transmitted to third-party providers potentially located outside the European Economic Area.

6 https://www.makewonder.com/privacy/ [accessed on 31/12/2019].
7 https://tinyurl.com/irobot-policy, https://www.irobot.com/legal/data-security, https://tinyurl.com/irobot-data-sharing [accessed on 17/04/2019].
8 https://reachrobotics.com/terms-conditions [accessed on 31/12/2019].
9 https://tinyurl.com/alphamini [accessed on 31/12/2019].
10 https://www.softbankrobotics.com/emea/en/privacy-policy [accessed on 26/12/2019].

7.8 Ecovacs – Deebot, Winbon

Ecovacs is one of the longest active companies in the field of robotic appliances and was founded in 1998. They currently develop robotic floor cleaners and robotic window cleaners, while the devices also connect with a mobile application to enable the user to control the robot. According to the company's website, some of their latest models feature an AI chipset and camera module that enable greater precision in the navigation of the robot; while Ecovacs' Privacy Policy[11] is a blanket policy covering all the product ranges.

8 Analysis of Privacy Policies according to the OECD privacy principles

Following the four-stage review process, each Privacy Policy was rated according to each OECD principle (see Table 4). This section provides an analysis of each principle and the practical recommendations that would bridge the gaps revealed in the way such Terms and Conditions are communicated.

Table 4: Scoring of privacy policies used in our study according to OECD privacy principles

Company name	Word count	P1	P2	P3	P4	P5	P6	P7	P8	Total score
Dyson	6,658	1	1	2	2	2	2	2	2	14
ANKI	3,252	0	2	2	1	1	1	2	2	11
Wonder Workshop	5,757	0	2	2	1	1	1	1	3	11
iRobot	3,252	0	2	2	1	3	1	1	0	10
Reach Robotics	2,918	0	1	2	1	1	1	2	1	9
UBtech	2,682	1	1	1	0	1	1	2	0	7
SoftBank	1,982	0	1	1	1	1	1	2	0	7
Ecovacs	3,750	0	1	1	1	1	1	1	0	6

Higher score corresponds to better compliance with the OECD privacy policies. P1 represents the Collection Limitation Principle, P2 the Data Quality Principle, P3 the Purpose Specification Principle, P4 the Use Limitation Principle, P5 the Security Safeguards Principle, P6 the Openness Principle, P7 the Individual Participation Principle and P8 the Accountability Principle.

8.1 P1: Collection Limitation Principle

Most Privacy Policies scored low in the Collection Limitation Principle. The reasoning behind this is the lack of explanation of the processes to grant the consent of data collection in an explicit and controllable manner. Most policies in the field of robotics seem to have a "take-it or leave-it" approach. There is no option to give consent "as you go," accepting or rejecting the options that fit each user and limiting data collection.In other sectors, for example, in an activity tracker Privacy Policy,[12] consent to process data is requested separately when the user takes action and as they interact with different services or features of the device. As a result, the user gains much more granular control of their data and allows them to control the company's access to their data. Consumer robotics companies can potentially borrow similar approaches to increase control users have over their data and limit the data collected through their services and products.

8.2 P2: Data Quality Principle

In terms of the Data Quality Principle, all Privacy Policies provide statements regarding the data collected. However, some Privacy Policies are much more explicit, listing the specific types of data collected and the data not collected. This is, for example, clearly demonstrated by comparing the policies between Wonder Workshop and UBtech. The first provides an exact list of the types of data collected. Simultaneously, the second gives some examples, including noncommittal terminology (i.e., etc.), which introduces ambiguity over what they may collect. A clearly defined list of the type data collected can give users more certainty regarding what is recorded and who may store it when it comes to their data. Therefore, consumer robotic companies may consider making explicit mention of what exactly is and what is not collected through their services and devices.

8.3 P3: Purpose Specification Principle

All Privacy Policies reviewed comprise statements related to the Purpose Specification Principle. Some policies,

11 https://www.ecovacs.com/us/privacy-policy [accessed on 30/12/2019].
12 https://www.fitbit.com/us/legal/privacy-policy [accessed on 10/4/2020].

however, comprise more assertive statements than others. For example, some policies note the storage location and encryption of photos taken by the robots. Other policies scoring lower make more generic statements, including phrases that introduce ambiguity. For example, declarations that all collected data may be used in other services in accordance with the legal obligations. Other ambiguous statements relate to the period that data will be held, i.e., data retained "for as long as is necessary."

