Privacy in the Age of the Internet of Things: Perceptions and Practices in Domestic Settings

Ana Delicado, Marta Rosales, Ana Viseu, Jussara Rowland, and Mónica Truninger

Privacy Studies Journal
ISSN: 2794-3941

Vol. 4 (2025): 31-58

Abstract:
Scientific and media discourse on the Internet of Things (IoT) emphasizes privacy concerns as a possible hurdle to widespread adoption. Drawing on a study conducted with users of home IoT devices and stakeholders, this article examines their perceptions, attitudes, and practices through the framework of privacy concerns, privacy rationales, and privacy work. The results show that users are ambivalent regarding data collection and transfer by IoT devices, oscillating between the advantages of personalization and fears of data commercialization, often accompanied by feelings of powerlessness and privacy resignation. Privacy rationales frequently translate into privacy work that includes rejection, digital housekeeping, and finding appropriate locations in the home. As IoT adoption expands beyond higher educated and higher skilled users, more effort should be made in regulating products and protecting citizens from the increased datafication of everyday life.

Keywords
IoT, home, privacy concerns, privacy rationales, privacy work

Introduction

Much like with other digital technologies, the media is awash with stories on how Internet of Things (IoT) devices breach the privacy of their users by collecting and sending out information on them. From teddy bears that spy on children to robot vacuum cleaners that photograph users in the bathroom, from security cameras that show what goes on at home to smart speaker assistants that eavesdrop on conversations, by design or by disaster these increasingly common appliances pose significant privacy risks.

How do users perceive these risks? How aware and concerned are they of the personal information being collected and made available to outsiders or even to other household members? What strategies ("privacy work") do they deploy to protect their data? Which "privacy rationales" do they mobilize? Or, conversely, do users express "privacy resignation" or apathy that their privacy will be breached anyway?

Based on interviews with household members and stakeholders in Portugal, in this article, we explore privacy perceptions and practices regarding the use of IoT devices at home by focusing on the triad of privacy concerns, privacy rationales, and privacy work. We also seek to examine whether these perceptions and practices vary according to gender, age, household composition (with/without children), or occupation. Furthermore, we compare these perceptions and practices with expert opinions from stakeholders regarding privacy risks and protection strategies in households.

Framework

One of the distinctive features of IoT devices is the ability to collect data through sensors, microphones, cameras, or information provided by users. These data can be stored on the device itself or another user device (mobile phone, computer) but are often sent to the "cloud" of the manufacturer or service provider. Data surveillance or "dataveillance"[1] can be used by the company to improve its services or for more nefarious purposes: advertising and selling other products (an expression of the surveillance capitalism coined by Zuboff)[2] or handing data over to other companies or security forces (see the case of the doorbell with camera marketed by Amazon studied by Bridges).[3] Another risk is that the data can be highjacked by hackers.[4]

1 José Van Dijck, "Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology," *Surveillance & society* 12, no. 2 (2014): 197–208, https://doi.org/10.24908/ss.v12i2.4776

2 According to Zuboff, surveillance capitalism appropriates private experiences and turns them fungible commodities to be bought and sold by companies. Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Public Affairs, 2019).

3 According to Bridges, the Amazon Ring doorbell with a camera is used by police forces to survey neighbourhoods and persecute people (usually from minority backgrounds) perceived as trespassers or potential criminals. Lauren Bridges, "Infrastructural Obfuscation: Unpacking the Carceral Logics of the Ring Surveillant Assemblage," *Information, Communication & Society* 24, no. 6 (26 April, 2021): 830–49, https://doi.org/10.1080/1369118X.2021.1909097.

4 Asreen Rostami, Minna Vigren, Shahid Raza, and Barry Brown, "Being Hacked: Understanding Victims' Experiences of IoT Hacking," *Eighteenth Symposium on Usable Privacy and Security* (SOUPS 2022) (2022): 613–631.

In an early review article on the social dimensions of IoT, Lupton examines sociotechnical imaginaries connected to these technologies. She identifies both utopian visions focused on economic and social benefits and dystopian imaginaries compounding surveillance by governments, leakage of personal data, breach of privacy, unauthorized access with pernicious intent, exploitation of data by third parties, discrimination against marginalized groups, cybercrime, identity theft, denial of opportunities (credit, insurance, social services), and intrafamilial violence. [5]

Concomitantly, in her work about the cultural ideas of home, Chambers devotes a chapter to the homes of the future, in which IoT devices take centre stage. She highlights how IoT raises critical questions about privacy: always on in the background, collecting vast amounts of data about personal habits, often without the user's knowledge "IoT enabled items are designed to generate a sense of security and control over the home yet these same devices generate palpable home precarities by causing breaches of privacy". [6]

Based on interviews with experts, Sovacool and Del Rio ascertained that privacy, security, and hacking were the most frequently identified barriers to adoption of smart home technology, thus suggesting policy recommendations to increase consumer protection, privacy, and data security. [7]

Studies of the lived experience of IoT users indicate concern about data privacy and potential security risks posed by external parties accessing data generated by IoT devices.[8] Coughlan and his team analysed the acceptance of IoT at home through a scenarios-based survey and learned that privacy was a key criterion for most users. The authors consider the home a highly personal space, where privacy, ownership, and control are paramount factors, even if many IoT users lack awareness of how their data is being collected and potentially used. IoT devices do not necessarily collect "personal data", but personal information can be derived through collation or contextual information. The survey also showed that privacy has a complex relationship with usefulness, even though higher perceived usefulness can make a device seem less invasive. Respondents were more reluctant to share their data with companies than with public entities and believed it was possible to opt out. They also showed concern with the information other household members could access, which, according to the authors, could cause particular tensions with children striving for autonomy and older people seeking to maintain their privacy and autonomy from carers.[9]

5 Deborah Lupton, "The Internet of Things: Social Dimensions," *Sociology Compass* 14, no. 4 (April, 2020), https://doi.org/10.1111/soc4.12770.

6 Deborah Chambers, *Cultural Ideals of Home: The Social Dynamics of Domestic Space* (Routledge, 2020), 203.

7 Benjamin K. Sovacool and Dylan D. Furszyfer Del Rio, "Smart Home Technologies in Europe: A Critical Review of Concepts, Benefits, Risks and Policies," *Renewable and Sustainable Energy Reviews* 120 (March, 2020): 109663, https://doi.org/10.1016/j.rser.2019.109663.

8 Yolande Strengers, Jenny Kennedy, Paula Arcari, Larissa Nicholls, and Melissa Gregg, "Protection, Productivity and Pleasure in the Smart Home: Emerging Expectations and Gendered Insights from Australian Early Adopters," *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (2019): 1–13, https://doi.org/10.1145/3290605.3300875.

9 Tim Coughlan, Michael Brown, Richard Mortier, Robert J. Houghton, Murray Goulden, and Glyn Lawson, "Exploring Acceptance and Consequences of the Internet of Things in the Home," *2012 IEEE International Conference on Green Computing and Communications* (2012): 148–55, https://doi.org/10.1109/GreenCom.2012.32.

