22nd International Conference e-Society 2024

Privacy and Digital Literacy in the Internet of Things

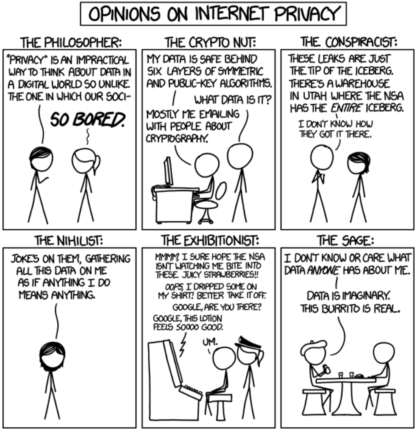
Nelson Vieira and Mary Barreto

University of Madeira
Faculty of Exact Sciences and Engineering

March 12, 2024

Table of Contents

1. Introduction
2. State of the Art
3. Methodology
   - Survey
4. Conclusion and Future Work
   - Future Work
   - Conclusion


OPINIONS ON INTERNET PRIVACY
THE PHILOSOPHER:
"PRIVACY" IS AN IMPRACTICAL WAY TO THINK ABOUT DATA IN A DIGITAL WORLD SO UNLIKE THE ONE IN WHICH OUR SOCI-
SO BORED.
THE CRYPTO NUT:
MY DATA IS SAFE BEHIND SIX LAYERS OF SYMMETRIC AND PUBLIC-KEY ALGORITHMS.
WHAT DATA IS IT?
MOSTLY ME EMAILING WITH PEOPLE ABOUT CRYPTOGRAPHY.
THE CONSPIRACIST:
THESE LEAKS ARE JUST THE TIP OF THE ICEBERG. THERE'S A WAREHOUSE IN UTAH WHERE THE NSA HAS THE ENTIRE ICEBERG.
I DON'T KNOW HOW THEY GOT IT THERE.
THE NIHILIST:
JOKE'S ON THEM, GATHERING ALL THIS DATA ON ME AS IF ANYTHING I DO MEANS ANYTHING.
THE EXHIBITIONIST:
MMMM, I SURE HOPE THE NSA ISN'T WATCHING ME BITE INTO THESE JUICY STRAWBERRIES!!
OOPS, I DRIPPED SOME ON MY SHIRT! BETTER TAKE IT OFF.
GOOGLE, ARE YOU THERE?
GOOGLE, THIS LOTION FEELS SOOOO GOOD.
UM.
THE SAGE:
I DON'T KNOW OR CARE WHAT DATA ANYONE HAS ABOUT ME.
DATA IS IMAGINARY. THIS BURRITO IS REAL.

```
diff privacy.c
↑       @@ -1,1 +1,1 @@
1  - Privacy
1  + Security
↓         ...
```

Introduction

The advent of ubiquitous computing has resulted in the widespread use of Internet of Things devices. These devices open up new avenues for the collection and exploitation of user and non-user personal data. Most end users are not even aware or have little control over the information that is being collected about them by these systems.

Privacy Paradox

The use of a variety of digital devices has numerous advantages, but they also bring the ubiquity of data capturing equipment, therefore, it is understandable why users have serious concerns about the privacy of their personal data. The privacy paradox happens when the opinions stated by the users are radically different from their actions.

Proven to be debased by a number of empirical studies [1, 2].

State of the Art

There are two main ways to provide privacy in IoT systems:

- Through security [3, 4, 5];
- User awareness (eg. privacy notices) [6, 7];

Legislation or a framework/architecture mainly fall into one these two categories.

State of the Art

There are two main ways to provide privacy in IoT systems:

- Through security [3, 4, 5];
- User awareness (eg. privacy notices) [6, 7];

Legislation or a framework/architecture mainly fall into one these two categories.

State of the Art

Skirpan et al. (2022) [8] developed an interactive theatre experience as a case study to gather user awareness about digital privacy. The authors noted that after contacting people months after the initial interviews that they did not really changed their behaviour regarding their privacy.

The Carnegie Mellon University CyLab designed a personalized privacy assistant (2020) [9] where users could see IoT devices near their location. The implementation is fragmented with the creation of an application [6] the cannot be interacted with and a webpage [7] where users can actually modify data.

