Human-data interaction and user rights at the personal robot era

Chatzimichali, Anna; Chrysostomou, Dimitrios

Published in:
4th International Conference on Robot Ethics and Standards

DOI (link to publication from Publisher):
10.13180/icres.2019.29-30.07.014

Publication date:
2019

Document Version
Publisher's PDF, also known as Version of record

ICRES 2019: International Conference on Robot
Ethics and Standards, London, UK, 29-30 July 2019.
https://doi.org/10.13180/icres.2019.29-30.07.id#

HUMAN-DATA INTERACTION AND USER RIGHTS AT THE PERSONAL ROBOT ERA

ANNA CHATZIMICHALI*

Department of Architecture and the Built Environment, University of West of England
Frenchay Campus, Coldharbour Ln, Stoke Gifford, BS16 1QY, Bristol, UK
**E-mail: Anna.Chatzimichali@uwe.ac.uk*

DIMITRIOS CHRYSOSTOMOU

Group of Robotics and Automation, Department of Materials and Production
Aalborg University, Fibigerstraede 16, DK 9220, Aalborg East, Denmark
E-mail: dimi@mp.aau.dk

In this paper, we explore issues related to privacy, data protection, and Intellectual Property rights around personal and collaborative robots. This is a discussion on personal and non-personal data in the context of robot privacy, specifically focused in the EU jurisdiction. This work is, however, not limited to such theoretic and legal constructs as it adds a new practical dimension in this discussion. The paper presents some initial findings of a comparative study of the publicly available privacy policies and data governance schemes for some of the widest used robots. The strategies of robotic companies are analysed based on three factors: access of the company to personal data collected by the robot, sharing personal data with third parties and users' rights regarding derivative work. This analysis makes an interesting observation; robots that can support more sophisticated levels of user interaction seem to offer the most limited privacy and user rights terms. The scope of this work is to present both the legal and the practical dimensions to the debate of handling user data and make a valuable contribution to the field of privacy-sensitive robotics.

Keywords: user privacy; user rights; Intellectual Property rights; personal data; privacy-sensitive robotics; human-robot interaction; human-data interaction

1. Introduction

Robots are as good as the data we feed them. Detailed records of user interactions may, therefore, be crucial to uncover user needs, preferences and expectations and develop systems that add value to the user. But how could those records be exploited in a way that respects the privacy of the user? Privacy and data governance were prioritized as a requirement in the recent Ethics Guidelines for trustworthy AI[1] by the EU Commission. It is, however, time for the debate to move from what those ethical principles dictate to how they get implemented.[2]

This work presents issues related to the current legal standing on data governance and explores for the first time how the definition of personal and non-personal data may impact personal robots under the EU jurisdiction. We compare the privacy policies and the terms and conditions of four of the biggest firms operating in the fields of social, personal and collaborative robots to shed light on how personal data, user records and Intellectual Property (IP) rights are approached in practice. Our goal is to make a contribution to the academic discourse in the nascent field of privacy-sensitive robots.[3,4]

Section 2 of the paper explores the definition of personal and non-personal data under the European legal regime in the context of personal robots. Section 3 presents how trust may relate to data governance. Section 4 discusses the current culture around the acceptance of company terms and privacy policies and section 5 presents a comparative analysis of terms of service and policies for four firms. Concluding remarks and future areas of research are

presented in Section 6.

2. Privacy, personal data and non-personal data

According to the European Civil Law Rules in Robotics *"for the time being our legal and regulatory framework is coping well with the current and impending emergence of autonomous robots"*.[5] This view, however, appears to be overoptimistic, especially considering that legal research on data collection, aggregation and governance is at an infant stage.

For example, many legal scholars in the area of smart energy technologies - a field much more mature and prevalent compared to personal robots - address the current lack of laws and regulations around the collection of consumer data.[6] Many of the challenges of emerging technologies, such as privacy and data protection, call for a systematically different approach to legal protection.[7] Existing privacy and data protection laws may be ill-suited since, in reality, consumer privacy is an afterthought[6] and the pervasive lack of transparency of existing systems is a real threat.[7] Legal scholars are just picking up these issues and stress test the scope of current standards and regulations.[8]

Some legal scholars[9–11] 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[12,12] (2012-2014) investigated how existing laws and regulations deal with robots.