Aguirre and colleagues address the personalization-privacy paradox of IoT. Personalized communication between companies and consumers can enhance engagement but can also raise privacy concerns regarding personal data and thus decrease engagement. IoT devices not only collect continuous information about consumers' daily lives but also contain "algorithms that enable them to learn from their interactions with the customer, in support of even greater personalization and optimization opportunities", which may heighten privacy concerns and hinder adoption.[10]

Another strand of literature focuses on privacy protection for particular types of users of IoT, specifically children. This strand prioritizes the analysis of internet-connected toys,[11] as well as other IoT devices, such as smart speaker assistants, smartwatches, cameras, or "baby tech" products (e.g. connected baby bottles)[12] and their role in datafying a generation who are too young to understand and consent to data collection and other security issues. These devices are prone to security flaws and data breaches that can endanger children's privacy and well-being and generate data that can be used to make decisions about their lives, giving "the illusion of objectivity and neutrality while […] representing only the aspects of a child's life that a company has chosen to record."[13]

Besides the literature on IoT in general, several studies focus on the privacy issues raised by particular types of IoT devices. Such is the case of "wearables": computational or sensory electronic devices worn with clothing or on the body that transmit information to phones or computers, but also to the manufacturing companies.[14] By monitoring daily movements and body functions (such as heart rate, breathing, and sleep), they contribute to the "quantified self",[15] allowing users to track and improve their health and fitness. However, this data collection raises privacy concerns regarding the security of data storage and transfer (e.g. encryption), as well as its unauthorized use for marketing or insurance purposes.[16]

Smart speakers are another type of device that merits particular attention in terms of privacy. Pridmore et al. conducted a study on smart speakers (using the term Intelligent Per-

10 Elizabeth Aguirre, Anne L. Roggeveen, Dhruv Grewal, and Martin Wetzels, "The Personalization-Privacy Paradox: Implications for New Media," *Journal of Consumer Marketing* 33, no. 2 (21 March, 2016): 103, https://doi.org/10.1108/JCM-06-2015-1458.

11 Donell Holloway and Lelia Green, "The Internet of Toys," *Communication Research and Practice* 2, no. 4 (October, 2016): 506–19, https://doi.org/10.1080/22041451.2016.1266124; Donell Holloway, "Surveillance Capitalism and Children's Data: The Internet of Toys and Things for Children," *Media International Australia* 170, no. 1 (February, 2019): 27–36, https://doi.org/10.1177/1329878X19828205.

12 Andra Siibak and Giovanna Mascheroni, "Children's Data and Privacy in the Digital Age," *CO:RE Short Report Series on Key Topics* (2021), https://doi.org/10.21241/SSOAR.76251; Victoria Nash, "The Rise of the Algorithmic Child: Protecting Children in Smart Homes," in *Families and New Media*, ed. N. Dethloff, K. Kaesling, and L. Specht-Riemenschneider (Springer Fachmedien Wiesbaden, 2023): 215–25,. https://doi.org/10.1007/978-3-658-39664-0_10.

13 Nash, "Rise of the Algorithmic Child", 219.

14 Peter Fernandez, "Wearable Technology: Beyond Augmented Reality," *Library Hi Tech News* 31, no. 9 (1 January, 2014), https://doi.org/10.1108/LHTN-09-2014-0082.

15 Deborah Lupton, *The quantified self* (Polity Press, 2016).

16 Hadi Habibzadeh, Karthik Dinesh, Omid Rajabi Shishvan, Andrew Boggio-Dandry, Gaurav Sharma, and Tolga Soyata, "A Survey of Healthcare Internet of Things (HIoT): A Clinical Perspective," *IEEE Internet of Things Journal* 7, no. 1 (January, 2020): 53–71, https://doi.org/10.1109/JIOT.2019.2946359.

sonal Assistants) that identified cultural differences in attitudes towards privacy. Based on focus groups conducted in the United States and The Netherlands, the authors found that while Americans often showed resignation toward surveillance technologies, frequently stating they "have nothing to hide", and valued convenience and other benefits over privacy concerns, Dutch participants displayed greater wariness towards data collection, particularly considering the large (American) platforms to which assistant smart speakers are associated (Google, Amazon, and Apple).[17]

In another study about smart speaker assistants, Brause and Blank ascertained that research on these devices usually focuses on three aspects of privacy: privacy concerns, privacy work, and privacy rationales. In their article, based on interviews with users, they identify several forms of privacy work, distinguishing between "secrecy techniques", such as avoiding the use of speakers for some tasks, placing speakers in carefully chosen locations at home, or limiting information flows to the manufacture companies and to house guests, and "demand management", such as interrupting conversations until the device deactivates. Regarding privacy rationales, the authors ascertain that they are connected to the normative framework and context-relative purposes (privacy violation as an infringement of informational norms), but also to "information consequences, privacy skills and awareness, and choice".[18]

Inspired by the privacy triad – privacy concerns, privacy rationales and privacy work – identified by Brause and Blank, this article extends the analysis to all kinds of IoT devices used at home, including "wearables" since they are based on the same kind of technology (internet connection) but raise heightened concerns.[19] We use Brause and Blank's definition of privacy concerns as the worries that users express, of privacy rationales as the perceptions and expectations regarding privacy norms, and of privacy work as the behavioural and technological measures taken to protect privacy and control access to private information. In combination, these concepts allow the examination of the interplay between narratives and practices around privacy. We focus on the narratives about the domestic practices of a group of families residing in Portugal, even though the findings are not necessarily case/nation specific. We try to advance knowledge on this topic by ascertaining whether concerns, rationales, and practices vary according to the type of the device and to the characteristics of the user. Furthermore, we contrast users' perceptions and practices with the visions from experts and stakeholders regarding privacy risks of domestic IoT.

17 Jason Pridmore, Michael Zimmer, Jessica Vitak, Anouk Mols, Daniel Trottier, Priya C. Kumar, and Yuting Liao, "Intelligent Personal Assistants and the Intercultural Negotiations of Dataveillance in Platformed Households," *Surveillance & Society* 17, no. 1/2 (31 March, 2019): 125–31, https://doi.org/10.24908/ss.v17i1/2.12936.

18 Saba Rebecca Brause and Grant Blank, "'There Are Some Things That I Would Never Ask Alexa' – Privacy Work, Contextual Integrity, and Smart Speaker Assistants," *Information, Communication & Society*, 17 (April, 2023): 12, https://doi.org/10.1080/1369118X.2023.2193241.

19 Brause and Blank, "There are Some Things", 2.

Methodology

The project underlying this article relied on a multi-method research approach, combining document analysis (for instance, of advertisement of IoT products, reports, and media articles), stakeholder interviews, as well as interviews with households that have IoT devices in their home. We considered that performing interviews (in lieu of a questionnaire survey, for instance) would allow us to better access the representations people have of IoT, as well as narratives about their practices, given the impossibility of observing them first-hand for extended periods.[20]

We assembled the sample of households (21, see Table 1) to be interviewed using various methods: personal contacts of the researchers (four interviews), snowballing (seven interviews), and the use of a market research company (ten interviews). The interviews took place in Portugal, mostly in the Lisbon region, between January and July 2023, in most cases (16), at the home of the interviewees (the other five were done online). The interviews were conducted in Portuguese, the native language of interviewers and interviewees. 16 interviews were conducted with only one adult member of the household (seven men, nine women) and five interviews with both members of the couple, according to the availability of the interviewees. However, the interview focused on household practices and questions were asked about different uses by different members of the household. No children were interviewed, although some were present during the interviews. Three interviewees lived alone, one with her parents, 15 with a partner, and 15 with co-residing children. All but three interviewees had higher education degrees. Five interviewees worked as Information Technology professionals. Although the sample seems skewed, it reflects the characteristics of IoT users found in large-scale surveys.[21] The households are identified in the citations in this paper by a number (e.g. #1) and basic sociodemographic traits: sex of the interviewee (M, F or M/F in the case of couples, highlighting the sex of the speaker in bold), age group (e.g., 30s), and occupation (e.g., service worker). Names used within the citations are aliases. The citations were translated into English by the authors.

