Empowering Users' Privacy Rights in the Internet of Things

1st Nelson Vieira
Faculdade de Ciências Exatas e da Engenharia
Universidade da Madeira
Funchal, Portugal
2080511@student.uma.pt

***Abstract*—Internet of things (IoT) devices are everywhere, since the birth of ubiquous computing that human every day life is envisioned containg millions of devices that control every aspect of our lives. Today we have smart cars, smart houses, smart cities, wearables among other things that use various types of devices and various types of networks to communicate. These devices create new ways of collecting and process personal data from users and non-users. Most end users aren't even aware or have little control over the information that is being collected by these systems. I tried to take a holistic approach to this problem by first doing a systematic literature review (SLR), then by doing a survey to gather information about the general knowledge of Portugal's population in this very topic and then, partly based in the information I gathered, I propose a system that gives users information about the devices that are nearby and how to protect the data that they don't want to share with these devices, this system is capable of detecting what type of devices are nearby, what kind of data is collected by these devices, show privacy choices to the user when it is possible to do so and what can be done to protect unwanted data from being collected.**

***Index Terms*—privacy, Internet of Things, ubiquitous computing, privacy assistant**

I. Introduction

Privacy as we know it is a somewhat recent concept [1], [2], before the digital age there was barely any notion of privacy for most people. For many centuries most people used to reside in small communities where they were continuously involved in one another's lives. Even more recent is the idea that privacy is a crucial component of personal security, in contrast to the undeniable necessity of public security, including the requirement for guarded walls and closed doors. Long considered a luxury, privacy is still frequently viewed as nice-to-have rather than an absolute necessity, even if it is recognized as an human right, as present in article 12 of the Universal Declaration of Human Rights [3]: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.". Privacy can be defined [4], [5] as the right to govern how personal information and data is collected, stored, and used, it frequently involves handling sensitive information with care, and as such, organizations must be open and honest about the kind of data they plan to gather, why they need it, and where and with whom they plan to share it. Users should have the right to control their shared information.

This definition can cause some confusion with the idea of security [6] and although privacy and security are interconnected, security involves measures taken to safeguard data from risk, threat or danger, it frequently alludes to safety. It is the practice of keeping users' personal information and data safe and preventing unauthorized access to it. The main distinction between privacy and security is that the former deals with information that is specific to users and how they wish their data is to be used and managed, whilst the latter deals with its protection from potential dangers. Security can exist without privacy, but the opposite is not true. For managing sensitive and personal data, privacy and computer security are equally crucial.

Concerns about digital privacy have been growing [7]–[9] in the last few years, especially after the *Anonymous* decentralized hacker group cyber attacks, *WikiLeaks* and Snowden's leaked top secret documents from United State's National Security Agency, these concerns can be noted with the increase of written literature on the subject, when searching for terms like "privacy", "online privacy", "digital privacy" in Google Scholar, ACM Digital Libary or Science Direct it can be seen that, in the last 5 years, it returns about 5000000, 650000 and 80000 documents repectively, including articles, books, conference papers etc.

Most research has been done with focus on the web, while privacy in IoT systems has not been explored as much, although IoT systems have been growing each year, this creates new ways to interact, collect and analyze data. Because it already exists a healthy amount of research out there focusing on web privacy and not on IoT privacy, it is a much more fertile ground to explore the theme of privacy in the context of Internet of Things devices.

Iot as a term began being used in the 90's, a connection can be drawn with Mark Weiser's article on ubiquous computing [10] and the rise of devices of various sizes that comunicate with each other to do various (small) tasks, that make Weiser's idea a reality. These devices are used in various applications, beginning at home [11] with thermostats, fridges, microwaves, etc, in smart cars [12], in the education system [13], in our clothes and our watches [14] and even into outer space [15]. IoT resources may include IoT equipment (like smart home assistants and autonomous vehicles), IoT services (like video analytics services linked to smart cameras and indoor position

tracking systems), or IoT apps (like smart TV remote apps) that track and use information about us. The first use of the term *Internet of Things* was in 1999 by Kevin Ashton [16], executive director of the Auto-ID Center of MIT, during a presentation for Procter & Gamble. A definition for the Internet of Things can be: "An open and comprehensive network of intelligent objects that have the capacity to auto-organize, share information, data and resources, reacting and acting in face of situations and changes in the environment" [17].

