Demo Abstract: PriviFy: Designing Tangible Interfaces for IoT Privacy Configuration

Bayan Al Muhander
School of Computer Science and Informatics
Cardiff University
Cardiff, UK
almuhanderb@cardiff.ac.uk

Omer Rana
School of Computer Science and Informatics
Cardiff University
Cardiff, UK
ranaof@cardiff.ac.uk

Charith Perera
School of Computer Science and Informatics
Cardiff University
Cardiff, UK
pereraC@cardiff.ac.uk

***Abstract*—As Internet of Things (IoT) devices can gather sensitive data from users, it is essential that users configure their privacy preferences to protect their data. Users, however, have difficulty configuring their privacy settings due to the numerous complexities involved. We follow design space recommendations and present PriviFy (Privacy Simplify-er), a novel tangible interface that simplifies the configuration of smart devices' privacy settings. PriviFy enables users to modify their data privacy preferences using interactive knobs and buttons. PriviFy also emits lights and displays messages to confirm user choices. PriviFy's goal is to simplify the complexity of privacy configuration and empower users to regain control over their privacy in the IoT. Consequently, users would be able to make more informed and conscious decisions about how their data is shared. Demo Video (https://youtu.be/sgnE9zCVQT0)**

***Index Terms*—Internet of Things, Design Space, Usable Privacy, Privacy Configuration, Tangible Interface**

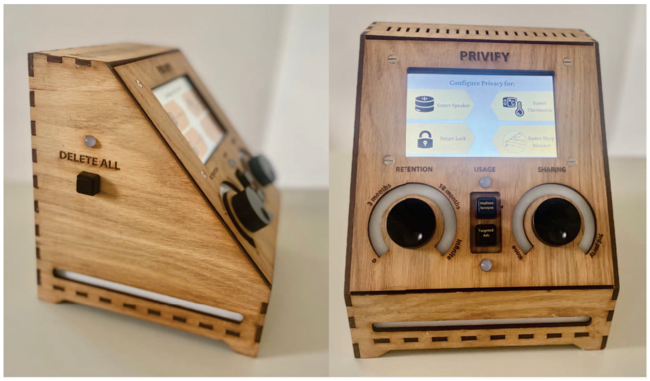

Fig. 1. PriviFy high fidelity prototype demonstrating interactive physical controls via knobs and buttons and feedback mechanism via lights and display.

I. Introduction and Related Work

The use of numerous IoT services frequently necessitates the sharing of user data. Data such as these are considered a valuable resource to service providers, but users are increasingly concerned about privacy threats, as their private information is released to multiple parties. To alleviate users' concerns, some IoT services provide privacy configuration options through which users can control the use of their data. Unfortunately, the majority of the available options fail to support users' privacy needs. This is because privacy options are usually difficult to locate and understand, are not user-friendly, and do not provide meaningful choices [1].

Privacy regulations, such as the General Data Protection Regulation (GDPR), enforce the need for transparency and give users control over their data. As a result, privacy research has investigated different ways to create usable and transparent privacy choice mechanisms to enhance users' privacy awareness and informed decision-making [2]. In spite of that, many of the available methods lack adaptation and are not appealing to users [3] due to their complexity, non-intuitiveness, and non-engaging interactions. Research in privacy has also introduced the concept of *tangible privacy*, which refers to systems that allow users to easily manage their privacy settings through tangible interaction [4]. *Tangible privacy* has shown its effectiveness in increasing users' interactivity and engagement with their privacy preferences [5].

Consequently, we leverage design space recommendations [6] to develop PriviFy as a tangible interface to allow direct interaction with privacy preferences. We validate our approach's feasibility and usability through a prototype implementation employing various physical components. We used knobs and buttons with concise, descriptive text to facilitate user interaction, enabling users to correlate them with specific privacy choices easily. We integrated lights and short confirmation messages on the display to give users meaningful and understandable feedback. Figure 1 depicts PriviFy's prototype.

In this paper, we report on our implementation of PriviFy as a simple and intuitive tool designed to assist IoT users in managing and understanding their privacy preferences. Through multiple focus group studies, we explored two main aspects: (i) how to make the privacy configuration practice transparent and intuitive to users and (ii) the potential of a tangible interface to motivate users to manage their privacy.

979-8-3503-7025-6/24/$31.00 ©2024 IEEE
DOI 10.1109/IoTDI61053.2024.00024

II. Design considerations and Process

We systematically design PriviFy's prototype through iterative low-, medium-, and high-fidelity stages, ensuring a comprehensive progression from problem identification to validation while adhering to design considerations.

Design considerations Informed by design space recommendations [6], we identify four key design considerations, guiding our privacy configuration tangible interface design.

- User needs: The interface should provide users with privacy choices that are consistent with their privacy preferences when making privacy decisions.
- User Engagement: The interface should effectively draw users to interact with it and provide a pleasant and satisfying user experience.
- Usability: The interface should enable users to perform the action they intend to perform with minimal effort.
- Findability: The interface should make it easy for the users to locate the specific privacy controls they require, regardless of their level of knowledge or expertise. Ideally, users should quickly regain proficiency in the interface after a period of inactivity.