20 Aimee Ambrose, Barry Goodchild, and Fin O'Flaherty, "Understanding the user in low energy housing: A comparison of positivist and phenomenological approaches," *Energy research & social science* 34 (2017): 163–171.

21 Ana Delicado, *Use of IOT devices in Portugal: Statistical Data*, 2022: 8–14. Zenodo. https://doi.org/10.5281/zenodo.14593555

Table 1: Sociodemographic traits of interviewees

Code	Gender	Age group	Education	Occupation (ISCO 08)	Household composition
1	M/F	50s/40s	Secondary education	Manager/Clerical Support Worker	Couple living with a teenage son
2	M	40s	Secondary education	IT Professional	Couple living with two children, a son and a daughter under 12 years old
3	F	40s	Higher education	Sports and Fitness Worker	Couple living with four daughters under 10 years old.
4	M	40s	Higher education	IT Professional	Single person household
5	F	40s	Higher education	Social Professional	Couple living with two sons under 10 years old
6	M	50s	Higher education	IT Professional	Single person household
7	F	20s	Higher education	Postgraduate Student	Woman living with her parents
8	F	20s	Higher education	Customer Services Clerk	Couple without children
9	F	30s	Higher education	Science and Engineering Professional	Couple living with a baby daughter
10	M	20s	Higher education	Creative and Performing Artist	Single person household
11	F	40s	Higher education	Sales and Purchasing Agent	Couple living with two sons under 10 years old
12	M	50s	Higher education	Administrative and Commercial Manager	Couple living with a teenage daughter
13	F	50s	Higher education	Financial Associate Professionals	Woman living with an adult daughter
14	M/F	30s	Higher education	IT Professional/ Administration Professional	Couple living with a new-born son

Code	Gender	Age group	Education	Occupation (ISCO 08)	Household composition
15	F	50s	Higher education	Unemployed	Couple living with two sons, one a teenager, another in his 20s
16	M/F	50s/40s	Secondary education	Clerical Support Workers	Couple living with two teenage daughters
17	M	30s	Higher education	IT Professional	Couple without children
18	F	50s	Higher education	Clerical Support Worker	Woman living with her adult children, a son and a daughter
19	M	40s	Higher education	Teaching Professional	Couple living with a son under 10 years old and two toddler daughters
20	M/F	30s/40s	Higher education	Travel Attendant/ Business and Administration Professional	Couple living with two toddler daughters
21	M/F	30s	Higher education	Other Health Professional/ Travel Attendant	Couple living with two toddlers, a son and a daughter

The interview protocol was designed based on the literature review and theoretical framework but also on the results of the documental and media analyses. The questions focused on 1) the process of buying IoT devices; 2) practices of use and routines (eliciting differences by household member); 3) data management; and 4) benefits and risks.

We performed 16 interviews with stakeholders: four with representatives from companies that develop IoT products (identified in citations as C#number), four with representatives from public bodies (PB#number), four with civil society organisations (CS#number), and four with academics that teach and research about IoT (A#number).

All interviews were recorded and transcribed in full and verbatim, including interjections, hesitations (marked with ellipses), repetitions, subject-verb agreement mistakes, and so on. The transcripts were subjected to content analysis with the assistance of specialized software (MaxQda 22).

The initial codebook for household interviews was built based on the literature review and theoretical framework (Appendix 1). The first order codes comprised the type of IoT device, buying process, practices of use, motivations for use, family roles, benefits, and risks. New codes were added to the codebook throughout the coding process, as new sub-topics, such as visions of the future

and the professional experience of users, emerged from the data, following an inductive approach. For this article, we focused on codes related to privacy, management of personal data, risks, and strategies to deal with risks. The codebook for stakeholder interviews has a few additional codes, addressing the concept of IoT, IoT ecosystem, training of IT professionals, and regulation of IoT.

Findings

Privacy concerns

The first step in understanding the users' perceptions and practices of privacy in relation to IoT is to determine whether users are at all aware of the privacy issues associated with IoT devices. Most interviewees did not show awareness or concern about the data that IoT devices collect about themselves and their homes, with some of them explicitly stating this is not something they actively think about:

> I don't have this paranoia about being watched by the camera, computer cameras... for example, this one is open... now that I'm talking about it, is this one open or closed...? I don't have much... data insecurity […] when I fill things in, I don't give any serious data. [#15, F, 50s, unemployed]

> I don't think much about these things. And Cesar [husband], even though he's into technology, doesn't think about it either. […] the truth is that the person is having this conversation here and in a while they open Instagram and there are suggestions there, right? But no, I don't worry. [#14, **F**/M, 30s, administration professional]

Another interviewee is aware of the impossibility of having control over his data, but has ceased to worry about it, putting it down to maturity and seeing things in perspective:

> With regard to, with regard to data, let's see, I'm not worried about it, because, I mean, I'd have more to worry about […] my data must be in Russia, it must be in China, it must be in the NSA [National Security Agency, USA], they must all be there and I must be being investigated to no end, but it doesn't worry me, it doesn't worry me at all [...] I used to be very concerned about security. As when you grow older and gain more maturity, you reach a point where you put things into perspective, and you want things to work well more than you want to know if your data is being searched. [#4, M, 40s, IT professional]

On a similar note, many interviewees also believe that they are relatively safe from harmful uses of their data since they see themselves as unimportant individuals, without any valuable information:

> About data, I'm not worried about it, because… I, I'm a mere unknown, that's not what's going to affect me. No, it doesn't affect me. So no, I'm not worried about data. [#4, M, 40s, IT professional]

> José: In general, I don't worry too much about it [improper data collection], because I don't have much to hide either […] I can understand those who worry about it, and I can understand why, but it doesn't bother me that much.

> Paula: We're not such important people. [#20, M/F, 30s/40s, travel attendant/ business and administration professional]

Conversely, other users stated that they are aware of the privacy issues raised by IoT, with some specifically referring to the fact that IoT devices collect data about themselves and their homes:

> Bimby [cooking device], for example, even knows what we eat, depending on what we cook, what we eat […] they all collect data on our usage. When we use it most, the type of use we make. For example, the Bimby tells us what types of recipes it makes; it stores lists of the last recipes made, we can also access it remotely on the app or the website. [#19, M, 40s, teaching professional]

> The vacuum cleaner collects a lot of information, it knows the layout of my whole house, it knows the internet credentials. Obviously, we always have to have everything connected to the same network [#9, F, 30s, science and engineering professional].