2.1. *Personal data*

In the European regime, part of the interaction records with smart technology potentially falls under the General Data Protection Regulation (GDPR) *personal data* definition: *any information related to an identified or identifiable natural person*. But what does *any information* mean in the context of personal robots? And how do we draw a line between what is personal or non-personal? Information like images of human faces are 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?

Legal scholars agree, that AI and Big Data challenge the scope of data protection law and especially the extend to which the data subject can be identifiable.[13–15] In particular, Putrova[14] 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.[8] Anonymised data, can be de-anonymised when combined or correlated with other data-sets and enable inferences to be drawn about specific aspects of an individual's life. This means that there is no guarantee that non-personal data would remain non-personal.

On the practical point of view, the cost to distinguish personal to non-personal data is high. As a result, companies increasingly treat non-personal data as personal data;[16] a practice that seem to be working for this current period. It is yet questionable for how long companies can sustain this, especially considering that the success of new services and technologies depends on interconnected data.

In the future, the broadening scope of the definition of what constitutes personal data would make the GDPR hard to maintain[14] and the law may fall behind new technological advantages.[17] It is, therefore, worthwhile examining another recently introduced legislative concept: non-personal data.

2.2. *Non-personal data*

The EU Communication on Building a European Data Economy[18] and the new Regulation on the free flow of non-personal data[19] initiated its application in May 2019. Machine-generated, non-personal data in the context of Industry 4.0 and Internet of Things (IoT) 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 non-personal, but there are still inferences that could be drawn about the habits or other socioeconomic factors related to an individual user. It is, therefore, unclear whether or how this definition complements the personal data definition and where the line between personal and non-personal should or could be drawn, especially for personal robotics and IoT technologies designed to serve a user.

3. Building trust with humans

The lack of transparency and distinction between personal and non-personal data can be one of the factors causing issues of trust in automation and human-robot interaction. Lewis et al.[20] mention system intelligibility and transparency as one of the core factors affecting trust in automation, while Hancock et al.[21] demonstrated in his meta-analysis that one of the critical factors related to the general performance of the robots in human-robot interaction scenarios included transparency of interaction and, consequently, establishing trust with the robot.

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.[22,23] In cases where the user of a personal robot is not aware of what kind of data are shared during the interaction with the robot, the trust between them suffers.[24,25]

It is also important to investigate further aspects of trust as other authors[3] point out. In human-robot interaction the whole is greater than the sum of its parts, since the social interaction adds an extra layer to the quality of the relationship between the human and the machine. It is, therefore, crucial to understand how users built such trust and whether it is trust in the software, the robot itself, the manufacturer, the brand or the service provided.

4. Agreeing with Terms and Conditions

It is a well-known idea that the vast majority of users rarely read digital contractual agreements, terms and conditions or privacy policy documents.[26] In the past, it has also been observed that firms might take steps to deliberately make such documents less comprehensible.[27]

Under the GPDR the users have to be informed about how their data will be used. There are, however, grey areas such as the relationship between the data processor and data controllers that require clarification.[28] Another area, much less explored, is how comprehensible the agreements between the user (or the 'data subject') and the data controller are and how users perceive such information presented to them.

Trust is built not only by creating transparency in the interaction, but by communicating in a concise way and allowing both parties to define clear boundaries. Trust is certainly an issue when "take-it or leave it" or boilerplate contractual agreements are the norm. In the next section, we explore the differences in such agreements for four firms operating in the fields of social, personal and collaborative robots.

5. A comparative analysis of Privacy Policies and Terms and Conditions

To shed more light on the way user data records are approached in practice, we run a comparative study between commercially available robots. Two of the robots are humanoid and fall under the social robot category, one is a widely used personal cleaning robot while the last one is a collaborative robot arm used in various applications in industrial, medical and personal domains. Table 1 presents the various strategies of the companies regarding data collection from the robot themselves, data sharing policies and how do they handle the derivative Intellectual Property (IP).

5.1. *SoftBank Robotics - Pepper, Nao*

Softbank Robotics humanoids Pepper and Nao are famous around the world for their capabilities as social assistants in education, health care centres and public spaces where they welcome, entertain and facilitate users and visitors.

