Anthropomorphism, privacy and security concerns: preliminary work

Eloïse Zehnder, Jérôme Dinet, François Charpillet

Anthropomorphism, privacy and security concerns: preliminary work

Eloïse Zehnder
Université de Lorraine, 2LPN, Inria
F-54000 Nancy & Villers-lès-Nancy, France
eloise.zehnder@univ-lorraine.fr

Jérôme Dinet
Université de Lorraine, 2LPN
F-54000 Nancy, France
jerome.dinet@univ-lorraine.fr

François Charpillet
University of Lorraine, CNRS, Inria, Loria
F-5400, Villers-lès-Nancy, France
francois.charpillet@inria.fr

Abstract
The acceleration of the diffusion of domestic and social robots leads to new issues specific to connected tools, such as the acceptability of data harvesting, the intrusion of privacy and the risks related to information security. While these concerns exist, individuals remain inclined to buy and use robots they are going to share intimate information. The objective of this paper is to address these issues by considering the anthropomorphic character and the social capabilities of robots. We then propose an experimental setting to explore how privacy, security and intimacy are perceived among the owners (while measuring their level of loneliness) of different types of personal or home robots.

Author Keywords
Human-robot interaction; anthropomorphism; intimacy; privacy; security.

CSS Concepts
• Security and privacy~Human and societal aspects of security and privacy~Usability in security and privacy; Human-centered computing~Interaction design;

Introduction
Today, ailments such as the feeling of loneliness can affect a significant percentage of the population while

having adverse effects on mental and physical health [7]. Social and other companion robots can then appear as a solution to respond in a direct way (with companions designed for companionship or inciting reconnection with others) or an indirect one (with robots or machines not designed to counter loneliness but which will give a sense of social presence, especially to people suffering from loneliness [11].

However, issues limiting the acceptability and adoption of companion or assistant robots remain, particularly with respect to privacy and security concerns [10, 24, 26].

Indeed, as machines, these companions and social robots have different types of sensors (e.g., touch sensors, localization, complex and simple vision, light, speed, sound...), which will collect and store data from users and their environment. Added to this, personal robots or companions are often linked to user accounts which, in turn, will contain data provided by the robot (environment, user preferences) or the user himself (identity, preferences, environment). The accounts can be managed through applications available on smartphones, web or tablets that will request authorizations from users in order to use the sensors of the device or to access some information. Thus, at least two devices can collect more or less intrusive data on users and their environment, and obtain authorizations on their devices, in exchange for their use.

Added to this, more or less social interactions can happen between users and their robots, inciting users to self-disclose more personal information that can be directly used and stored, or not.

Indeed, following the CASA (Computers are social actors) paradigm [29], humans will automatically apply social rules and expectations to computers even while knowing they are just machines. This type of interaction can serve as "social snacking" while an individual may experience loneliness or at least, the need to belong [21]. For example, in a study on Roomba© robots [13], half of the families using the vacuum cleaners (which are not socially oriented robots) had social relationships with them (such as talking to it while it was running). Robots can then easily intrude into a user's intimate life.

But as privacy and security concerns remain among the population, millions of robots and assistants are still sold to this day, which means data collection seems, a priori, accepted and acceptable for some users. This seems paradoxical when privacy concerns, and by extension security concerns, affect trust, usage intentions, and information sharing intentions.

While there is a privacy and security trade-off for better usability of the systems, how can we explain the apparent acceptability of robots and companions while the concerns remain?

Privacy and security regarding personal robots

Privacy and security concerns are known to be a barrier to adoption [31]. The concepts of privacy and privacy concerns have been studied in various number of contexts. In mobile apps, it represents "the ability of the individual to control when, how and to what extent, their personal information is communicated to mobile apps [15]. Other authors [25] focus on the context of social robots, distinguishing the concept of physical privacy (the physical and or private space or surroundings a robot can have access to), from the concept of

informational privacy. Informational privacy is then divided into two subcategories, with one relating to institutional threats (data processed by institutions, e.g. robot manufacturers, government agencies and third parties) and one relating to social threats (data processed by private individuals; e.g. familiar users or hackers) [33, 41].