Additionally, some users showed a deeper concern with how the devices send back information to manufacturers and the fact that devices can be hacked, potentially allowing unauthorized people to gain access to their data or even manipulate the functioning of devices (cyber-physical attacks):

> I'm interested in aligning everything [under a single control software] […] from a security point of view if these applications have security flaws or have backdoors deliberately created by the brands themselves, they end up allowing third parties to enter, directly or indirectly, inside our home network. […] Having a webcam or a webcam feed exposed on the internet is something that is dangerous, potentially dangerous. […] we access our banks through our home network, don't we? And so if someone, through a system, whether it's a camera, the lights, whatever if they're here actively listening to our network, they can get that data, can't they? At the end of the day, it would even be able to reach our health, understand routines, understand everything and anything. So, for me, that's the biggest point, the question of security. [#17, M, 40s, IT professional]

In short, IoT users show different levels of concern regarding their privacy. Whereas some dismiss these worries, others do fret about the safety of their data and the potential for misuse. In the next section we will delve into how these concerns are justified by the users.

Privacy rationales

Data also yielded relevant results regarding IoT users' perceptions and expectations of privacy norms. As seen above, one of the most touted advantages of IoT devices is their capacity to adapt to user preferences, based on the data collected on their practices.

Interviewees have different understandings regarding the dilemma between personalization and privacy. For example, in the case of cooking devices, such as kitchen robots or airfryers, that collect information about users' culinary and dietary habits, one interviewee sees only the advantages of receiving personalized recommendations and recipes to vary the family's diet. He hence downplays the relevance of the data being collected as unrelated to their habits but rather focused on machine operation:

> In the case of the Bimby [kitchen robot], we also use all the features, yes. When we first bought the Bimby, the Cookidoo [recipe] plan was a gift. And we began to realize the advantage it had in our daily lives, even to experiment and diversify our diet a little, […] sometimes in our free time we can be looking at what we're going to have for the next meals, […] and then we send it to the Bimby. […] maybe the data they collect is the frequency with which we put recipes in there, how many times we make them or use certain functions, how long the motor runs at full speed... but it's not data that compromises us as individuals, is it? It ends up being more data on how the thing is used. [#17, M, 40s, IT professional]

Conversely, another interviewee felt that the level of personalization offered by a cooking appliance is unnecessary and feared that the data being collected about their food preferences could be sold to retail companies for advertisement purposes:

> The airfryer, it only collects data through its app in the sense that it has presets for certain types of food, such as tofu, chicken legs, nuggets, whatever, and if [...] I'm frying tofu, it will then collect that data to give me more personalized recipes. But that's only if I use the food's default settings, in other words, if I just set the app to cook for 20 minutes at 180°, it doesn't know what I'm doing in there and it can't personalize my searches, my recipes. [...] an app doesn't need to know what I'm eating every day. [...] And in any case […] I don't know to what extent this data can't also be bought or sold to supermarkets. [#7, F, 20s, post-graduate student]

In the case of smart speaker assistants, these perceptions about the privacy-personalization trade-off are usually heightened, particularly if it is always on listen-feature:

> It's actually listening, isn't it? Constantly! Because the device is always waiting to hear a command. We've talked about that too, but then it's that old discussion of what we have to weigh up in terms of what we get out of it and what we lose in terms of privacy, isn't it? [#8, F, 20s, customer services clerk]

IoT users are also often torn between the health benefits of smartwatches, fitness bracelets, and other wearable devices and the fear that their health data might someday be used by insurance companies to increase premiums or even to deny services:

> The part about sleep data doesn't worry me. I don't draw any great conclusions from it, at least not mine. Okay, sports data is what it is, that's it. It records the places I run, the routes I take, etc. But there must be a trade-off, right? If you want to take advantage of it and get some value out of it, you also must realize that it's going to be stored somewhere, but in that case, I think it's the least bad thing. [#17, M, 40s, IT professional]

> The one that's the most intrusive, strangely enough, is the [fitness] bracelet. […] I mean, let's imagine that in 20 years' time I want to take out health insurance and these companies that are taking out health insurance have, by chance, access to the data from my bracelet, and they're already going to give me a different type of health insurance based on my data than the ones I might eventually tell them. […] I feel very out in the open with it [bracelet]. I feel very out there, I feel that anyone can pick up my mobile phone and see that I had an anxiety attack on X day, at X time, because they can see my heart or see that I'm breathing heavily. So, it's data that makes me very vulnerable, deep down. [#7, F, 20s, postgraduate student]

Interviewees are particularly worried that companies will infringe on their privacy for commercial purposes, that their data will be used both for profiling customers to sell more things and for providing/denying services:

> There is some relative risk. The main use of this is not that someone wanted to spy on something, but to gather aggregated information to create consumer profiles and classify people according to purchasing power bands, isn't it? If you have four robots in your house, it's because you have more money than sense and they might try to sell you other things. So I don't think it's an individualized issue, it's clear that everything is exposed to the internet, connected to the network, and can be used [...] so there are two risks: legal and illegal. There's the illegal risk of someone hacking this and publishing the data or sel-

> ling it somewhere, which is a marginal risk. It can happen, but it isn't something I'm too worried about. And there's the legal risk, that is, of them using this data to sell to insurance companies and other things and to create profiles of this and that [#2, M, 40s, IT professional]

One of the interviewees went further in expressing annoyance that usefulness would come at the cost of open-ended choice, as users will be more typified and manipulated:

> The biggest risk is that this is sold as making our lives easier or better, […] It's so good, so useful [...] what's the catch for it being so good for me, for whoever is doing it? I don't think it's clear. In the future I'm afraid that this isn't going to make my life any easier, it's going to make my life narrower because we're going to have predictive models of people's behaviour, our lives are going to be more catalogued, not as individuals, (…) we as people are going to be more standardized or more typified, more of a business facilitator, as an abstract entity, than a human being. I don't think this has a humanist vision at all. [...] I'm a little annoyed by the loss of privacy [#16, M/**F**, **40s**50s, clerical support worker]

This issue was particularly highlighted in the case of smart speaker assistants, which, like smartphones, users believe are "always listening" and using the information for advertisement purposes:

> It's always listening to us, isn't it?... The data, the conversations, everything! We never know to what extent they're listening to us. We know, because if I say Nike trainers, in a while, here on my phone, when I go to Instagram or something, I'm already being advertised with Nike trainers, without typing it. So I guess it already happens [#19, M, 40s, teaching professional]

In other cases, users consider that illegal access to their data, particularly images from inside the home and of children, or potential access to their banking information, poses a higher risk:

> It bothers me that there are images from inside my house, of my daughter, that could be, I don't know, intercepted in some way through the use of the internet. This bothers me. […] I think it's a very big risk for us to have images, in this case of our daughter, exposed to possible intruders. Any kind of hacking could take place and they could intercept the footage of our daughter sleeping or playing in her room, or whatever. That's completely out of the question for me, whether it's that or something else. […] I think these devices have a lot of risks, namely... I think it [smartwatch] can hear me whenever it wants, and, I don't know, I make payments with this, how can this not be dangerous? [#9, F, 30s, science and engineering professional]

Some interviewees also highlighted that even the most seemingly innocuous device, like an IoT meteorological station or a light switch, can give insights into household habits:

> Something as insignificant as that [IoT meteorological station] lets you know if the person is at home or not, and the same goes for the switches. By having access to this data, you can tell if the person is there or not, or when they were there, or their routines. [#20, **M**/F, 30s/**40s**, travel attendant]

It was also acknowledged that IoT devices can infringe on the privacy of household members by allowing, for example, spouses to monitor each other or parents to monitor their children:

> When I come to this application and suddenly see that Paulo [husband] is also using Alexa, […] I don't know what that information is for, it feels a bit intrusive? Because just as I can see that Paulo is using it, Paulo also knows that Carolina [herself] is using it, right? It's nothing to take offence at. But... It's data that I wouldn't share if I could avoid it. When we sign those consents, we're never aware of the limits, of whether we're sharing information or not [#11, F, 40s, sales and purchasing agent].