IoT is one of the fastest growing tecnhologies [18], it is predicted that it will grow into the trillions of devices by 2030 [19], and with this expansion new security vulnerabilities and data gathering dangers appear, the lack of security in these devices makes them ideal targets for privacy violations and inadequate customer disclosure of device capabilities and data practices aggravates privacy and security issues.

Privacy in IoT systems in not seen as a crucial factor in development [20]. Specific standards for privacy options have been imposed by data privacy regulations including the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA), but even these regulations have been criticized [21]–[25].

A. Privacy paradox

We have to address the privacy paradox before going any further, there have been some studies done on this subject and it is an interesting one because of it's premise: even though privacy concerns have been increasing the bahaviour of people when online doesn't seems to have changed, people still continue to use same applications they have been using before and companies still take advantage of the informations the users have been providing on their platforms. According to [] this paradox can be seen from three diferrent perpectives, on one side people use whatever platforms they want to use even though they say they are worried about their online privacy making them hypocrites in the process, another way to look at it is that people use the platforms because they get something in return and so they are ok losing some privacy because the convenience is too great a factor, and the third perspective is this bla bla bla. This paradox has been proven to be false in a number of other studies but some still take it as fact propagating this false believe that people just don't care.

II. Literature review

In this section I conduct a systematic literature review of the most relevant papers discussing methodologies and tecnhiques for the protection of users' privacy data with special focus on IoT systems. For this SLR I considered focusing only on papers from the last 12 years, from 2010 until 2022, since papers before then become out of date with the evolution of technology. I reviewed 100 papers published in top computer science, security, privacy and software engeneering outlets.

I followed Keshav's three-pass aproach [26] when choosing which papers to read fully and which ones to ignore, first I would read the title, abstract, introduction and conclusion and briefly skim the rest of the paper and then decide if it was worth reading any further, the focal point in this phase was aswering the following question: does the paper present a new methodology or interesting angle to tackle users' privacy concerns? Only then the document would be read in it's entirety while ignoring any tables, figures, images or graphs. If the paper failed to present any interesting idea, approach, or technique it would be discarded, but if not, it would be read carefully from the beginning again in order to fully understand what it presents.

Some papers propose better laws [] as a way to force service providers to give more choices to users, but as stated in the paper this aproach will be met with opposition from most companies because most of them have a stake in keeping things the way they are.

For the literature review interactive theatre experience [27]

According to this systemtic literature review [28] most papers that have written about privacy in iot systems focus in one or two devices, ignore the sensitivity of collected information, don't emphasize real-time notification to users and.

A. Related work

There exists a number of privacy assistants in the market. Privacy assistants have the objective of giving the user flexibility in choosing the prefered privacy options in available applications, most are used in smartphones, very few are made for devices in the internet of things.

The Carnegie Mellon University CyLab, which is the university's security and privacy research institute, started developing in 2019 an IoT Infrastructure that intended to be free of privacy leaks and software covered by their Secure and Private IoT Initiative 2019, this project would fall under their main research theme of Trust. In this project they started the design of a Personalized Privacy Assistant (PPA) [29], this would involve the use of semi-structured interviews with 17 participants to examine user perceptions of three hypothetical PPA implementations, each of which is potentially more autonomous, while outlining the advantages and disadvantages of each implementation. The interviews were divided into three sections: exploratory, anchoring and the PPA; While the exploratory phase's purpose was to learn about participants' attitudes and understanding of IoT, the anchoring phase aimed to normalize participants' basic understanding of how IoT functions. In order to get people to think about potential privacy concerns towards the end of the anchoring section, the authors asked participants about their opinions on data privacy. In the PPA section, it was proposed the idea of a PPA for IoT as a potential future project. The authors clarified that the PPA could distinguish between active data requests such as a gadget asking biometric information from the user's health tracker and passive data collection such as a smart device with a microphone that could record people's utterances while they were nearby. The Notification, Recommendation, and Auto implementations of an IoT PPA were the three that the authors and attendees discussed. Notification PPAs can

determine which adjacent devices are requesting data and alert users to those devices' presence and requests so that users can approve or reject each request. Building on notification PPAs, recommendation PPAs offer consumers advice on how to share their data based on their preferences. The user's data sharing decisions would be made by auto PPAs. This would lessen the cognitive load on consumers but also take away their ability to influence the process. They found that The participants' attitudes regarding the various implementations were generally favorable, although they also voiced worries, which varied depending on the degree of automation. Given the divergent motivations of participants some desired increased control, while others wished to avoid being overtaken by notifications and the lack of agreement regarding the optimal PPA implementation.