According to the Purpose Specification Principle, Privacy Policies need to have explicit statements defining how the company will use the collected data and the period the data will be held. Determining how all the collected data will be used can be challenging for a company, mainly because they may not be able to foresee how they might use the data in the future. This may lead to ambiguous statements about the purpose of data and their retainment period. To avoid ambiguity, the policy needs to commit to specific practices and time frames to define and publicly disclose data management plans.

8.4 P4: Use Limitation Principle

The Use Limitation principle directs limiting data collected and used by the company or provided to the third parties. Most policies reviewed here comprise some provisions on this principle to an extent. However, the highest-scoring policy provides additional details regarding the circumstances in which they may share the data with the third parties. Nevertheless, no Privacy Policy provides specific details regarding the third parties with whom they share data.

To improve Privacy Policies in terms of this principle, additional pieces of information need to be provided. First, disclosing the purpose behind data sharing with the third parties, second the jurisdiction of those third parties, and finally revealing those third parties.

8.5 P5: Security Safeguards Principle

All Privacy Policies reviewed mention security measures taken to safeguard data, such as data encryption or measures taken to transfer data across country borders and jurisdictions. The policy achieving the highest score explicitly mentions the type of encryption protocols and details the circumstances under which they are used. Other policies scoring lower make very generic statements regarding abstract security measures.

An explicit mention of the specific security measures taken when transferring or storing data, rather than abstract mentions on security, can enhance a Privacy Policy in line with the Security Safeguards principle. This can also give insights to the users regarding the tools the company might be using and whether they use the most modern security protocols.

8.6 P6: Openness Principle

All Privacy Policies reviewed make statements regarding updating the policies and updating the consumers of these changes. In this case, the highest score was attributed to a policy that makes a specific reference of the timeline of the updating process and the specific ways these updates will be communicated to consumers. Therefore, a Privacy Policy can be enhanced in term of the Openness Principle by disclosing how often the policy will be revised to incorporate new developments and practices, as well as how consumers will be informed of these revisions.

8.7 P7: Individual Participation Principle

Data subjects' rights and the ways consumers can exercise them were part of all Privacy Policies reviewed. The main difference between scores rests in the fact that some policies make explicit mention of the consumers' data rights independent of the jurisdiction. Other policies are more subtle and even leave it to the consumer to judge whether some provisions violate the agreement. For example, consumers can contact the company in case of a violation, and the company can delete the personal data. Providing a clear definition of the specific rights a consumer has in terms of the data collected clarifies and can significantly enhance a Privacy Policy.

8.8 P8: Accountability principle

References and statements on the ways a policy comply with specific rules, regulations, and ethical guidelines are dictated by the Accountability principle. In this case, only half of the policies reviewed comprised such references. The highest score was granted to a policy with an in-

creased level of detail in referencing relevant regulations and guidelines related to specific user groups (i.e., children).

Providing details in terms of the rules, regulations, and ethical guidelines that were taken into consideration when the policy was formed or updated has a positive impact on the policy. This also demonstrates that the company is up to date with current discourses on privacy and may, therefore, be in a better position to provide the state-of-the-art service to users.

9 Concluding remarks

Privacy, transparency, and trust are fundamental concepts that the human–robot interaction community recently started exploring. To the best of the authors' knowledge, this is one of the earliest works in the field, which adds a practical dimension to the gray areas of user privacy rights. This work provides some interesting insights into the structure and context of privacy terms and conditions of personal and consumer robots. This analysis of privacy terms and conditions revealed gaps in the ways such conditions are communicated to the users.

Despite the limitations in our analysis in terms of the extensiveness of this study, the trend appears to be that consumer robotic companies do not uniformly consider privacy. It would be important to understand the extent to which this is a design choice in the robot architecture, an actual functional requirement for the robot's operation, or a legal requirement depending on the jurisdiction the company operates. In this study, for example, the jurisdiction did not appear to play a significant role.

The size of the policy and word count also do not seem to play significant roles in the specific ranking. A lengthy policy does not necessarily mean that all principles are covered to a greater extent. Nevertheless, a broad trend is evident, as the average word count for the top performers was higher than the average word count of the bottom performers. This means that a large word count does not necessarily mean that all principles will be better covered, but it may hint at the level of detail comprising each policy.

A way forward to improve a Privacy Policy would be to clearly define the information that a robot can process locally and the information necessary to be sent back to the company (e.g., troubleshooting to improve specific features and data for training an algorithm).