The awareness that their data is being collected and potentially shared leads some interviewees to express feelings of powerlessness and resignation towards surveillance by companies and governments:

> The texts are big, aren't they, people usually accept them almost straight away, don't they? […] we end up accepting a lot of things in those big texts. When we update any application, there's the giant text, updating the data policy and that... we don't really look into it, no. […] What worries us is always the data management that's done, that's the biggest concern, it's always the data management, that they monitor everything: when we're at home, when we're not, when we use the most, what we use the most... they have access to all that kind of information, don't they? [#19, M, 40s, teaching professional]

Interviewees also acknowledged that giving away access to private data is largely a precondition for using these devices, a requirement set by manufacturers and to which consumers have no other option but to agree:

> I'm not afraid of the smartwatch. The worst it can do is collect my biometric data and decide to sell it all to the US state. So, the worst is already happening, I'm not afraid of anything worse than that! […] these biometric data are being collected whether we like it or not. […] And, well, privacy policies are that 'either you accept or you don't have access' and they'll keep collecting the data anyway. Honestly, my

> policy is 'data are being collected anyway, so if they want to access the data, they can anyway' [#10, M, 20s, creative and performing artist]

Some acknowledge that they already overshare on social media or are being tracked in whatever they do online, so they are aware that they are seen as "products" by digital companies and using IoT devices does not seem to make much difference in the grand scheme of things:

> That was a conversation we had, like 'is it worth it to jeopardize our privacy?'. And then we came to the conclusion that it's like 'so, but what can Google find out about our private lives that it doesn't already know, that we don't already share when we search on Google?' […] I think we're already from a generation that's used to exposing ourselves to the internet in some way, we realize that we sacrifice some privacy. Truth be told, they collect a lot [of data] and we go from being customers to products. So, it's that thing, it doesn't impact our lives directly, it's not tangible, is it? It's a bit abstract. So, it's a little easier to accept than if it was something more obvious, let's put it that way. Okay, it does cause me some discomfort from time to time, but it's something you easily forget is happening, so I think it's expendable. [#8, F, 20s, customer services clerk]

In short, privacy rationales of IoT users tend to focus on how they can be affected by the infringement of privacy norms by companies and what they imagine their data can be used for. Two other kinds of reasoning also stand out: the dilemma between the benefits of customization and the risks of privacy infringement and the sentiment of privacy resignation, when users feel powerless to uphold their privacy.

Privacy work

Interviewees displayed a wide range of practices to control access to private information. First and foremost, the non-adoption of IoT devices. For instance, even though most are parents, none of the children of the interviewees own internet-connected toys or wearable devices. In other cases, users declare that they have deliberately not bought specific devices because they thought the trade-off was not worth it:

> I'm only going to invest in something that really solves the problem. Now getting a video intercom connected to the net. What's the point? Maybe in a context where my house needed a lot of security, if it was a company or something. Each thing in its own way. There are things in everyday life, personal things like this, sometimes I feel like throwing it [IoT] away. [#6, M, 50s, IT professional]

Other informants explain that they gather information about privacy and safety before acquiring any IoT products:

> I've always been very aware of what each of these types of technologies entails. And for me, caution and planning have always been very important, that is to say, I may even want to invest in something, but when I make an investment, I study a lot before I start using anything. To avoid malpractice, misuse, that might turn against us… to understand the limitations [#17, M, 40s, IT professional]

Some interviewees report rejecting the use of purchased or gifted IoT devices. This occurs more often in the case of web cameras since users consider them to carry higher risks, particularly in households with children:

> I don't have the camera switched on, I've never switched it on, and I'm not going to switch it on. It's going to be thrown out. The camera is a problem for me, so it even invalidates its use. […] even if I wanted to put that camera in the house for video surveillance or whatever, I wouldn't do it because that would be exposing myself [#9, F, 30s, science and engineering professional]

Also, in the case of smart speaker assistants some informants reject using them due to concerns about breach of privacy:

> If I get sick and have a broken leg and I'm here alone at home, maybe I'd find it more useful to be able to tell Siri… […]. Now, I don't think so. With the issues that have arisen of a certain... lack of privacy or breach of privacy and, in fact, not knowing how our data is being used no matter how much they try to reassure us that there is... we haven't seen much need. Our daughters, of course, think it's great to talk, as well as having voice commands, but I mean, they're from another generation, aren't they? […] I don't feel any need to use it. […] There's nothing to guarantee that someone won't intrude. As long as we don't have that guarantee, it's the same as leaving the door open at home. [#16, F, 50s, clerical support worker]

Other users, in most cases the male member of the couple, conduct privacy work by deploying basic IT safety strategies such as choosing specific devices considered safer, changing router passwords, using firewalls, or setting up VPN (Virtual Private Networks):

> The issue of data is not to be overlooked. When we opted for the radio frequency camera, we also considered this issue, which was the fact that we knew it wasn't accessible to anyone outside, whereas an internet connection can always be used by someone who knows about it and isn't supposed to be used by anyone else. [#21, M, 30s, other health professional]

> My network is already segmented and with open source routers... […] Shelly [smart] sockets only work on the local network so that I always

> have an entry point, which is my VPN, and by accessing the VPN from the street, then I can have access to things in the house, but the things in the house aren't public or directly exposed to the internet. [#17, M, 40s, IT professional]

More tech-savvy users (often with an IT-related occupation, and again male) can contravene the devices' default settings of sending out data to the parent company by installing different software to control them and storing data in private servers:

> For security reasons and because I want to control all these devices, my goal will be to join them inside a pool that I control, using Home Assistant here. [#17, M, 40s, IT professional]

Some users choose not to use or to turn off certain features of IoT devices that they consider having higher risks. For example, the recording function in web cameras or the robot vacuum cleaner making a plan of the house:

> As I haven't mapped the house, it [robot vacuum cleaner] doesn't collect it [data about the house layout]. […] I didn't map it because... firstly, because there you go, I haven't had time to commit to that subject yet. Because I don't want to use this function without knowing what it's going to entail. [#17, M, 40s, IT professional]

Another example is accessing personal data and conversations in smart speaker assistants:

> The thing that shocks me the most is having the active voice thing [in smart speaker assistants]. I have deactivated it, so I don't have those commands to always be listening […]. So I press the button, and only when I press the button does it jump up and allow me to give it a command. […] I don't need to expose any more of my data and information [#17, M, 40s, IT professional]