SoftBank Robotics clearly states in their privacy policy website[29] the practice of collecting dialog data, which may include spoken words and potentially personal or other sensitive information. The sharing of personal data with third parties - which is also part of the policy - may result in personal information being transmitted to third-party providers located outside the European Economic Area. This means the user's data may no longer fall under the scope of the GDPR as they would potentially be transferred to countries with much weaker data or privacy protection regulations.

Under the terms and conditions[30] and more specifically the Intellectual Property section of the agreement, derivative works (including the software generated by a user) are automatically licensed to the company. This may mean that the code a user is creating for the robot could be used, exploited or distributed by the company.

5.2. *Engineered Arts - Robothespian*

Robothespian is an iconic robot actor which is expertly designed for human-robot interaction in the public and capable of expressing a multitude of emotions and speaking more than 30 languages.

When it comes to information related to the interaction with the robot, Engineered Arts[31] collects information associated with the user identity and the time of activity. The data are stored in proprietary servers, and there is no mention of third-party sharing in the privacy policy. Personal data (name, email, address and phone number) are collected as means to contact users. Again no mention of third-party access to personal data is made and according to the policy, only Engineered Arts employees have access to these data.

In terms of Intellectual Property rights, there is no reference to users' rights in relation to any work created using the robot. Considering that Robothespian has been used as an actor in a theatre setting, it might be reasonable to assume that the company does not make any claims of such work as it might conflict with Intellectual Property rights for artistic work.

5.3. *iRobot Corporation - Roomba*

It is has been more than a decade since iRobot Corporation introduced its first robot vacuum in the market, the infamous Roomba, and thereafter altered the landscape of consumer robots and autonomous cleaning devices. Latest products from iRobot are using a machine-generated map of the floor plan that the robot is working on, raising multiple questions regarding the security of the personal data in relation to their users' homes.[32]

The company states clearly in their privacy policy[33] and data protection policy[34,35] the ways they communicate with their users and how their personal data are utilised 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. However, the operational data produced by the robot itself, such as the machine-generated floor plans that include the location of obstacles, are stored in the company's Cloud and are encrypted using unique encryption keys. Nevertheless, there is a grey area in 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.

In terms of Intellectual Property rights, the terms of service[36] clearly state that all the software and services belongs to iRobot and the company holds full rights for all content.

5.4. *Universal Robots - UR3/5/10*

Universal Robots revolutionized the market of industrial robots by launching a family of lightweight, versatile robot arms that are now classified as collaborative ones based on their special design and unique safety features. They are widely used in industry but also in medical, entertainment, and social domains.

The company provides documents online of their privacy policy,[37] the terms of use[38] and the general terms for the developer program.[39] None of these documents mention user-generated data records. Both the privacy policy and the general terms relate mainly to personal data associated with the use and the content of the company's website. We could, therefore, assume that the company does not collect any data related to the operation of the robot or the interaction with the user. [a]

Company	Robot data collection[a]	Data sharing	Derivative IP[b]
SoftBank Robotics	Dialog data	3rd parties	User - Company
Engineered Arts	ID / Activity time log	No	User
iRobot Corporation	Home floor plans	Cloud	N/A
Universal Robots	No	No	User

Table 1: Comparison of different strategies of data collection, sharing and IP.

6. Concluding remarks

This work poses some open questions around the overall framework that personal robots would operate in the future. Privacy and trust are fundamental concepts that the human-robot interaction community recently started exploring. To the best of the authors' knowledge, this is one the earliest work in the field adds a practical dimension to the grey areas of user rights and human-data interaction in the field of robotics.

Despite the limitations in our analysis in terms of extensiveness of this study, the trend appears to be that robots with more sophisticated levels of interaction with the user, may provide less privacy. The question that naturally arises is whether this sacrifice in privacy is the price we have to pay for a smart device. It would be important to define the extend to which this is a design choice in the product architecture made by the firm or an actual functional requirement for the operation of the robot. A way forward would be defining clearly the information that can be processed locally by a robot and the information that

[a] initiated by the hardware
[b] related to software or cyber-physical components

is necessary to be sent back to the firm (e.g. trouble-shooting to improve specific features, data for training an algorithm).

Another concept to explore is whether the business scope of a firm 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.