In the policy agenda, the absence of technical tools and standards to simplify and empower users to exercise their rights has been noted [81]. Some interesting points have been suggested on consent, reducing complexity and tailoring privacy notices by one of the leading European bodies on data privacy, the Article 29 Working Party (also known as WP29[13]) which acted as an advisory body comprising representatives from the European Commission, each EU Member State data protection authority and the European Data Protection Supervisor. Rather than displaying all information in a single notice or document, the WP29 suggested that privacy documents can present information in a layered manner, so users can access only information relevant to them each time [82]. This includes a "just-in-time" approach where privacy notices are "pushed" before a user makes a specific decision to share data or additional information is "pulled" upon the user's request [83]. Another interesting idea mentioned in the opinion 3/2020 on the European strategy for data would be to provide information through standardized and machine-readable icons [83], which could facilitate not only users but also algorithms to interpret the main points of a privacy notice quickly.

Another concept to explore is whether a firm's business scope is a predictor of its level of privacy. For example, a service-orientated firm might justify collecting personal data differently than a product-orientated firm providing hardware. Similarly, it is important to clearly define user rights separate from consumer rights, especially when the consumer and the user are different. In general, many open questions need to be answered from a business perspective, and more in-depth research is required into the inner workings of a company to understand how organizations take privacy decisions and how they choose to communicate them.

This study was the first step to develop a rating scheme based on the preexisting privacy principles. One of the main limitations may lay on the qualitative and subjective nature of rating by the researchers. Future research will focus on creating a more robust methodology and rating scheme.

To drive more transparency and flexibility in the human–robot interaction, this work needs to expand on the user-friendliness and customizable aspects of digital agreements. It is also important to open such a discussion and incorporate a user-centered research approach to develop novel ways that privacy and user rights accommodate user needs. The final goal is to create more transparency in data governance during user interactions and

13 WP29 has recently been replaced by the European Data Protection Board (EDPB) under GDPR.

accommodate a stronger perception of trust and a symbiotic relationship with robots.

Acknowledgments: The work reported in this paper is supported by a South West Creative Technology Network Fellowship in Automation and partially supported by EPSRC Grant EP/R033838/1.

References

[1] E. Estolatan, A. Geuna, M. Guerzoni, and M. Nuccio, *Mapping the evolution of the robotics industry: A cross country comparison*, Department of Economics and Statistics Cognetti de Martiis, University of Turin, Jul 2018. https://ideas.repec.org/p/uto/dipeco/201812.html.

[2] G.-Z. Yang, B. J. Nelson, R. R. Murphy, H. Choset, H. Christensen, S. H. Collins, et al., "Combating COVID-19' the role of robotics in managing public health and infectious diseases," *Sci. Robot.* vol. 5, no. 40, art. eabb5589, 2020. DOI: 10.1126/scirobotics.abb5589.

[3] M. M. de Graaf, S. B. Allouch and J. A. van Dijk, "Long-term acceptance of social robots in domestic environments: insights from a user's perspective," in *2016 AAAI Spring Symposium Series*, 2016.

[4] M. M. de Graaf, S. Ben Allouch and J. A. van Dijk, "Why would I use this in my home? A model of domestic social robot acceptance," *Hum.-Comput. Interact.*, vol. 34, no. 2, pp. 115–173, 2019. DOI: 10.1080/07370024.2017.1312406.

[5] J. Sung, R. E. Grinter and H. I. Christensen, "Domestic robot ecology," *Int. J. Soc. Robot.*, vol. 2, pp. 417–429, 2010. DOI: 10.1007/s12369-010-0065-8.

[6] U. Pagallo, "The impact of domestic robots on privacy and data protection, and the troubles with legal regulation by design," in S. Gutwirth, R. Leenes, and P. De Hert, Eds., *Data Protection on the Move, Law, Governance and Technology Series*, vol. 24, Springer, Dordrecht, 2016, pp. 387–410. DOI: 10.1007/978-94-017-7376-8_14.

[7] A. F. Winfield and M. Jirotka, "Ethical governance is essential to building trust in robotics and artificial intelligence systems," *Philos. Trans. R. Soc. A*, vol. 376, no. 2133, pp. 1–13, 2018. DOI: 10.1098/rsta.2018.0085.

[8] L. Floridi, "Translating principles into practices of digital ethics: Five risks of being unethical," *Philosophy Technol.*, vol. 32, pp. 185–193, 2019. DOI: 10.1007/s13347-019-00354-x.