Some users carefully choose the placement of IoT devices in their homes to safeguard their privacy. They avoid installing devices such as smart speaker assistants or cameras in the most private spaces of the house, like bedrooms and bathrooms:

> We had some concerns because it [the camera] was also filming us, it was always filming us. We were careful not to leave it in the bedroom when we were there. Even when it was with the girls, we didn't leave it when they weren't there. We take care of that. It's in places in the house other than bedrooms, bathrooms... Usually now it's in the living room. [#19, M, 40s, teaching professional]

Others impose restrictions on the operation of IoT devices, limiting the time of their use. For example, they may only turn on web cameras when the household members are away from home:

> We don't use [the Internet-connected camera] regularly. [...] We use it more on holiday, we leave it on, and we use it to monitor the house and as an alarm, because it also detects movement and warns us when there's movement. We don't use it day-to-day, we don't have it switched on day-to-day now. [#19, M, 40s, teaching professional]

Or they use wearable devices solely for specific functions, such as collecting health data during exercise:

> Then I realized that it [fitness bracelet] probably collects a lot about me, and I don't know what it's going to be used for, I have no idea. So I've ended up reducing my use of the bracelet a lot. I use it more when I'm exercising because, after all, that was the whole point of buying it in the first place. I don't use it when I'm sleeping. When I'm at home, I don't use it. And I use it very little too, less and less when I'm out and about. [#7, F, 20s, postgraduate student]

In short, IoT users develop different types of strategies to protect their privacy and safeguard their data. Although some cease to use the devices altogether, others, particularly the more tech-savvy users, impose restrictions on their operation, in order to reap the benefits of IoT without endangering their privacy.

What stakeholders say about privacy issues of IoT

Although some of the IoT users in our sample were fairly knowledgeable and proficient on privacy risks, we sought to contrast their perceptions and practices with the opinions of experts in the field of IoT: representatives from companies that develop IoT products (C), representatives from public bodies (PB), representatives from civil society organisations (CS), and academics who teach and research about AI (A).

All stakeholders mentioned knowing of international privacy infringement or private data breaches through IoT objects but had no evidence that there had been any serious cases in Portugal. However, most, particularly from government and civil society organizations, were fairly concerned with the lack of consumers' general awareness regarding privacy issues:

> We have a fundamental problem: there is currently no legal obligation for anyone who produces this type of equipment to take safety precautions. […] The second problem is that safety is not yet a common concern for all of us. [PB#4]

> The devices are sometimes very complex. As I was saying, they have a lot of settings, a lot of functions, and sometimes it's difficult for people to realize what [information] they're giving, even if they're giving more. [CS#2]

Additionally, they pointed out the absence of preventive measures (privacy work):

> People also don't know how to set up the right cyber security measures, weak passwords or outdated systems or... it's not... and they're vulnerable to attacks, and there could be an increased risk to users' privacy and security...People don't realize what cyber hygiene is, do they? [CS#2]

> Nowadays, with all the technological innovation […] the average consumer is no longer able to protect himself […] technological development is evolving, it's evolving at such an overwhelming pace that even the most informed consumer can't keep up, no matter how much they want to, no matter how hard they try. […] And this in fact creates […] digital vulnerability, in other words, perhaps the need to think about protecting consumers who until now didn't need that same protection. [CS#4]

They advocate for more education of consumers:

> I think we have to have a cautious, educated society on this issue of cybersecurity. […] Maybe it's time to introduce computer education at school, just as sex education was introduced in our time. [PB#4]

> On the part of the user, there has to be, let's say, at least a minimum knowledge of how this equipment or integrated technology is going to work and what the risks are and how, let's say, to protect one's interests involving these risks. This is a challenge for society. [CS#4]

But also, for more regulation:

> The legislation should impose a certain set of requirements, so it should be the states, things like GDPR [General Data Protection Regulation], etc., at this level of requirements and there shouldn't be… products shouldn't be allowed on the market that don't have some kind of basic certification or, in short, fulfil minimum safety requirements from that perspective, so, in other words, it's the states that have to impose, or the European Union, eventually. And then there has to be some sort of ASAE [food safety authority] for these types of products. But there are certifications that you look at... every product has seals that they certify for a number of things, for example, washing machines, etc., have energy certificates and things like that. There could be the same type of certification from a safety perspective. [A#1]

Although some also see regulation as an obstacle to technological progress:

> On the one hand, the lack of legislation is positive in the sense that it allows technological progress and excessive legislation hinders technological progress. On the other hand, it obviously poses threats, it poses security threats, it poses confidentiality threats, it poses data protection threats, it poses all sorts of threats, but everyone knows that our data protection agency is one of the major factors holding back our progress in a number of areas, right? The truth is that this balance is always difficult. [CS#1]

Company representatives, though acknowledging privacy issues with IoT, downplay the risks and underline the security work they perform:

> Risks, there are always risks. As I was saying, data is a good thing and a bad thing. That's why basically all of our projects, I'm telling you, all of our projects, especially with big companies, we spend six months going through security things, all the encryptions, we have to make sure that we can be suppliers or not, that we follow all the possible and imaginary guidelines, so that we can never lose a piece of data that leaves here, but there is always this risk. […] In my opinion, at least our data, that we collect, ends up being data that is of no interest to anyone, it's not personal data, it's data that, for the manufacturer or the person selling it, is very important data. [C#2]

In short, stakeholders have the perception that most IoT users are unaware of the privacy risks that affect them, disregarding the fact that a fair proportion of users are quite technically skilled. Therefore, some believe that more regulation is needed, but also call for a better education of consumers.

Discussion and conclusions

In line with previous research, but also with stakeholders' statements, the majority of IoT users we interviewed (but not all) did not show particular privacy concerns about the data that devices collect about them, their practices, routines, or homes.[22] This dominant position often stemmed from lack of knowledge of how these devices operate. Still, in some cases, it translated into "privacy resignation" or "digital resignation" (feeling powerlessness against big digital companies), often accompanied by the assertion of having "nothing to hide" or being persons of "no importance".[23]

22 Coughlan et al., "Exploring Acceptance".

23 Pridmore et al., "Intelligent Personal Assistants"; Nora A. Draper and Joseph Turow, "The corporate cultivation of digital resignation," *New media & society* 21, no. 8 (2019): 1824–1839; Brause and Blank, "There Are Some Things".