When it comes to privacy concerns regarding robots, Lutz and Tamo-Larrieux [25] found three types of privacy concerns in their study. Respondents worried most about their informational privacy, especially regarding institutions such as the social robot manufacturer. Social privacy risks, such as hacking and stalking, also evoked considerable concerns. Physical privacy concerns were less prevalent. Along with privacy, security perceptions affect user intentions and behaviors [32, 40]. The concept of perceived security has been studied a lot in the field of online transactions and little has been made regarding robotics. Following the Balapour et al. [3] definition of the perceived security of mobile apps, we could define it as the perception of the robot provider's appropriate actions to safeguard shared information from security breaches during and after transmission through the robotic system [4, 18, 32].

Users' perceptions of security can affect their attitudes and behaviors directly and indirectly. For example, Chellappa [8] and Bansal [4] demonstrated that an individual's perception of security is very important for trust (indirect) during any form of electronic transaction, which can fuel users' behavioral intentions (direct), such as their intention to share private information with websites [5]. Users have little control over the information security of a robotic system, choosing the information and data to transmit or not is more accessible than the security of a system for users. But to engage informed behaviors and decisions about their privacy and private information, users should first be aware of the privacy policies.

Privacy paradox and biases in disclosure

But among individuals, inconsistencies between the stated privacy preferences and the actual disclosure behavior remain. In 2007, Norberg and al. [30] called it the "privacy paradox". The phenomenon happens even when, for example, in the context of internet usage, users show a strong interest in privacy while disclosing substantial personal information. For example, a study from Huberman et al. [16], suggests that people will disclose less desirable, or embarrassing data for a greater price but are willing to disclose information they perceive as harmless for little to no rewards. When it comes to disclosure and privacy individuals do not make rational decisions [2]. In his work, Waldman [39] outlines biases and dark patterns that could influence users' privacy decisions. For example, privacy policies are known to be generally so long [34] and difficult, which can even give trouble to experts [28]. It would also take an average of 244 hours per year to read every privacy policy that an individual visits [9]. In the same work, Waldman [39] also cites potential dark patterns and cognitive biases which represent a barrier to rational privacy and disclosure decision making [1] such as anchoring, framing, hyperbolic discounting or overchoices.

Thus, making informed decisions when it comes to privacy policies of an application, a website or even a robot can demand a substantial effort from the user.

The robots' design

When it comes to privacy and security perception, the robots' appearance can play another role. In "Averting Robot Eyes" [20], Kaminsky and her colleagues identify a potential "dishonest anthropomorphism" exhibited by robots which may be designed to trigger very human and social reactions to robots' anthropomorphic appearances and behaviors. Leong and Selinger [23] deepen this notion of dishonest anthropomorphism through examples of designs allowing to abuse or to mislead users about the real capabilities of robots. For example, human responses to the appearance or the attractiveness of a robot may impact how humans are likely to try to please a robot and display other innate responses to beauty, which may nudge bonding, attachment and trust. Moreover, loneliness impacts the perception of non-human entities. Lonely people for example, compensate for their lack of social connection through anthropomorphization (the attribution of human traits, emotions, intentions or to non-human entities) [11]. Loneliness even increases the anthropomorphization of non-human agents and makes lonely people feel a higher social presence [22], increasing the effects of a potential dishonestly anthropomorphic robot.

While privacy policies may be unclear or difficult for users to access, the appearance of robots and their behavior can add more difficulty to this and mislead users into disclosing more information than they'd want.

Disclosing to a robot: the role of intimacy

What could also be misleading for users is the intimacy process they can possibly have with machines or robots. Disclosing information to another human leads to intimacy and so does it with robots. For Reis and Shaver [36], intimacy is a transactional process where two components (self-disclosure and perceived responsiveness) facilitate a close connection between people. The intimacy process happens when a person (speaker) discloses personal information and feelings to a partner (listener), who will then respond by also disclosing personal information and feelings. For them, the interaction is perceived as intimate when the speaker interprets the listener's response as understanding, validating, and caring. Later, Reis and Patrick [35] suggest it's actually more important than the actual disclosure. Thus, according to the model, self-disclosure and partner disclosure both predict intimacy, with perceived partner responsiveness as a mediator in the model.

Thus, a human-robot interaction can easily become intimate, especially if the robot has well developed social skills. But it's not mandatory. For example, [38] showed in their study how users have come to show signs of intimacy with their robot vacuum cleaners (which are not social robots). The other way around [19], in another study where a highly social robot was sharing a secret with participants, most participants (59%) chose to not share it afterward. As a result, robots with different social skills and different appearances can bring users to become intimate with them and develop relationships resembling human-human interaction. But as beneficial anthropomorphism could be to build a fulfilling relationship with a robot, especially for lonely people [22], it could also be misleading with it comes to making informed decisions regarding what users know about privacy policies and the information they choose to disclose. We make the assumption that H1: the higher the intimacy scores will be, the lower the security and privacy scores will be.