Intellectual Property in relation to derivable work generated by the user, such as code, software or cyber-physical components, is another important area of the interaction that has not been previously explored in the literature. In this work, the robot with the most sophisticated levels of interaction may be considered to create additional limitations the user's Intellectual Property rights by granting a license of the derivable work to the firm. Especially under the lens of the user as a prosumer[40] (the individual that may both consume and produce a product), a question that may arise is how any alternative or more refined models of user rights would be desirable or beneficial to both the user and the firm.

To drive this discourse beyond the research context, we need to consider new ways to resolve the issues presented in this paper. A practical area of action would be working on the user-friendliness and customisable aspects of digital agreements to drive more transparency and flexibility in the user-robot interaction. Also, as it has been already suggested by other authors,[3] Standardisation (e.g. ISO standards) and the creation of a new class of jobs[41] to bridge the gap between privacy and engineering could create immense value in the field.

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.

The authors would like to extend their deepest gratitude to Dr. Matthew Rueben for his valuable feedback and contribution in this paper.

References

1. E. Commission, Ethics guidelines for trustworthy ai (visited on 09-03-2019).
2. L. Floridi, Translating principles into practices of digital ethics: Five risks of being unethical *Philosophy & Technology* (Springer, 2019). https://doi.org/10.1007/s13347-019-00354-x.
3. M. Rueben, A. M. Aroyo, C. Lutz, J. Schmolz, P. Van Cleynenbreugel, A. Corti, S. Agrawal and W. D. Smart, Themes and research directions in privacy-sensitive robotics, in *2018 IEEE Workshop on Advanced Robotics and its Social Impacts (ARSO)*, (Genova, Italy, 2018).
4. M. Rueben and W. D. Smart, Privacy in human-robot interaction: Survey and future work, in *We Robot 2016: the Fifth Annual Conference on Legal and Policy Issues relating to Robotics. University of Miami School of Law, 2016, Discussant: Ashkan Soltani, Independent Researcher*, 2016.
5. N. Nevejans, European civil law rules in robotics (visited on 08-02-2019).
6. M. Mylrea, Smart energy-internet-of-things opportunities require smart treatment of legal, privacy and cybersecurity challenges *The Journal of World Energy Law & Business* **10**2017. https://doi.org/10.1093/jwelb/jwx001.
7. M. Hildebrandt and B.-J. Koops, The challenges of ambient law and legal protection in the profiling era *The Modern Law Review* **73**2010. https://doi.org/10.1111/j.1468-2230.2010.00806.x.
8. A. Mattoo and J. P. Meltzer, International data flows and privacy: The conflict and its resolution *Journal of International Economic Law* **21** (Oxford University Press, 2018). https://doi.org/10.1596/1813-9450-8431.
9. M. E. Kaminski, Robots in the home: What will we have agreed to *Idaho L. Rev.* **51** (HeinOnline, 2014).
10. R. Y. Wong and D. K. Mulligan, These aren't the autonomous drones you're looking for: investigating privacy concerns through concept videos *Journal of Human-Robot Interaction* **5** (Journal of Human-Robot Interaction Steering Committee, 2016).

