Tangible Privacy

Piero Romare

Master's Thesis Proposal

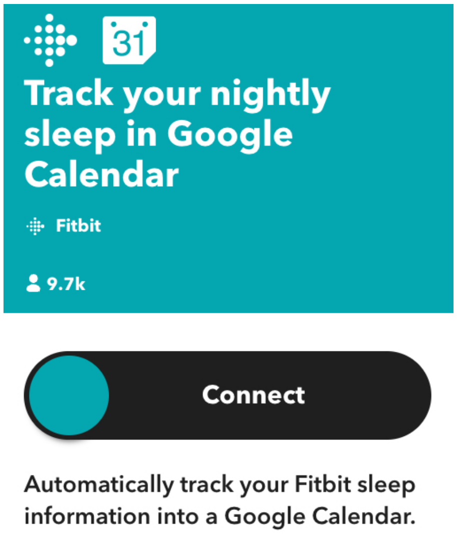
1 Abstract

Tangible privacy offers an innovative approach, incorporating physical controls and feedback mechanisms that empower users to manage their privacy intuitively. By bridging the gap between digital processes and human comprehension, tangible privacy tools can enhance transparency, improve user trust, and promote greater engagement. As IoT continues to evolve, embedding tangible privacy into smart environments represents a relevant step toward a more secure and user-centric future. This approach not only prioritizes user autonomy but also encourages a cultural shift towards proactive privacy control in an increasingly interconnected world. Ultimately, tangible privacy can redefine how individuals interact with technology and manage their data, making privacy an integral part of everyday experiences.

2 Background

As smart homes and smart cities become increasingly interwoven with IoT devices and sensors, concerns surrounding privacy and data security are becoming more pronounced. The rapid proliferation of new IoT devices and online services demands significant amounts of personal data to function effectively. When end-users interact with IoT devices, their data fuels these services, often without transparent mechanisms to manage how this information is processed or shared. Moreover, platforms like IFTTT, Make, and Zapier enable users to integrate and connect these devices within smart environments—such as homes, cities, or wearable ecosystems—creating automations that simplify daily tasks. Using End-User Development (EUD) frameworks based on "if-then" formulas (e.g., if entering a room, then turning on the light), these platforms enhance interoperability and empower users to design their own IoT applications efficiently. Figure 1 illustrates how users can download pre-configured applets, while Figure 2 showcases the interface for creating custom automations.

However, the usability of these platforms must align with fundamental user rights, ensuring individuals retain control over their data and remain informed about its processing, particularly in IoT environments (Caivano et al., 2018; Paternò & Santoro, 2019). Traditional privacy solutions often fail to provide sufficient transparency, leaving users uncertain about who or what has access to their personal information in these interconnected ecosystems.


Track your nightly sleep in Google Calendar

Automatically track your Fitbit sleep information into a Google Calendar.

Figure 1: IFTTT as store to download pre-created app

Figure 2: IFTTT interface for creating automations

To address these challenges, tangible privacy employs physical, intuitive controls and feedback mechanisms to help users manage privacy within smart environment settings (Ahmad et al., 2020). This approach addresses the uncertainties often faced by bystanders and visitors (e.g., secondary users) regarding the privacy implications of IoT devices equipped with embedded sensors. Research shows that tangible privacy controls are perceived as more trustworthy, user-friendly, and engaging compared to non-tangible alternatives (Ahmad et al., 2022; Delgado Rodriguez, Prange, Vergara Ossenberg, et al., 2022). Examples such as PriKey and physical privacy controls integrated into smart voice assistants (Ahmad et al., 2022; Delgado Rodriguez, Prange, Vergara Ossenberg, et al., 2022).

Despite its promise, the extend implementation of tangible privacy in future smart environments presents challenges. These include scaling solutions to accommodate multiple interconnected devices and balancing granular control of individual sensors with overarching privacy needs at the system level, such as in a smart home (Windl et al., 2023). Overall, tangible privacy represents a significant opportunity to enhance privacy assurance, empower user control, and improve awareness in IoT ecosystems.