We have also encountered privacy rationales that illustrate the privacy-personalization paradox described in the literature of the field.[24] Some users believe that giving away some of their privacy is worth it for the affordances it brings, such as convenience or access to their own data to modulate behaviour or become healthier. Also, the more useful the devices are for the user, the less concerned they are with privacy issues, as Coughlan et al. ascertained, since intensive use tends to "naturalize" and "normalize" the devices' features and presence at home.[25] Others, however, seem less keen to have their usage preferences and frequency of use collected and "fitted into a mould". These users are particularly concerned with the commercial utilization of their data and how it can negatively impact them in the future.[26]

Multiple studies use the concept of "creepy" to describe the feelings of discomfort, anxiety, and suspicion that are aroused by IoT devices, particularly those that can facilitate surveillance of intimate spaces by external parties (including potentially criminal actors) or be used for target advertising, such as internet-connected cameras and smart speaker assistants.[27] Some of our interviewees also voiced their uneasiness at the ability of these devices to film their homes or listen to their conversations. They felt uncomfortable with the potential for devices to share this information with outsiders but also with other household members, allowing them to monitor their actions.[28]

Privacy rationales are then in some cases materialized into privacy work. Users develop different strategies to protect privacy. These strategies range from foregoing the acquisition or use of some IoT devices (non-adoption)[29] to performing what some authors call "digital housekeeping",[30] by changing passwords, protecting their home networks, changing the software of the devices, or disconnecting some features.[31]

In our study, different types of IoT devices raise different concerns. While cleaning and cooking devices are often seen as innocuous, "wearables", smart speakers, and cameras

24 Aguirre et al., "The Personalization-Privacy Paradox"; Coughlan et al., "Exploring acceptance"; Sabrina Karwatzki, Olga Dytynko, Manuel Trenz, and Daniel Veit, "Beyond the Personalization–Privacy Paradox: Privacy Valuation, Transparency Features, and Service Personalization." *Journal of Management Information Systems* 34, no. 2 (3 April, 2017): 369–400, https://doi.org/10.1080/07421222.2017.1334467.

25 Coughland et al. "Exploring Acceptance".

26 Chambers, C*ultural ideas of home.;* Habibzadeh et al., "Survey of Healthcare Internet of Things"; Michael S. Gal and Niva Elkin-Koren, "Algorithmic consumers," *Harvard Journal of Law & Technology* 30 (2016): 309.

27 Coughland et al. "Exploring Acceptance"; James Pierce, "Smart home security cameras and shifting lines of creepiness: A design-led inquiry," *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (2019): 1–14. ; Lupton, *The quantified self*; Daragh Byrne, Dan Lockton, Matthew Cruz, Christi Danner, Karen Escarcha, Katherine Giesa, Meijie Hu et al., *Spooky technology: A reflection on the invisible and otherworldly qualities in everyday technologies*, (Imaginaries Lab, 2021). Yolande Strengers and Jenny Kennedy, *The Smart Wife: Why Siri, Alexa, and Other Smart Home Devices Need a Feminist Reboot*, (MIT Press, 2020).

28 Coughlan et al, "Exploring Acceptance"; Lupton, "The Internet of Things".

29 Sovacool and Del Rio, "Smart Home Technologies".

30 Jenny Kennedy, Bjorn Nansen, Michael Arnold, Rowan Wilken, and Martin Gibbs, "Digital Housekeepers and Domestic Expertise in the Networked Home," *Convergence: The International Journal of Research into New Media Technologies* 21, no. 4 (November, 2015): 408–22, https://doi.org/10.1177/1354856515579848. Chambers, *Cultural ideas of home.*

31 Brause and Blank, "There Are Some Things".

are perceived as more dangerous, capable of spying on the users and sending out sensitive information.

User characteristics also seem to play a role in shaping attitudes towards privacy. On the one hand, privacy concerns and privacy work were more acute in the case of families with children, as the literature has already shown.[32] More technologically experienced users (in particular men, and often IT professionals) are more able to protect their privacy by contravening built-in features introduced by manufacturers, but, paradoxically, in some cases, they are also the least concerned and the more resigned to having their data harvested, aware that the value of data lies mostly in big numbers and not in individual cases. There is a gender difference at play here, with men often taking on the tasks of "digital housekeeping", setting up the appliances and putting in place safeguards. We did not find other sociodemographic traits that played a relevant role in differentiating practices or perceptions, mostly due to the homogeneity of the sample (and of IoT users in general, as shown by surveys) in terms of age or education.

Other contextual factors can also play a role. The interviews were carried out in Portugal, a European country often characterized as an "early adopter" of digital technology but where online privacy concerns tend to be high.[33] However, survey results show that IoT adoption in Portugal is very low in some kinds of devices (energy management), low in others (security solutions, home appliances, virtual assistants), and only very high in internet connected TV, in a pattern similar to Eastern European and some Southern European countries.[34] The same survey shows that rates of concern about privacy and protection of personal data as a reason not to use IoT in Portugal are more than double the European average.[35] However, these data do not tell us how privacy concerns, rationales, and work vary across Europe. For that, further research is needed.

As IoT devices become more common and their use is democratized to less technically proficient households, privacy risks will tend to increase. Like most domestic devices, IoT presence in the home will tend to become increasingly "invisible"[36] and therefore powerful and potentially challenging concerning privacy issues. As the stakeholders we interviewed advise, more stringent regulations and digital skills training are needed to address the increased datafication of everyday life in ways that protect the privacy and well-being of users.

In short, our study offers a rather comprehensive approach to the privacy issues raised by domestic IoT, by encompassing a wide range of devices (including appliances, smart speakers and "wearables") and establishing comparisons between them, by exploring

32 Holloway and Green, "The Internet of Toys"; Holloway, "Surveillance Capitalism and Children's Data"; Nash, "The Rise of the Algorithmic Child".

33 Emma Engström, Kimmo Eriksson, Marie Björnstjerna, and Pontus Strimling, "Global variations in online privacy concerns across 57 countries," *Computers in Human Behavior Reports* 9 (2023): 100268.

34 Delicado, *Use of IoT devices,* 6–7; Aurel Stefan Pica, Laura Marcu, Denisa Cornelia Ivan, and Nicoleta Angelescu, "Statistical analysis of Internet of Things (IoT) penetration in individual consumption in EU countries," *Journal of Science and Arts* 23, no. 2 (2023): 553-566, https://doi.org/10.46939/J.Sci.Arts-23.2-c03.

35 Delicado, *Use of IoT devices,* 16.

36 Daniel Miller, *Stuff* (Polity Press, 2009).

both perceptions and practices of privacy in the light of sociodemographic characteristics, and by confronting user narratives and expert opinions of privacy in an age of increased interconnectedness.

Disclosure Statement

The project on which this paper is based was funded by the Portuguese Foundation for Science and Technology (ref. EXPL/SOC-SOC/1375/2021, http://doi.org/10.54499/EXPL/SOC-SOC/1375/2021). The authors have no conflicting interests.

We are most grateful for the reviewers and editors' comments, which greatly improved the manuscript.

Bibliography

Aguirre, Elizabeth, Anne L. Roggeveen, Dhruv Grewal, and Martin Wetzels. "The Personalization-Privacy Paradox: Implications for New Media". *Journal of Consumer Marketing* 33, no. 2 (21 March 2016): 98–110. https://doi.org/10.1108/JCM-06-2015-1458.

Ambrose, Aimee, Barry Goodchild, and Fin O'Flaherty. "Understanding the user in low energy housing: A comparison of positivist and phenomenological approaches." *Energy research & social science* 34 (2017): 163–171.

Brause, Saba Rebecca, and Grant Blank. "'There Are Some Things That I Would Never Ask Alexa' – Privacy Work, Contextual Integrity, and Smart Speaker Assistants". *Information, Communication & Society*, 27, no. 1 (17 April 2023): 1–16. https://doi.org/10.1080/1369118X.2023.2193241.