11. J. M. Balkin, Free speech in the algorithmic society: big data, private governance, and new school speech regulation *UCDL Rev.* **51** (HeinOnline, 2017).
12. C. Holder, V. Khurana, F. Harrison and L. Jacobs, *Computer Law & Security Review* **32**, 383 (2016).
13. P. Nemitz, Constitutional democracy and technology in the age of artificial intelligence *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* **376** (The Royal Society Publishing, 2018). https://doi.org/10.1098/RSTA.2018.0089.
14. N. Purtova, The law of everything. broad concept of personal data and future of eu data protection law *Law, Innovation and Technology* **10** (Taylor & Francis, 2018). https://doi.org/10.1080/17579961.2018.1452176.
15. 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).
16. H. Richter and P. R. Slowinski, The data sharing economy: On the emergence of new intermediaries *IIC-International Review of Intellectual Property and Competition Law* **50** (Springer, 2019). https://doi.org/10.1007/s40319-018-00777-7.
17. T. Li, E. F. Villaronga and P. Kieseberg, Humans forget, machines remember: Artificial intelligence and the right to be forgotten (LawArXiv, 2017). https://doi.org/10.31228/osf.io/zs8kb.
18. T. E. Commission, Digital single market strategy - building a european data economy (visited on 08-02-2019), https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy.
19. T. E. Parliament and the Council of the European Union, Regulation on the free flow of non-personal data (visited on 08-02-2019), https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1546942605408&uri=CELEX:32018R1807.
20. M. Lewis, K. Sycara and P. Walker, *The Role of Trust in Human-Robot Interaction*, in *Foundations of Trusted Autonomy*, eds. H. A. Abbass, J. Scholz and D. J. Reid (Springer International Publishing, Cham, 2018), Cham, pp. 135–159. https://doi.org/10.1007/978-3-319-64816-3_8.
21. 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 *Human factors* **53** (Sage Publications Sage CA: Los Angeles, CA, 2011). https://doi.org/10.1177/0018720811417254.
22. K. Sycara and M. Lewis, Forming shared mental models, in *Proc. of the 13th Annual Meeting of the Cognitive Science Society*, 1991.
23. P. F. Dominey and F. Warneken, The basis of shared intentions in human and robot cognition *New Ideas in Psychology* **29** (Elsevier, 2011). http://doi.org/10.1016/j.newideapsych.2009.07.006.
24. S. Vinanzi, M. Patacchiola, A. Chella and A. Cangelosi, Would a robot trust you? developmental robotics model of trust and theory of mind *Philosophical Transactions of the Royal Society B: Biological Sciences* **374**2019. https://doi.org/10.1098/rstb.2018.0032.
25. P. A. Hancock, D. R. Billings and K. E. Schaefer, Can you trust your robot? *Ergonomics in Design* **19**2011. https://doi.org/10.1177/1064804611415045.
26. M. J. Radin, The deformation of contract in the information society *Oxford Journal of Legal Studies* **37** (Oxford University Press, 2017). https://doi.org/10.1093/ojls/gqx001.
27. R. Van Loo, Helping buyers beware: The need for supervision of big retail *University of Pennsylvania Law Review* **163** (HeinOnline, 2014).
28. J. Lindqvist, New challenges to personal data processing agreements: is the gdpr fit to deal with contract, accountability and liability in a world of the internet of things? *International Journal of Law and Information Technology* **26** (Oxford University Press, 2017). https://doi.org/10.1093/ijlit/eax024.
29. S. Robotics, Privacy policy (visited on 04-03-2019), https://www.softbankrobotics.com/emea/en/privacy-policy.
30. S. Robotics, Terms of use (visited on 04-03-2019), https://www.softbankrobotics.com/emea/en/term-use.
31. E. Arts, Privacy policy (visited on 04-03-2019), https://www.engineeredarts.co.uk/privacy-policy/.
32. T. N. Y. Times, Your roomba may be mapping your home, collecting data that could be shared (visited on 01-06-2019), https://www.nytimes.com/2017/07/25/technology/roomba-irobot-data-privacy.html.

33. iRobot Corporation, Privacy policy (visited on 17-04-2019), https://www.irobot.com/legal/privacy-policy.
34. iRobot Corporation, Data security (visited on 17-04-2019), https://www.irobot.com/legal/data-security.
35. iRobot Corporation, irobot roomba privacy and data sharing (visited on 17-04-2019), https://homesupport.irobot.com/app/answers/detail/a_id/964/~/irobot-roomba-privacy-and-data-sharing.
36. iRobot, irobot terms of service (visited on 17-04-2019), https://www.irobot.ie/legal/terms-of-service.
37. U. Robots, Privacy policy (visited on 15-04-2019), https://www.universal-robots.com/media/1802831/privacy-policy-universal-robots-2018.pdf.
38. U. Robots, Universal robots a/s terms of use (visited on 15-04-2019), https://www.universal-robots.com/media/876344/tou_universalrobots_ukversion_markup_28082015-final.pdf.
39. U. Robots, Development agreement (visited on 15-04-2019), https://www.universal-robots.com/media/1800135/urplus-developer-agreement-v4.pdf.
40. P. Kotler, The prosumer movement, in *Prosumer Revisited*, (Springer, 2010) pp. 51–60.
41. C. Galindo, A. Saffiotti, S. Coradeschi, P. Buschka, J.-A. Fernandez-Madrigal and J. González, Multi-hierarchical semantic maps for mobile robotics, in *2005 IEEE/RSJ International Conference on Intelligent Robots and Systems*, 2005.