[9] European Commission, *Ethics Guidelines for Trustworthy AI* [accessed on March 9, 2019].

[10] A. Chatzimichali and D. Chrysostomou, "Human-data interaction and user rights at the personal robot era," in: M. O. Tokhi, M. I. A. Ferreira, N. S. Govindarajulu, M. Silva, G. S. Virk, E. Kadar, and S. R. Fletcher, Eds., *Artificial Intelligence, Robots and Ethics – Proceedings of the Fourth Int. Conf. on Robot Ethics and Standards* (*ICRES 2019*), CLAWAR Association Ltd, 2019.

[11] M. Rueben, A. M. Aroyo, C. Lutz, J. Schmolz, P. Van Cleynenbreugel, A. Corti, et al., "Themes and research directions in privacy-sensitive robotics," in *2018 IEEE Workshop on Advanced Robotics and its Social Impacts* (*ARSO*), Genova, Italy, 2018. DOI: 10.1109/ARSO.2018.8625758.

[12] M. Rueben and W. D. Smart, "Privacy in human-robot interaction: survey and future work," in *We Robot 2016: the Fifth Annual Conf. on Legal and Policy Issues relating to Robotics*, University of Miami School of Law, 2016, Discussant: Ashkan Soltani, Independent Researcher [cited with permission from the main author], 2016.

[13] N. Nevejans, *European Civil Law Rules in Robotics* [accessed on February 8, 2019].

[14] B.-J. Koops, "Should ICT regulation be technology-neutral? *Starting points for ICT ergulation*," in *Deconstructing Prevalent Policy One-Liners, IT & Law Series*, B.-J. Koops, M. Lips, C. Prince and M. Schellekens, Eds., Vol. 9, pp. 77–108, The Hague: T.M.C. Asser Press, 2006.

[15] W. R. Wiewiorowski, *Opinion 4/2020 – EDPS opinion on the european commission's white paper on artificial intelligence – a European approach to excellence and trust* [accessed on August 10, 2020].

[16] E. F. Project, *RoboLaw – Regulating Emerging Robotic Technologies in Europe: Robotics facing Law and Ethics* [accessed on August 23, 2020].

[17] European Commission, *White paper on artificial intelligence – A European approach to excellence and trust* [accessed on August 22, 2020].

[18] European Parliament, Committee on Legal Affairs, *Draft report with recommendations to the commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies* [accessed on August 22, 2020].

[19] European Parliament, *Civil Law Rules on Robotics, European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics* [accessed on August 22, 2020].

[20] European Commission, *Liability for Artificial Intelligence and other emerging digital technologies* [accessed on August 22, 2020].

[21] P. B. Newell, "Perspectives on privacy," *J. Environ. Psychol.*, vol. 15, no. 2, pp. 87–104, 1995. DOI: 10.1016/0272-4944(95)90018-7.

[22] J. Balkin, "The Hohfeldian approach to law and semiotics," *Univ. Miami. Law Rev.*, vol. 44, pp. 1119–1142, 1990.

[23] L. Wenar, "The nature of rights," *Philosophy Public Aff.*, vol. 33, no. 3, pp. 223–252, 2004. DOI: 10.1111/j.1088-4963.2005.00032.x.

[24] W. A. Edmundson, *An Introduction to Rights*, Cambridge University Press, Cambridge, 2012. DOI: 10.1017/CBO9780511820670.

[25] M. Richardson, *The Right to Privacy: Origins and Influence of a Nineteenth-century Idea*, Cambridge University Press, 2017. DOI: 10.1017/9781108303972.

[26] B.-J. Koops, B. C. Newell, T. Timan, I. Škorvánek, T. Chokrevski, and M. Gali, "A typology of privacy," *Univ. Pa. J. Int. Law*, vol. 38, no. 2, pp. 483–575, 2017.

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

[28] M. Rueben, C. M. Grimm, F. J. Bernieri, and W. D. Smart, "A taxonomy of privacy constructs for privacy-sensitive robotics," *arXiv preprint arXiv*:1701.00841 2017.