Design Process: We initiated the design process for PriviFy by thoroughly examining IoT devices that offer any type of tangible interaction. We evaluated 100 IoT devices, of which only 30 devices have physical control capabilities. Typically, other IoT devices are managed via a software application. Based on these findings, we created three low-fidelity prototypes for PriviFy, as depicted in Figure 2 (i). We proceeded by conducting a focus group study involving ten participants at the University department. The objective of the focus group was to generate ideas for a potential physical interface and collect feedback on PriviFY's initial low-fidelity designs.

1) Low Fidelity Prototyping: We introduced participants to IoT privacy and discussed challenges in managing privacy preferences. We presented images of tangible interfaces to evaluate their suitability for IoT privacy configuration. Participants were engaged in collaborative low-fidelity tangible interface design tasks, developing different prototypes. We then presented three prototypes, seeking participants' feedback.

2) Medium Fidelity Prototyping: Leveraging the low-fidelity prototyping session findings, we iteratively refined PriviFy's design and created two medium-fidelity prototypes. We provided the participants with IoT use cases and instructed them to use the prototypes to configure their preferences. Figure 2 (ii) depicts the participants setting their privacy choices using the medium-fidelity prototype. Participants were encouraged to think aloud, discussing their chosen configurations and expressing preferences or concerns about the prototypes, while also suggesting usability improvements.

3) High Fidelity Prototyping: Informed by insights from the multiple user studies, we built PriviFy's high-fidelity prototype (Figure 1). PriviFy is carefully designed to incorporate a small number of configuration options following literature on usable privacy interfaces [7], which facilitate a quick and efficient configuration of privacy preferences for diverse users.

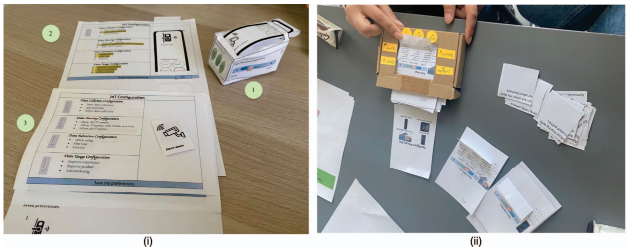

Fig. 2. The iterative prototyping process employed in this study shows three initial low-fidelity prototypes created by the research team (i), followed by participants interacting with the medium-fidelity prototype (ii).

We intend to conduct evaluations with individuals who use IoT devices to assess PriviFy's usability and its adherence to design considerations. We also plan to compare users' experiences configuring their privacy preferences using PriviFy to state-of-the-art designs. This comparison is expected to yield valuable insights contributing to the advancement of research and potentially reshaping how individuals manage their data.

III. Demonstration

To demonstrate PriviFy's capabilities, we present a fictional use case of Sara engaging with a smart speaker. Sara uses PriviFy to tailor her privacy preferences as follows:

- Sara configures data retention by rotating the knob, which activates lights as she rotates that provide visual confirmation of the selected data duration. Once Sara stops at a selected time, a notification appears on the display for her to confirm her choice.
- Sara configures data usage, including targeted ads and service improvement, through the button switches. The light signals activation and deactivation, with notifications on the display prompting Sara to confirm her choices.
- Sara configures sharing by rotating the knob. The light illuminates as she rotates it, and a notification appears to confirm her choices of sharing with third parties.

References

[1] H. Habib, S. Pearman, E. Young, I. Saxena, R. Zhang, and L. F. Cranor, "Identifying user needs for advertising controls on facebook," *Proceedings of ACM on Human-Computer Interaction*, vol. 6, no. CSCW1, 2022.

[2] Y. Yao, J. R. Basdeo, O. R. Mcdonough, and Y. Wang, "Privacy perceptions and designs of bystanders in smart homes," *Proceedings of the ACM on Human-Computer Interaction*, vol. 3, no. CSCW, 2019.

[3] J. Im, R. Wang, W. Lyu, N. Cook, H. Habib, L. F. Cranor, N. Banovic, and F. Schaub, "Less is not more: Improving findability and actionability of privacy controls for online behavioral advertising," in *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, 2023.

[4] I. Ahmad, R. Farzan, A. Kapadia, and A. J. Lee, "Tangible privacy: Towards user-centric sensor designs for bystander privacy," *Proceedings of the ACM on Human-Computer Interaction*, vol. 4, no. CSCW2, 2020.

[5] Y. Jansen, P. Dragicevic, P. Isenberg, J. Alexander, A. Karnik, J. Kildal, S. Subramanian, and K. Hornbæk, "Opportunities and challenges for data physicalization," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pp. 3227–3236, 2015.

[6] H. Habib and L. F. Cranor, "Evaluating the usability of privacy choice mechanisms," in *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, pp. 273–289, 2022.

[7] J. Kolter and G. Pernul, "Generating user-understandable privacy preferences," in *2009 International Conference on Availability, Reliability and Security*, pp. 299–306, IEEE, 2009.