Also, since lonelier people tend to turn to robots more easily for social interactions, thus, leading to more intimacy, we assume the following hypothesis: H2: The lonelier a user is, the more he'll perceive as intimate the relationship he has with his robot

We note that the consequences of a security breach in the robotic system leading to an attack, not only would harm trust in the company but also harm the human-robot relationship. It then appears important for users to at least be conscious of the security risks while using a robotic system. A recent work, "The Principles of Robotics" [6] includes the maxim that robots "should not be designed in a deceptive way to exploit vulnerable users," which, more specifically, means that "their machine nature should be transparent and the illusion of emotions and intent should not be used to exploit vulnerable users". We could easily see lonely people who will tend to anthropomorphize technologies more and are more likely to confide in them as such.

Since a robots' appearance can influence a user into perceiving it in a more anthropomorphic way, we suppose that this appearance can lead users to think of robots are more reliable when it comes to perceived privacy and security. We then make the hypothesis: H3: the more anthropomorphic the robot will be perceived as, the more secure and private it's going to be perceived as.

Proposed method

Since the design of technologies and more precisely robots, seem to influence privacy and to an extent, security perceptions, we plan to study the perception of the owners (minimum 15) of these 5 different robots:

- iRobot Roomba© (vacuum robot)
- Amazon Echo© (vocal assistant)
- Google Home© (vocal assistant)
- Replika© (personal chatbot)
- Cozmo© (toy robot).

These robots were all widely sold (at least a million of sales, or downloads for the applications) and all have anthropomorphic traits or have been anthropomorphized at least once by users, despite having very different purposes and appearances. Each of these robots is linked to an application that can be found on the Google Play Store. For users, it is required to install and use those applications which require authentications and authorizations for proper use of the robot. The Exodus website [12] allows us to easily make a comparison of the permissions and trackers found in each of the applications in order to realize the more or less invasive character of the various robots (Table 1). This listing provides us with material for interpreting future results. In Table 1, we chose to only gather the permissions considered as dangerous or special according to Googles' types of permissions. Special permissions generally allow an application to deploy powerful actions such as drawing over another application, while dangerous permissions give an application access to restricted or private data.

The following scales are chosen to measure perceived security and privacy concerns, the level of loneliness, perceived anthropomorphism, intimacy with the robot and overall acceptance of the robot for its use:

- Perceived Security and privacy [8]
- Miller Social Intimacy Scale (MSIS) [27]
- UCLA Loneliness scale (short) [17]

- Anthropomorphism (Human-Robot Interaction Evaluation Scale (HRIES)) [37]
- Acceptance (The Almere model) [14]

Comparing the previous scales depending on the different robots types, the levels of anthropomorphism, and intimacy and loneliness should lead us to better see how users perceive personal robots and how they become accepting and motivated to make concessions with their personal information privacy and security to gain access to the use of a robot.

Our paper proposes a literature study that highlights the impact of different phenomena on the perception and acceptance of personal and domestic robots as data gatherers. We combined this work with a listing of the trackers and permissions of the most sold robots (which users are not always aware of).

The whole reinforces the idea that privacy and security issues are important to consider for the development of robotic technologies. We thus hope that the results will bring a contribution to drawing one of the many lines of robotics' ethical issues.

	Google Home	**Amazon Alexa**	**iRobot Roomba**	**Replika**	**Cozmo**
Dangerous or special permissions	6	15	5	5	3
ACCESS_COARSE_LOCATION		X	X		X
ACCESS_FINE_LOCATION	X	X	X		
ANSWER_PHONE_CALLS		X			
CALL_PHONE	X	X			
CAMERA	X	X		X	
GET_ACCOUNTS	X	X			
READ_CONTACTS		X			
READ_EXTERNAL_STORAGE		X	X	X	X
READ_PHONE_STATE		X		X	
READ_SMS		X			
RECEIVE_MMS		X			
RECEIVE_SMS		X			
SEND_SMS		X			
RECORD_AUDIO	X	X		X	
WRITE_EXTERNAL_STORAGE	X	X	X	X	X
Permissions (total)	20	80	17	17	26
Trackers	2	5	5	9	1

Table 1: Number of permissions and trackers found in each application, linked to each assistant or social robot

References

[1] Alessandro Acquisti, Laura Brandimarte and George Loewenstein. 2015. Privacy and human behavior in the age of information. *Science*, *347*, 6221: 509-514.