[29] D. J. Solove, "I've got nothing to hide and other misunderstandings of privacy," *San Diego Law Review*, vol. 44, p. 745, 2007, GWU Law School Public Law Research Paper No. 289, Available at SSRN: https://ssrn.com/abstract=998565.
[30] D. J. Solove, *Understanding Privacy*, Harvard University Press, May 2008, GWU Legal Studies Research Paper No. 420, GWU Law School Public Law Research Paper No. 420, Available at SSRN: https://ssrn.com/abstract=1127888.
[31] R. Leenes and S. De Conca, "Artificial intelligence and privacy – AI enters the house through the cloud," in W. Barfield, U. Pagallo, Eds., *Research Handbook on the Law of Artificial Intelligence*, Edward Elgar Publishing, Cheltenham, pp. 280–306, 2018.
[32] A. M. Aroyo, F. Rea, G. Sandini, and A. Sciutti, "Trust and social engineering in human robot interaction: Will a robot make you disclose sensitive information, conform to its recommendations or gamble?" *IEEE Robot. Autom. Lett.*, vol. 3, no. 4, pp. 3701–3708, 2018. DOI: 10.1109/LRA.2018.2856272.
[33] M. Mylrea, "Smart energy-internet-of-things opportunities require smart treatment of legal, privacy and cybersecurity challenges," *J. World Energy Law Bus.*, vol. 10, no. 2, pp. 147–158, 2017. DOI: 10.1093/jwelb/jwx001.
[34] G. Bellantuono, "Comparing smart grid policies in the USA and EU," *Law, Innov. Technol.*, vol. 6, no. 2, pp. 221–264, 2014. DOI: 10.5235/17579961.6.2.221.
[35] N. Friedrichsen, "Governing smart grids: the case for an independent system operator," *Eur. J. Law Econ.*, vol. 39, pp. 553–572, 2015. DOI: 10.1007/s10657-012-9345-0.
[36] L. Urquhart and D. McAuley, "Avoiding the internet of insecure industrial things," *Comput. Law Secur. Rev.*, vol. 34, no. 3, pp. 450–466, 2018. DOI: 10.1016/j.clsr.2017.12.004.
[37] M. Hildebrandt and B.-J. Koops, "The challenges of ambient law and legal protection in the profiling era," *Mod. Law Rev.*, vol. 73, no. 3, pp. 428–460, 2010. DOI: 10.1111/j.1468-2230.2010.00806.x.
[38] A. Mattoo and J. P. Meltzer, "International data flows and privacy: The conflict and its resolution," *J. Int. Econ. Law*, vol. 21, no. 4, 2018, pp. 769–789. DOI: 10.1093/jiel/jgy044.
[39] M. E. Kaminski, "Robots in the home: What will we have agreed to," *Idaho L. Rev.*, vol. 51, pp. 661–677, 2015. DOI: 10.2139/ssrn.2592500.
[40] R. Y. Wong and D. K. Mulligan, "These aren't the autonomous drones you're looking for: investigating privacy concerns through concept videos," *J. Hum. Robot Interact.*, vol. 5, no. 3, 2016. DOI: 10.5898/JHRI.5.3.Wong.
[41] J. M. Balkin, "Free speech in the algorithmic society: big data, private governance, and new school speech regulation," *UC Davis Law Review, Yale Law School, Public Law Research*, art. 615, vol. 51, p. 1149, 2017. DOI: 10.2139/ssrn.3038939.
[42] K. Ishii, "Comparative legal study on privacy and personal data protection for robots equipped with artificial intelligence: looking at functional and technological aspects," *AI Soc.*, vol. 34, pp. 509–533, 2019. DOI: 10.1007/s00146-017-0758-8.
[43] C. Holder, V. Khurana, F. Harrison, and L. Jacobs, "Robotics and law: Key legal and regulatory implications of the robotics age (part I of II)," *Comput. Law Secur. Rev.*, vol. 32, no. 3, pp. 383–402, 2016. DOI: 10.1016/j.clsr.2016.03.001.