Bridges, Lauren. "Infrastructural Obfuscation: Unpacking the Carceral Logics of the Ring Surveillant Assemblage". *Information, Communication & Society* 24, no. 6 (26 April 2021): 830–49. https://doi.org/10.1080/1369118X.2021.1909097.

Byrne, Daragh, Dan Lockton, Matthew Cruz, Christi Danner, Karen Escarcha, Katherine Giesa, Meijie Hu et al. *Spooky technology: A reflection on the invisible and otherworldly qualities in everyday technologies*. Imaginaries Lab, 2021.

Chambers, Deborah. *Cultural Ideals of Home: The Social Dynamics of Domestic Space*. Routledge, 2020.

Coughlan, Tim, Michael Brown, Richard Mortier, Robert J. Houghton, Murray Goulden, and Glyn Lawson. "Exploring Acceptance and Consequences of the Internet of Things in the Home". In *2012 IEEE International Conference on Green Computing and Communications*, 148–55. Besancon, France: IEEE, 2012. https://doi.org/10.1109/GreenCom.2012.32.

Delicado, Ana (2022). *Use of IOT devices in Portugal: Statistical Data*. Zenodo. https://doi.org/10.5281/zenodo.14593555.

Draper, Nora A., and Joseph Turow. "The corporate cultivation of digital resignation." *New media & society* 21, no. 8 (2019): 1824–39. https://doi.org/10.1177/1461444819833331.

Engström, Emma, Kimmo Eriksson, Marie Björnstjerna, and Pontus Strimling. "Global variations in online privacy concerns across 57 countries." *Computers in Human Behavior Reports* 9 (2023): 100268.

Fernandez, Peter. "Wearable Technology: Beyond Augmented Reality". *Library Hi Tech News* 31, no. 9 (1 January 2014). https://doi.org/10.1108/LHTN-09-2014-0082.

Habibzadeh, Hadi, Karthik Dinesh, Omid Rajabi Shishvan, Andrew Boggio-Dandry, Gaurav Sharma, and Tolga Soyata. "A Survey of Healthcare Internet of Things (HIoT): A Clinical Perspective". *IEEE Internet of Things Journal* 7, no. 1 (January 2020): 53–71. https://doi.org/10.1109/JIOT.2019.2946359.

Holloway, Donell, and Lelia Green. "The Internet of Toys". *Communication Research and Practice* 2, no. 4 (October 2016): 506–19. https://doi.org/10.1080/22041451.2016.1266124.

Holloway, Donell. "Surveillance Capitalism and Children's Data: The Internet of Toys and Things for Children". *Media International Australia* 170, no. 1 (February 2019): 27–36. https://doi.org/10.1177/1329878X19828205.

Karwatzki, Sabrina, Olga Dytynko, Manuel Trenz, and Daniel Veit. "Beyond the Personalization–Privacy Paradox: Privacy Valuation, Transparency Features, and Ser-

vice Personalization". *Journal of Management Information Systems* 34, no. 2 (3 April 2017): 369–400. https://doi.org/10.1080/07421222.2017.1334467.

Kennedy, Jenny, Bjorn Nansen, Michael Arnold, Rowan Wilken, and Martin Gibbs. "Digital Housekeepers and Domestic Expertise in the Networked Home". *Convergence: The International Journal of Research into New Media Technologies* 21, no. 4 (November 2015): 408–22. https://doi.org/10.1177/1354856515579848.

Lupton, Deborah. *The quantified self*. Oxford, Polity Press, 2016.

Lupton, Deborah. "The Internet of Things: Social Dimensions". *Sociology Compass* 14, no. 4 (April 2020). https://doi.org/10.1111/soc4.12770.

Miller, Daniel. *Stuff*. Cambridge, Polity Press, 2009.

Nash, Victoria. "The Rise of the Algorithmic Child: Protecting Children in Smart Homes". In *Families and New Media*, edited by Nina Dethloff, Katharina Kaesling, and Louisa Specht-Riemenschneider. Springer Fachmedien Wiesbaden, 2023. https://doi.org/10.1007/978-3-658-39664-0_10.

Pica, Aurel Stefan, Laura Marcu, Denisa Cornelia Ivan, and Nicoleta Angelescu. "Statistical Analysis of Internet Of Things (IoT) penetration in individual consumption in EU countries." *Journal of Science and Arts* 23, no. 2 (2023): 553–566. https://doi.org/10.46939/J.Sci.Arts-23.2-c03.

Pierce, James. "Smart home security cameras and shifting lines of creepiness: A design-led inquiry." In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*: 1–14. 2019. https://doi.org/10.1145/3290605.3300275.

Pridmore, Jason, Michael Zimmer, Jessica Vitak, Anouk Mols, Daniel Trottier, Priya C. Kumar, and Yuting Liao. "Intelligent Personal Assistants and the Intercultural Negotiations of Dataveillance in Platformed Households". *Surveillance & Society* 17, no. 1/2 (31 March 2019): 125–31. https://doi.org/10.24908/ss.v17i1/2.12936.

Rostami, Asreen, Minna Vigren, Shahid Raza, and Barry Brown. "Being Hacked: Understanding Victims' Experiences of {IoT} Hacking." In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*: 613–31. 2022.

Siibak, Andra, and Giovanna Mascheroni. "Children's Data and Privacy in the Digital Age". *CO:RE Short Report Series on Key Topics*, 2021. https://doi.org/10.21241/SSOAR.76251.

Sovacool, Benjamin K., and Dylan D. Furszyfer Del Rio. "Smart Home Technologies in Europe: A Critical Review of Concepts, Benefits, Risks and Policies". *Renewable and Sustainable Energy Reviews* 120 (March 2020): 109663. https://doi.org/10.1016/j.rser.2019.109663.

Strengers, Yolande, Jenny Kennedy, Paula Arcari, Larissa Nicholls, and Melissa Gregg. "Protection, Productivity and Pleasure in the Smart Home: Emerging Expectations and Gendered Insights from Australian Early Adopters". In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 1–13. Glasgow Scotland UK: ACM, 2019. https://doi.org/10.1145/3290605.3300875.

Strengers, Yolande, and Jenny Kennedy. *The Smart Wife: Why Siri, Alexa, and Other Smart Home Devices Need a Feminist Reboot*. MIT Press, 2020.

Van Dijck, José. "Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology." *Surveillance & society* 12, no. 2 (2014): 197–208. https://doi.org/10.24908/ss.v12i2.4776.

Zuboff, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* Public Affairs, 2019.

Appendices

Appendix 1: Household interviews coding book

IoT devices
- Audio systems
- Blinds
- Climate control
- Fitness
- Games consoles
- Geolocation tags
- Health devices
- Hoovers
- Kitchen appliances
- Lighting
- Smart home
- Smart watch
- Solar panels
- Surveillance cameras
- Televisions
- Toys
- Virtual assistant

Family roles
- Women
- Men
- Children
- Young people
- Elderly
- Pets
- Professional IT experience

Purchase process
- Information search
- Counselling
- Brands
- Decision not to buy

Motivations for use

Usage practices
- Usage problems

Data management
- Control apps
- Monitoring the data collected by devices

- Personal data management
- Benefits/advantages
- Risks
  - Identifying risks
  - Preventive strategies
  - Future intentions