[2] Alessandro Acquisti. Jens Grossklags. 2007. What can behavioral economics teach us about privacy. *Digital privacy: theory, technologies and practices*, 18: 363-377.

[3] Ali Balapour, Hamid Reza Nikkhah, and Rajiv Sabherwal. 2020. Mobile application security: Role of perceived privacy as the predictor of security perceptions*. International Journal of Information Management 52*: 102063.

[4] Gaurav Bansal. 2016. Distinguishing between Privacy and Security Concerns: An Empirical Examination and Scale Validation*. Journal of Computer Information Systems 57*, 4: 330–343.

[5] Gaurav Bansal, Fatemeh 'Mariam' Zahedi, and David Gefen. 2015. The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern. *European Journal of Information Systems 24*, 6: 624–644.

[6] Margaret Boden, Joanna Bryson, Darwin Caldwell, et al. 2017. Principles of robotics: regulating robots in the real world. *Connection Science 29*, 2: 124–129.

[7] John T. Cacioppo and Stephanie Cacioppo. 2018. Loneliness in the Modern Age: An Evolutionary Theory of Loneliness (ETL). In Advances in Experimental Social Psychology. *Elsevier*, 127–197.

[8] Ramnath K. Chellappa. 2008. Consumers' trust in electronic commerce transactions: the role of perceived privacy and perceived security. *under submission*, *13*.

[9] Lorrie Faith Cranor. 2012. Necessary but not sufficient: standardized methods for privacy notice an choice. *J. on Telecomm. & High Tech L, 10*: 273-307.

[10] Tamara Dinev and Paul Hart. 2006. An Extended Privacy Calculus Model for E-Commerce Transactions*. Information Systems Research 17*, 1: 61–80.

[11] Nicholas Epley, Scott Akalis, Adam Waytz, and John T. Cacioppo. 2008. Creating Social Connection Through Inferential Reproduction. *Psychological Science 19*, 2: 114–120.

[12] Exodus Privacy. 2021. Retrieved April 30, 2021 from https://exodus-privacy.eu.org/fr/

[13] Jodi Forlizzi and Carl DiSalvo. 2006. Service robots in the domestic environment. *Proceeding of the 1st ACM SIGCHI/SIGART conference on Human-robot interaction - HRI '06,* ACM Press.

[14] Marcel Heerink, Ben Kröse, Vanessa Evers, and Bob Wielinga. 2010. Assessing Acceptance of Assistive Social Agent Technology by Older Adults: the Almere Model. *International Journal of Social Robotics 2*, 4: 361–375.

[15] Weiyin Hong and James Y. L. Thong. 2013. Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies*. MIS Quarterly 37*, 1: 275–298.

[16] Bernardo A. Huberman, Eytan Adar, and Leslie R. Fine. 2005. Valuating Privacy. *IEEE Security and Privacy Magazine 3*, 5: 22–25.

[17] Mary Elizabeth Hughes, Linda J. Waite, Louise C. Hawkley, and John T. Cacioppo. 2004. A Short Scale for Measuring Loneliness in Large Surveys. Research on Aging 26, 6: 655–672

[18] Vess L. Johnson, Angelina Kiser, Ronald Washington, and Russell Torres. 2018. Limitations to the rapid adoption of M-payment services: Understanding the impact of privacy risk on M-

Payment services. *Computers in Human Behavior 79*: 111–122.

[19] Peter H. Kahn Jr., Takayuki Kanda, Hiroshi Ishiguro, et al. 2015. Will People Keep the Secret of a Humanoid Robot?. Proceedings of the Tenth Annual ACM/IEEE International Conference on Human-Robot Interaction, ACM.

[20] Margot E. Kaminski, Matthew Rueben, William D Smart and Cindy M. Grimm. 2016. Averting robot eyes. *Md. L. Rev.*, *76*, 983.

[21] Nicole C. Krämer, Gale Lucas, Lea Schmitt, and Jonathan Gratch. 2018. Social snacking with a virtual agent – On the interrelation of need to belong and effects of social responsiveness when interacting with artificial entities. *International Journal of Human-Computer Studies 109*: 112–121.