The concept of tangible privacy has emerged in the context of IoT devices and smart environments as a means to improve privacy control and transparency. It refers to physical systems that enable users to actively manage their data sharing. Key aspects of tangible privacy include:

- Sensor Control: the ability to control devices with multiple sensors (e.g., cameras, microphones, smartwatches) either individually (Tiefenau et al., 2019) or collectively through standardized manufacturer protocols (Windl et al., 2023), thereby enhancing privacy.
- User-Centric Sensor Design: systems designed to provide users with clear, unambiguous feedback on data collection activities. These mechanisms, which shift from software to hardware-based solutions, enhance both usability and privacy in smart environments (Ahmad et al., 2022).
- Boundary Regulation with IoT Devices: tangible privacy offers practical tools for boundary regulation, ensuring that both primary and secondary users (Ahmad et al., 2020) retain control over their data and privacy within IoT ecosystems.

3 Related Work

An ideation toolkit (Mehta et al., 2023) designed to inspire the creation of tangible privacy management tools functions as a collaborative game, fostering group engagement. Complementing this, a framework proposed by the same authors (Mehta et al., 2021) explores fundamental dimensions of privacy management: control and awareness. The framework's effectiveness is grounded in features such as directness, ready-to-hand access, and contextual adaptation:

- Directness: reduces cognitive load by leveraging intuitive metaphors, making privacy controls easier to understand and use (Delgado Rodriguez et al., 2023).
- Ready-to-Hand Access: enhances accessibility by ensuring privacy tools are immediately available when needed while maintaining fine-grained privacy preference settings and non-intrusive implementations.
- Contextual Adaptation: supports customization through modular designs and flexible settings that align with user-specific needs and environments.

A list of tools follows:

- PriKey (Delgado Rodriguez, Prange, Knierim, et al., 2022; Delgado Rodriguez, Prange, Vergara Ossenberg, et al., 2022) has been developed and evaluated with the goal of providing awareness and control to the primary and secondary users. The interface is organized by grouping the sensors that are in different rooms or environments. Both the IoT device owners and the visitors of them can know and decide about their privacy settings (see Figure 3).
- PrivacyCube (Muhander et al., 2022) is a physical tool with four faces that are collected data type, data location plus the retention time, data access and data usage. It allows the end-users to keep track of what's

going on with their IoT devices and the fuel - data - that drives them (see Figure 4a).

- Privacy Band (Mehta, 2019) that is a forearm wearable following by a user-centric approach evaluation has the goal of providing interactive privacy management using haptic vibrations (see Figure 4b).
- PriviFy (Muhander et al., 2024) which allow the users to control the sharing, usage and retention time on their data by rotating a knob. The confirmation about the users decision are visualized in a screen (see Figure 4c).

4 Conclusion

In an increasingly interconnected world where IoT devices pervade smart homes and cities, tangible privacy provides a user-centric solution to the challenges of data control and transparency. By utilizing physical, intuitive controls and feedback mechanisms, tangible privacy empowers users with real-time control over data collection and usage, improving trust and enhancing engagement. This project aims to design and develop a tangible privacy prototype that integrates physical interaction with IoT devices, enabling users to manage privacy settings dynamically while offering clear and transparent feedback about their data sharing activities.

5 Skills

- Hardware prototyping skills (Arduino or Raspberry PI)
- Conducting interviews and analyzing response data
- Programming skills

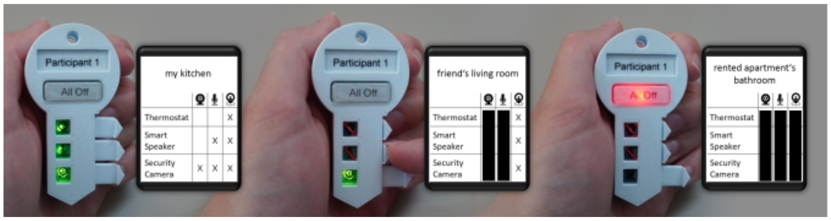


Figure 3: PriKey

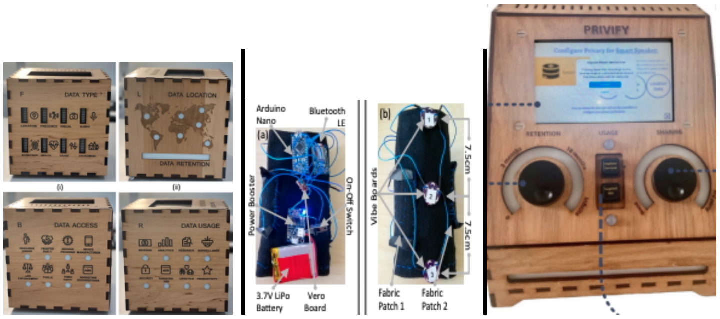


Figure 4: Privacy Band

References

Ahmad, I., Akter, T., Buher, Z., Farzan, R., Kapadia, A., & Lee, A. J. (2022). Tangible Privacy for Smart Voice Assistants: Bystanders' Perceptions of Physical Device Controls. *Proceedings of the ACM on Human-Computer Interaction*, *6*(CSCW2), 1–31. https://doi.org/10.1145/3555089