Survey

86 Questions

- General knowledge and attitudes towards privacy
- Disposition for sharing personal information
- Privacy concerns
- Current online habits and practices
- Profile identification
- Knowledge and habits regarding the Internet of Things
- Demographic data

Google Forms, https://www.google.com/images/about/forms-icon.svg

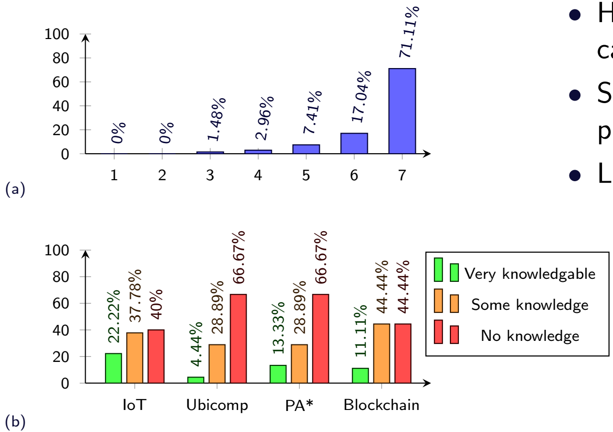
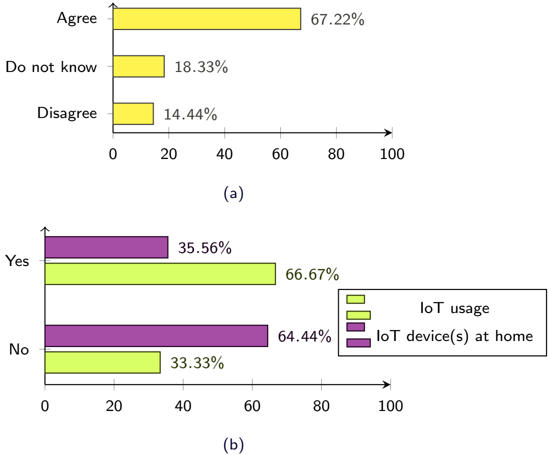


Figure 1: Participant responses regarding: (a) participants' privacy importance perception and (b) general IT knowledge. (Section 4)

- High regard for privacy, with some caveats;
- Some difficulty understating digital privacy;
- Low literacy of technical jargon;

*PA - Privacy Assistant

Survey



(a)

(b)

Figure 2: Participant responses regarding: (a) unwillingness to read privacy notices and (b) IoT usage. (Section 4)

- Dismissal of privacy notices due to various factors;
- Some individuals (55%) use fake private data online;
- Some interaction with Internet of Things devices but low knowledge generally;
- Low grasp of IoT privacy;

Limitations and Future Work

Survey limitations:

- Too dense;
- Limited number of participants.

Topics for further research:

- Privacy literacy in IoT systems;
- Application of privacy in the design/development of IoT systems;
- User-centric approaches to IoT privacy.

Conclusion

- Results from majority viewpoint of portuguese participants;
- Survey results reveal that there is a large privacy knowledge gap;
- There should be more tools focused on privacy literacy.

Thank you for your attention.

References I

- S. Sannon, N. N. Bazarova, and D. Cosley, “Privacy lies: Understanding how, when, and why people lie to protect their privacy in multiple online contexts,” in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 2018, pp. 1–13.

- W. Xie and K. Karan, “Consumers’ privacy concern and privacy protection on social network sites in the era of big data: empirical evidence from college students,” *Journal of Interactive Advertising*, vol. 19, no. 3, pp. 187–201, 2019.

- Y. Zhao, J. Zhao, M. Yang, T. Wang, N. Wang, L. Lyu, D. Niyato, and K.-Y. Lam, “Local differential privacy-based federated learning for internet of things,” *IEEE Internet of Things Journal*, vol. 8, no. 11, pp. 8836–8853, 2020.

- Q. Zhang, L. T. Yang, Z. Chen, P. Li, and M. J. Deen, “Privacy-preserving double-projection deep computation model with crowdsourcing on cloud for big data feature learning,” *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2896–2903, 2017.

References II

- M. S. Ali, K. Dolui, and F. Antonelli, "IoT data privacy via blockchains and ipfs," in *Proceedings of the Seventh International Conference on the Internet of Things*, ser. IoT '17. New York, NY, USA: Association for Computing Machinery, 2017. [Online]. Available: https://doi.org/10.1145/3131542.3131563

- 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

- 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.

References III

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, 02 2022. [Online]. Available: https://doi.org/10.1145/3512325

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