[22] Kwan Min Lee, Younbo Jung, Jaywoo Kim, and Sang Ryong Kim. 2006. Are physically embodied social agents better than disembodied social agents?: The effects of physical embodiment, tactile interaction, and people's loneliness in human–robot interaction*. International Journal of Human-Computer Studies 64*, 10: 962–973.

[23] Brenda Leong and Evan Selinger. 2019. Robot Eyes Wide Shut. Proceedings of the Conference on Fairness, Accountability, and Transparency, ACM.

[24] Paul Benjamin Lowry, Jinwei Cao, and Andrea Everard. 2011. Privacy Concerns Versus Desire for Interpersonal Awareness in Driving the Use of Self-Disclosure Technologies: The Case of Instant Messaging in Two Cultures. *Journal of Management Information Systems 27*, 4: 163–200.

[25] Christoph Lutz and Aurelia Tamó-Larrieux. 2020. The Robot Privacy Paradox: Understanding How Privacy Concerns Shape Intentions to Use Social Robots. *Human-Machine Communication 1*: 87–111.

[26] Naresh K. Malhotra, Sung S. Kim, and James Agarwal. 2004. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research 15*, 4: 336–355.

[27] Rickey S. Miller and Herbert M. Lefcourt. 1982. The Assessment of Social Intimacy. *Journal of Personality Assessment 46, 5*: 514–518.

[28] George R. Milne, Mary J. Culnan, and Henry Greene. 2006. A Longitudinal Assessment of Online Privacy Notice Readability. *Journal of Public Policy & Marketing 25, 2*: 238–249.

[29] Clifford Nass and Youngme Moon. 2000. Machines and Mindlessness: Social Responses to Computers. Journal of Social Issues 56, 1: 81–103.

[30] Patricia A. Norberg, Daniel R. Horne, and David A. Horne. 2007. The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. Journal of Consumer Affairs 41, 1: 100–126.

[31] Pardis Emami-Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Cranor and Norman Sadeh. 2017. Privacy Expectations and Preferences in an IoT World, in: Proceedings of the 2017 Symposium on Usable Privacy and Security, SOUPS'17, USENIX Association, Berkeley, CA, USA. 399-412.

[32] Paul A. Pavlou, Huigang Liang, and Yajiong Xue. 2007. Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective*. MIS Quarterly 31*, 1: 105

[33] Kate Raynes-Goldie. 2010. Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. First Monday.

[34] Joel R. Reidenberg, Travis Breaux, Lorrie Faith Cranor, et al. 2014. Disagreeable Privacy Policies: Mismatches between Meaning and Userss Understanding. *SSRN Electronic Journal*, 39.

[35] Harry T. Reis and Brian C. Patrick. 1996. Attachment and intimacy: Component processes. In E. T. Higgins & A. W. Kruglanski (Eds.), *Social psychology: Handbook of basic principles*. The Guilford Press. 523-563.

[36] Harry T. Reis and Phillip Shaver. 1988. Intimacy as an interpersonal process. In S. Duck (Ed.), *Handbook of personal relationships*. Chischester, England: Wiley. 367-389.

[37] Nicolas Spatola, Barbara Kühnlenz, and Gordon Cheng. 2021. Perception and Evaluation in Human–Robot Interaction: The Human–Robot Interaction Evaluation Scale (HRIES)—A Multicomponent Approach of Anthropomorphism. *International Journal of Social Robotics,* 1-23.

[38] Ja-Young Sung, Lan Guo, Rebecca E. Grinter, and Henrik I. Christensen. "My Roomba Is Rambo": Intimate Home Appliances. In UbiComp 2007: Ubiquitous Computing. *Springer Berlin Heidelberg*, 145–162.

[39] Ari Ezra Waldman. 2020. Cognitive biases, dark patterns, and the 'privacy paradox.' *Current Opinion in Psychology 31*: 105–109.

[40] Garry White, Tahir Ekin, and Lucian Visinescu. 2016. Analysis of Protective Behavior and Security Incidents for Home Computers. *Journal of Computer Information Systems 57*, 4: 353–363.

[41] Alyson Leigh Young and Anabel Quan-Haase. 2013. Privacy protection strategies on Facebook. *Information, Communication & Society 16*, 4: 479–500.