Ahmad, I., Farzan, R., Kapadia, A., & Lee, A. J. (2020). Tangible Privacy: Towards User-Centric Sensor Designs for Bystander Privacy. *Proceedings of the ACM on Human-Computer Interaction*, *4*(CSCW2), 1–28. https://doi.org/10.1145/3415187

Caivano, D., Fogli, D., Lanzilotti, R., Piccinno, A., & Cassano, F. (2018). Supporting end users to control their smart home: Design implications from a literature review and an empirical investigation. *Journal of Systems and Software*, *144*, 295–313. https://doi.org/https://doi.org/10.1016/j.jss.2018.06.035

Delgado Rodriguez, S., Dao Phuong, A., Bumiller, F., Mecke, L., Dietz, F., Alt, F., & Hassib, M. (2023). Padlock, the Universal Security Symbol? - Exploring Symbols and Metaphors for Privacy and Security. *Proceedings of the 22nd International Conference on Mobile and Ubiquitous Multimedia*, 10–24. https://doi.org/10.1145/3626705.3627770

Delgado Rodriguez, S., Prange, S., Knierim, P., Marky, K., & Alt, F. (2022). Experiencing Tangible Privacy Control for Smart Homes with PriKey. *Proceedings of the 21st International Conference on Mobile and Ubiquitous Multimedia*, 298–300. https://doi.org/10.1145/3568444.3570585

Delgado Rodriguez, S., Prange, S., Vergara Ossenberg, C., Henkel, M., Alt, F., & Marky, K. (2022). PriKey – Investigating Tangible Privacy Control for Smart Home Inhabitants and Visitors. *Nordic Human-Computer Interaction Conference*, 1–13. https://doi.org/10.1145/3546155.3546640

Mehta, V. (2019). Tangible Interactions for Privacy Management. *Proceedings of the Thirteenth International Conference on Tangible, Embedded, and Embodied Interaction*, 723–726. https://doi.org/10.1145/3294109.3302934

Mehta, V., Gooch, D., Bandara, A., Price, B., & Nuseibeh, B. (2021). Privacy Care: A Tangible Interaction Framework for Privacy Management. *ACM Transactions on Internet Technology*, *21*(1), 1–32. https://doi.org/10.1145/3430506

Mehta, V., Gooch, D., Bandara, A., Price, B. A., & Nuseibeh, B. (2023). A Card-based Ideation Toolkit to Generate Designs for Tangible Privacy Management Tools. *Proceedings of the Seventeenth International Conference on Tangible, Embedded, and Embodied Interaction*, 1–13. https://doi.org/10.1145/3569009.3572903

Muhander, B. A., Rana, O., Arachchilage, N., & Perera, C. (2022). Demo Abstract: PrivacyCube: A Tangible Device for Improving Privacy Awareness in IoT. *2022 IEEE/ACM Seventh International Conference on Internet-of-Things Design and Implementation (IoTDI)*, 109–110. https://doi.org/10.1109/IoTDI54339.2022.00024

Muhander, B. A., Rana, O., & Perera, C. (2024). Privify: Designing tangible interfaces for configuring iot privacy preferences. https://arxiv.org/abs/2406.05459

Paternò, F., & Santoro, C. (2019). End-user development for personalizing applications, things, and robots [50 years of the International Journal of Human-Computer Studies. Reflections on the past, present and future of human-centred technologies]. *International Journal of Human-Computer Studies*, *131*, 120–130. https://doi.org/https://doi.org/10.1016/j.ijhcs.2019.06.002

Tiefenau, C., Häring, M., Gerlitz, E., & von Zezschwitz, E. (2019). Making privacy graspable: Can we nudge users to use privacy enhancing techniques? *ArXiv*, *abs/1911.07701*. https://api.semanticscholar.org/CorpusID:199530719

Windl, M., Schmidt, A., & Feger, S. S. (2023). Investigating Tangible Privacy-Preserving Mechanisms for Future Smart Homes. *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, 1–16. https://doi.org/10.1145/3544548.3581167