[44] C. Holder, V. Khurana, J. Hook, G. Bacon, and R. Day, "Robotics and law: Key legal and regulatory implications of the robotics age (part II of II)," *Comput. Law Secur. Rev.*, vol. 32, no. 4, pp. 557–576, 2016. DOI: 10.1016/j.clsr.2016.05.011.
[45] T. E. Commission, *Digital single market strategy – building a European data economy* [accessed on February 8, 2019], https://tinyurl.com/european-data-economy.
[46] T. E. Parliament and the Council of the European Union, *Regulation on the free flow of non-personal data* [accessed on February 8, 2019], https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1546942605408uri=CELEX:32018R1807.
[47] P. Nemitz, "Constitutional democracy and technology in the age of artificial intelligence," *Philos. Trans. R. Soc. B*, vol. 376, art. 2133, pp. 1–14. 2018. DOI: 10.1098/RSTA.2018.0089.
[48] N. Purtova, "The law of everything. Broad concept of personal data and future of EU data protection law," *Law, Innov. Technol.*, vol. 10, no. 2, pp. 40–81, 2018. DOI: 10.1080/17579961.2018.1452176.
[49] L. Mitrou, *Data protection, artificial intelligence and cognitive services in the general data protection regulation (GDPR) artificial intelligence-proof?* Tech. Rep., Commissioned by Microsoft, 2019.
[50] H. Richter and P. R. Slowinski, "The data sharing economy: On the emergence of new intermediaries," *Int. Rev. Intellect. Prop. Compet. Law*, vol. 50, pp. 4–29, 2019. DOI: 10.1007/s40319-018-00777-7.
[51] T. Li, E. F. Villaronga and P. Kieseberg, "Humans forget, machines remember: Artificial intelligence and the right to be forgotten," (LawArXiv, 2017). DOI: 10.31228/osf.io/zs8kb.
[52] A. Tapus and M. J. Mataric, "Socially assistive robots: The link between personality, empathy, physiological signals, and task performance," in *AAAI Spring Symposium: Emotion, Personality, and Social Behavior*, 2008.
[53] A. Barco, J. Albo-Canals, C. Garriga-Berga, X. Vilass-Cardona, L. Callejón, M. Turón, et al., "A drop-out rate in a long-term cognitive rehabilitation program through robotics aimed at children with TBI," in *The 23rd International Symposium on Robot and Human Interactive Communication*, 2014. DOI: 10.1109/ROMAN.2014.6926251.
[54] E. F. Villaronga and J. Albo-Canals, "Implications of the Google's US 8,996,429 B1 patent in cloud robotics-based therapeutic researches," in A.J.R. Neves, Ed., *Service Robots*, IntechOpen, United Kingdom, pp. 145–163, 2017. DOI: 10.5772/intechopen.70279.
[55] S. Barth and M. D. De Jong, "The privacy paradox – investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review," *Telemat. Inform.*, vol. 34, no. 7, pp. 1038–1058, 2017. DOI: 10.1016/j.tele.2017.04.013.
[56] T. Political and Social, Flash Eurobarometer 443. Report: e-Privacy [accessed on August 25, 2020].
[57] A. Acquisti and J. Grossklags, "Privacy and rationality in individual decision making," *IEEE Security Privacy*, vol. 3, no. 1, pp. 26–33, 2005. DOI: 10.1109/msp.2005.22.
[58] K. D. Martin and P. E. Murphy, "The role of data privacy in marketing," *J. Acad. Mark. Sci.*, vol. 45, pp. 135–155, 2017. DOI: 10.1007/s11747-016-0495-4.
[59] H. Xu, X. R. Luo, J. M. Carroll, and M. B. Rosson, "The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing," *Decis. Support Syst.*, vol. 51, no. 1, pp. 42–52, 2011. DOI: 10.1016/j.dss.2010.11.017.

