

22nd International Conference e-Society 2024

# Privacy and Digital Literacy in the Internet of Things

Nelson Vieira and Mary Barreto

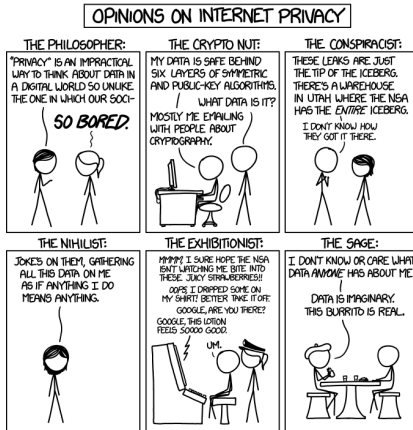
University of Madeira  
Faculty of Exact Sciences and Engineering

March 10, 2024

# Table of Contents

- 1 Introduction
- 2 State of the Art
- 3 Methodology

- Survey
- 4 Conclusion and Future Work
  - Future Work
  - Conclusion



© Randall Munroe, CC BY-NC 2.5 License

```
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

It happens when the opinions stated by the users are radically different from their actions.

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

# State of the Art

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

- Through security [?, ?, ?];
- User awareness (eg. privacy notices) [?, ?];

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 [?, ?, ?];
- User awareness (eg. privacy notices) [?, ?];

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

# State of the Art

Skirpan et al. (2022) [?] 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) [?] where users could see IoT devices near their location. The implementation is fragmented with the creation of an application [?] the cannot be interacted with and a webpage [?] where users can actually modify data.



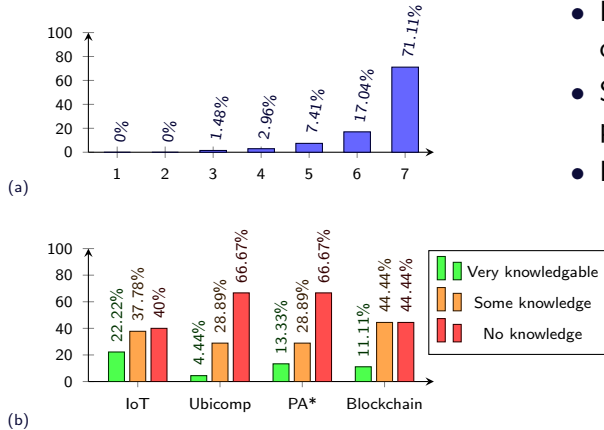
# Survey

## 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>

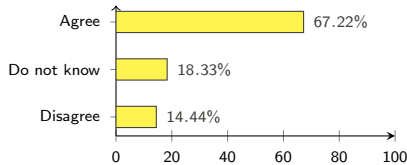


- High regard for privacy, with some caveats;
- Some difficulty understating digital privacy;
- Low literacy of technical jargon;

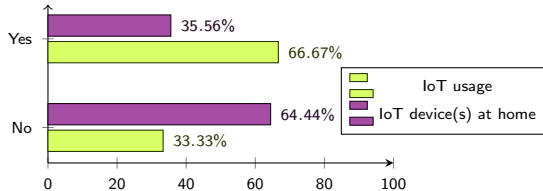
\*PA - Privacy Assistant

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

## Survey



(a)



(b)

- 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;

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

# 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