After the design phase, the institute implemented a privacy assistant (PA) [30], the authors called it IoT Assistant, because the predominant approach of "Notice and choice" for data privacy protection, they decided the PA would also fall into this approach, but because many systems implement notice as a form of consent, without sometimes offering choices to the end user, they also wanted this work to provide a conceptual framework that views user-centered privacy choice as well as a taxonomy for practitioners to use when designing meaningful privacy choices for their systems. The authors define meaningful privacy choices as "the capabilities provided by digital systems for users to control diferent data practices over their personal data", They extend the notion of privacy choices with five facets: efectiveness (the opportunity to establish privacy preferences that precisely and completely match the data collection and use methods that a user is okay with), efciency (the capacity to specify these options with the least amount of effort and time), user awareness (where significant privacy options should be prominently and clearly communicated to users), comprehensiveness (users should understand their options, how they affect the gathering and potential use of their data, as well as what conclusions might be drawn from this data and the potential repercussions of these conclusions) and neutrality (meaningful privacy decisions should not be subject to manipulation or bias). The IoT Assistant offers four privacy settings, giving end users a variety of alternatives to better suit their varied privacy preferences and as a result, privacy options are more effective in the IoT environment. The IoT Assistant acts as a centralized privacy choice platform by implementing various privacy options, allowing consumers to more effectively govern their data privacy in IoT. The three IoT system discovery modes that the IoT Assistant supports are QR codes, push notifications, and location-based map interfaces. These discovery tools are probably going to make users more aware of the installed IoT devices and the privacy options they have. Additionally, the united viewpoint of the integrated notification and option in the the IoT Assistant gives succinct yet thorough information regarding IoT data practices to help users better understand the implications of their privacy choices. Additionally, the authors work to implement the integrated notice and option in the IoT Assistant without bias or framing, attempting to offer consumers a neutral space to execute their privacy choices. Although the authors consider the IoT Assistant to be a significant step towards "meaningful privacy options" in IoT, this assistant still has many issues such as this application is still in the early stages of it's existence, and because this was created in 2020 and we are in 2022 there was not much growth. Maybe the main reason this application was not able to be developed further is that he application iself serves to show the user the data that is already in the IoT infastructure that was created before, and as such it is not capable of identifying new IoT devices without the end users themselfs create on the infastructure's main webpage [31] a new entry for the device in question that the user wants to interact with. Another reason that cripples this application and many like it that want to provide better privacy in IoT systems is that many systems don't offer any type of privacy choices to the end user or to other users that are not the intented end users but the devices are still collecting data about.

The IoT infastructure that was developed [31] is built on an open, distributed design that allows for the deployment and management of IoT resources to be carried out by any number of actors. Part of this infastructure is the Internet of Things Resource Registry, it is a web platform that enables resource owners to declare not only the place where a resource is deployed but also data practices like the reason(s) for a particular data collecting process, the level of detail in the data being gathered, retention, the recipients of the data, and more. Additionally, it discloses any user-configurable privacy settings that might be connected to a particular resource.

A similar project is LTEye [32] that is an open platform that provides granular temporal and spatial analytics on the performance of LTE radios without access to private user data or provider assistance. Despite the presence of multipath, LTEye uses a revolutionary extension of synthetic aperture radar to communication signals in order to precisely pinpoint mobile users.

III. Methodology

The proposed methology is composed of two phases, the first phase consists of making a study on the region's general concern with their privacy when using and interacting with IoT devices, their knowledge of privacy rights, what they do to protect their privacy rigths. One one side the objective of this study consist in demistefying the privacy paradox in the region and gather information about their idea to solve this problem with respect to iot devices. The second phase consists in doing an application that can detect iot devices nearby the user with at least a 10 meters radius. The application should do the following when detecting a device: 1. it should show some information about the device; 2. it should categorize the device; 3. it should provide the user with privacy options, if the device allows the user to decline data harvesting. This application at first sight might appear to be a mere privacy assistant but it's not, beacause iot assistants merely choose what privacy options the user first sets and mantains it for every other application that the user might

use. The proposed app doesn't have the objective to conform to the user's prefered privacy choices, it merely informs the user about nearby iot devices and can provide the user with privacy options. But the main objective is creating awareness in individuals about the various devices that are around and make the user questions their choices.