[60] S. Kokolakis, "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon," *Comput. Secur.*, vol. 64, no. C, pp. 122–134, 2017. DOI: 10.1016/j.cose.2015.07.002.

[61] C. Lutz and A. Tamò-Larrieux, "The robot privacy paradox: Understanding how privacy concerns shape intentions to use social robots," *Hum.-Mach. Commun.*, vol. 1, pp. 87–111. 2020. DOI: 10.30658/hmc.1.6.

[62] K. Sycara and M. Lewis, "Forming shared mental models," in *Proc. of the 13th Annual Meeting of the Cognitive Science Society*, 1991.

[63] P. F. Dominey and F. Warneken, "The basis of shared intentions in human and robot cognition," *New Ideas Psychol.*, vol. 29, no. 3, pp. 260–274, 2011. DOI: 10.1016/j.newideapsych.2009.07.006.

[64] M. Lewis, K. Sycara and P. Walker, "The Role of Trust in Human-Robot Interaction," in *Foundations of Trusted Autonomy*, H. A. Abbass, J. Scholz and D. J. Reid, Eds., Springer International Publishing, Cham, 2018, pp. 135–159. DOI: 10.1007/978-3-319-64816-3_8.

[65] P. A. Hancock, D. R. Billings, K. E. Schaefer, J. Y. Chen, E. J. De Visser, and R. Parasuraman, "A meta-analysis of factors affecting trust in human-robot interaction," *Hum. Factors*, vol. 53, no. 5, pp. 517–527, 2011. DOI: 10.1177/0018720811417254.

[66] P. A. Hancock, D. R. Billings and K. E. Schaefer, "Can you trust your robot?" *Ergonomics Des.*, vol. 19, pp. 24–29, 2011. DOI: 10.1177/1064804611415045.

[67] S. Vinanzi, M. Patacchiola, A. Chella, and A. Cangelosi, "Would a robot trust you? Developmental robotics model of trust and theory of mind," *Philos. Trans. R. Soc. B*, vol. 374, no. 1771, art. 20180032, 2019. DOI: 10.1098/rstb.2018.0032.

[68] H. Felzmann, E. Fosch-Villaronga, C. Lutz, and A. Tamo-Larrieux, "Robots and transparency: The multiple dimensions of transparency in the context of robot technologies," *IEEE Robot. Autom. Mag.*, vol. 26, no. 2, pp. 71–78, 2019. DOI: 10.1109/MRA.2019.2904644.

[69] H. Felzmann, E. F. Villaronga, C. Lutz, and A. Tamò-Larrieux, "Transparency you can trust: Transparency requirements for artificial intelligence between legal norms and contextual concerns," *Big Data Soc.*, vol. 6, no. 1, 2019. DOI: 10.1177/2053951719860542.

[70] M. J. Radin, "The deformation of contract in the information society," *Oxf. J. Leg. Stud.*, vol. 37, no. 3, pp. 505–533, 2017. DOI: 10.1093/ojls/gqx001.

[71] R. Van Loo, "Helping buyers beware: The need for supervision of big retail," *Univ. Pa. Law Rev.*, vol. 163, pp. 1311–1392, 2014.

[72] OECD, *OECD guidelines on the protection of privacy and transborder flows of personal data* [accessed on August 25, 2020].

[73] G. Greenleaf, "It's nearly 2020, so what fate awaits the 1980 OECD privacy guidelines? (A background paper for the 2019 OECD privacy guidelines review)," *A Background Paper for the* 2019.

[74] C. Kuner, "Reality and illusion in eu data transfer regulation post schrems," *Ger. Law J.*, vol. 18, no. 4, pp. 881–918, 2017. DOI: 10.1017/S2071832200022197.

[75] A. Mattoo and J. P. Meltzer, "International data flows and privacy: The conflict and its resolution," *Int. Econ. Law*, vol. 21, no. 4, pp. 769–789, 2018. DOI: 10.1093/jiel/jgy044.

[76] M. Khalil, P. Prinsloo and S. Slade, "User consent in MOOCs – micro, meso, and macro perspectives," *Int. Rev. Res. Open Distrib. Learn.*, vol. 19, pp. 61–79, 2018. DOI: 10.19173/irrodl.v19i5.3908.

[77] R. Nokhbeh Zaeem and K. S. Barber, "A study of web privacy policies across industries," *J. Inf. Priv. Secur.*, vol. 13, no. 4, pp. 169–185, 2017. DOI: 10.1080/15536548.2017.1394064.

[78] G. Das, C. Cheung, C. Nebeker, M. Bietz, and C. Bloss, "Privacy policies for apps targeted toward youth: descriptive analysis of readability," *JMIR mHealth uHealth*, vol. 6, no. 1, art. e3, 2018. DOI: 10.2196/mhealth.7626.

[79] K. O'Loughlin, M. Neary, E. C. Adkins, and S. M. Schueller, "Reviewing the data security and privacy policies of mobile apps for depression," *Internet Interv.*, vol. 15, pp. 110–115, 2019. DOI: 10.1016/j.invent.2018.12.001.

[80] The New York Times, *Your roomba may be mapping your home, collecting data that could be shared* [accessed on June 1, 2019], https://www.nytimes.com/2017/07/25/technology/roomba-irobot-data-privacy.html.

[81] European Commission, *Communication from the commission to the European parliament, the council, the European economic and social committee of the regions a European strategy for data* [accessed on August 13, 2020].

[82] European Commission, *Guidelines on transparency under regulation 2016/679* [accessed on August 22, 2020].

[83] W. R. Wiewiorowski, *Opinion 3/2020 on the European strategy for data* [accessed on August 21, 2020].