

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 ubiquitous computing that human every day life is envisioned containing 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. When it comes to privacy rights, most service providers only do what the legislation "forces" them to and the users aren't aware or have little control over the information that is being collected. First it will be done a survey to gather the knowledge that Portugal's population has on this very topic and then in this thesis it is proposed a system that gives users information about the devices that are nearby and how to protect the data that the user doesn'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—privacidade, Internet of Things, computação ubíqua, assistente de privacidade

I. INTRODUÇÃO

Concerns about digital privacy have been growing in these last few years, specially after the anonymous group attacks, wikileaks and NSA controversies [11, 34], these concerns can be noted with the increase of papers on the subject, when searching for terms like "privacy", "online privacy", "digital privacy" in Google Scholar, ACM Digital Library or Science Direct it can be seen that, in the last 5 years, it returns about 1500000, 200000 and 60000 papers respectively. 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 its premise: even though privacy concerns have been increasing the behaviour of people when online doesn't seem 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 different perspectives, 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.

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 and many companies allocate much of their budget to develop these systems and create new ways to interact, collect data and analyse such data, privacy in these systems is not seen as a crucial factor in development, maybe because there isn't much interest in researching this aspect of IoT or because companies view other aspects of the development process as having higher priority. 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 ubiquitous computing and the rise of devices of various sizes that communicate with each other to do various (small) tasks, that make Weiser's idea a reality. These devices are used in various applications starting at home with thermostats, fridges, microwaves, etc, and embeded in cars, in the education system, in our clothes, our phones, watches and even into outer space. The first use of the term Internet of Things was in 1999 Kevin Ashton

It is predicted that iot will grow into trillions of devices by 2030 [1]

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.

Privacy and security might at first appear almost the same thing, but privacy is about the user's data and security is about protecting that data.

II. REVISÃO DE LITERATURA

A. *Trabalhos Relacionados*

There exists a number of privacy assistants in the market. Privacy assistants have the objective of giving the user flexibility in choosing the preferred 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) [2], 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) [3], 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 different data practices over their personal data", They extend the notion of privacy choices with

five facets: effectiveness (the opportunity to establish privacy preferences that precisely and completely match the data collection and use methods that a user is okay with), efficiency (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 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 its 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 the application itself serves to show the user the data that is already in the IoT infrastructure that was created before, and as such it is not capable of identifying new IoT devices without the end users themselves create on the infrastructure's main webpage [4] 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 intended end users but the devices are still collecting data about.

The IoT infrastructure that was developed [4] 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 infrastructure 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 [5] 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. METADOLOGIA

The proposed methodology 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 rights. On one side the objective of this study consist in demystifying 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, because IoT assistants merely choose what privacy options the user first sets and maintains it for every other application that the user might use. The proposed app doesn't have the objective to conform to the user's preferred 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 experience [2] 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 members practices with their data on their daily lives. 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 their behaviour, one member said that it took more care of The information that made available online because it had a bad experience 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.

AGRADECIMENTOS

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] 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.
- [2] 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, p. 1–13. [Online]. Available: <https://doi.org/10.1145/3313831.3376389>
- [3] 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>
- [4] 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.
- [5] 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, p. 211–222. [Online]. Available: <https://doi.org/10.1145/2619239.2626320>