A. User Awareness

There has been some work done to determine the users awareness of their actions online in regard to privacy. An interactive theatre expericence [29] was proposed in order to expose privacy malpractices in companies, specially in the capitalistic world where profit is prioritize above all else, in this experiment the public is able to interact with the actors and influence the story of the play, there are various endings depending on the public's choices throughout the play, some endings the company would bury the corruption that was going on, in another ending a team of hackers is able to expose the company's practices to the world. After the play the team responsible for the experiment would talk with public members about what they experienced and discussed what was it about and the memebers pratices with their data on their daily lifes. After some months the team would talk again with the members that were present in the play and talk about any changes they have done in the meantime, most said they did not change thei behaviour, one member said that it took more care of The information that made available online because it had a bad expericence before where some private data was exposed that should have not been exposed. All in all the experiment did not prove to be a success in changing people's behaviour.

ACKNOWLEDGMENT

The preferred spelling of the word "acknowledgment" in America is without an "e" after the "g". Avoid the stilted expression "one of us (R. B. G.) thanks ...". Instead, try "R. B. G. thanks...". Put sponsor acknowledgments in the unnumbered footnote on the first page.

REFERENCES

[1] D. Vincent, *Privacy: A short history*. John Wiley & Sons, 2016.

[2] B. Moore, *Privacy: Studies in social and cultural history*. Routledge, 2017.

[3] E. Roosevelt, P. C. Chang, C. Malik, W. R. Hodgson, H. S. Cruz, R. Cassin, A. E. Bogomolov, C. D. 1st Baron Dukeston, and J. P. Humphrey. (1948) Universal declaration of human rights. [Online]. Available: https://www.un.org/en/about-us/universal-declaration-of-human-rights

[4] I. A. for Privacy Professionals. (2021) What does privacy mean? [Online]. Available: https://iapp.org/about/what-is-privacy/

[5] S. Spiekermann and L. F. Cranor, "Engineering privacy," *IEEE Transactions on Software Engineering*, vol. 35, no. 1, pp. 67–82, 2009.

[6] HIV.gov. (2018) The difference between security and privacy and why it matters to your program. [Online]. Available: https://www.hiv.gov/blog/difference-between-security-and-privacy-and-why-it-matters-your-program

[7] P. Emami-Naeini, H. Dixon, Y. Agarwal, and L. F. Cranor, "Exploring how privacy and security factor into iot device purchase behavior," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 2019, pp. 1–12.

[8] Y. J. Park, "Personal data concern, behavioral puzzle and uncertainty in the age of digital surveillance," *Telematics and Informatics*, vol. 66, p. 101748, 2022.

[9] N. A. Zhang, C. A. Wang, E. Karahanna, and Y. Xu, "Peer privacy concern: Conceptualization and measurement." *MIS Quarterly*, vol. 46, no. 1, 2022.

[10] M. Weiser, "The computer for the 21 st century," *Scientific american*, vol. 265, no. 3, pp. 94–105, 1991.

[11] D. Marikyan, S. Papagiannidis, and E. Alamanos, "A systematic review of the smart home literature: A user perspective," *Technological Forecasting and Social Change*, vol. 138, pp. 139–154, 2019.

[12] F. Arena, G. Pau, and A. Severino, "An overview on the current status and future perspectives of smart cars," *Infrastructures*, vol. 5, no. 7, p. 53, 2020.

[13] M. Al-Emran, S. I. Malik, and M. N. Al-Kabi, "A survey of internet of things (iot) in education: Opportunities and challenges," *Toward social internet of things (SIoT): enabling technologies, architectures and applications*, pp. 197–209, 2020.

[14] N. Niknejad, W. B. Ismail, A. Mardani, H. Liao, and I. Ghani, "A comprehensive overview of smart wearables: The state of the art literature, recent advances, and future challenges," *Engineering Applications of Artificial Intelligence*, vol. 90, p. 103529, 2020.

[15] I. F. Akyildiz and A. Kak, "The internet of space things/cubesats," *IEEE Network*, vol. 33, no. 5, pp. 212–218, 2019.

[16] K. Ashton. (2009) That "internet of things" thing. [Online]. Available: https://www.rfidjournal.com/that-internet-of-things-thing

[17] S. Madakam, V. Lake, V. Lake, V. Lake *et al.*, "Internet of things (iot): A literature review," *Journal of Computer and Communications*, vol. 3, no. 05, p. 164, 2015.

[18] M. Hasan. (2022) State of iot 2022: Number of connected iot devices growing 18% to 14.4 billion globally. [Online]. Available: https://iot-analytics.com/number-connected-iot-devices/

[19] S. Al-Sarawi, M. Anbar, R. Abdullah, and A. B. Al Hawari, "Internet of things market analysis forecasts, 2020-2030," in *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, 2020, pp. 449–453.

[20] N. Alhirabi, O. Rana, and C. Perera, "Security and privacy requirements for the internet of things: A survey," *ACM Transactions on Internet of Things*, vol. 2, no. 1, pp. 1–37, 2021.

[21] D. Peloquin, M. DiMaio, B. Bierer, and M. Barnes, "Disruptive and avoidable: Gdpr challenges to secondary research uses of data," *European Journal of Human Genetics*, vol. 28, no. 6, pp. 697–705, 2020.

[22] A. Gladis, N. J. Hartwich, and O. Salge, "Weaponizing the gdpr: How flawed implementations turn the gold standard for privacy laws into fool's gold," 2022.

[23] G. Gentile and O. Lynskey, "Deficient by design? the transnational enforcement of the gdpr," *International & Comparative Law Quarterly*, vol. 71, no. 4, pp. 799–830, 2022.

[24] B. Green, "The flaws of policies requiring human oversight of government algorithms," *Computer Law & Security Review*, vol. 45, p. 105681, 2022.

[25] D. Y. Byun, "Privacy or protection: The catch-22 of the ccpa," *Loy. Consumer L. Rev.*, vol. 32, p. 246, 2019.

[26] S. Keshav, "How to read a paper," *SIGCOMM Comput. Commun. Rev.*, vol. 37, no. 3, pp. 83–84, jul 2007. [Online]. Available: https://doi.org/10.1145/1273445.1273458

[27] M. Skirpan, M. Oates, D. Byrne, R. Cunningham, and L. F. Cranor, "Is a privacy crisis experienced, a privacy crisis avoided?" *Commun. ACM*, vol. 65, no. 3, pp. 26–29, feb 2022. [Online]. Available: https://doi.org/10.1145/3512325

[28] S. Gupta and S. Ghanavati, "Privacy in the internet of things: Where do we stand? a systematic literature review," 5 2022. [Online]. Available: https://www.techrxiv.org/articles/preprint/Privacy_in_the_Internet_of_Things_Where_do

[29] J. Colnago, Y. Feng, T. Palanivel, S. Pearman, M. Ung, A. Acquisti, L. F. Cranor, and N. Sadeh, "Informing the design of a personalized privacy assistant for the internet of things," in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, ser. CHI '20. New York, NY, USA: Association for Computing Machinery, 2020, pp. 1–13. [Online]. Available: https://doi.org/10.1145/3313831.3376389

[30] Y. Feng, Y. Yao, and N. Sadeh, "A design space for privacy choices: Towards meaningful privacy control in the internet of things," in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, ser. CHI '21. New York, NY, USA:

Association for Computing Machinery, 2021. [Online]. Available: https://doi.org/10.1145/3411764.3445148

[31] A. Das, M. Degeling, D. Smullen, and N. Sadeh, "Personalized privacy assistants for the internet of things: Providing users with notice and choice," *IEEE Pervasive Computing*, vol. 17, pp. 35–46, 07 2018.

[32] S. Kumar, E. Hamed, D. Katabi, and L. Erran Li, "Lte radio analytics made easy and accessible," in *Proceedings of the 2014 ACM Conference on SIGCOMM*, ser. SIGCOMM '14. New York, NY, USA: Association for Computing Machinery, 2014, pp. 211–222. [Online]. Available: https://doi.org/10.1145/2619239.2626320