Poster Abstract: *PrivacyVis*: Interactive Visualization Tool for Privacy Risks of Internet of Things Sensors

Dipu Ram Roy
rdipu.roy01@gmail.com
BUET
Dhaka, Bangladesh

Jieqiong Zhao
jiezhao@augusta.edu
Augusta University
Augusta, GA, USA

Shijia Pan
span24@ucmerced.edu
Univ. of California, Merced
Merced, CA, USA

Shiwei Fang
shfang@augusta.edu
Augusta University
Augusta, GA, USA

ABSTRACT

The widespread adoption of Internet of Things (IoT) devices has significantly enhanced convenience for consumers, yet the privacy implications of these devices remain unclear to most users, even with the availability of privacy policies. To address this challenge, we introduce a novel visualization tool that provides an informative and expressive visual representation of the sensors, data processing workflows, and associated privacy risks of IoT devices. This user-friendly tool is designed to enhance user understanding, empowering them to make informed decisions about their privacy.

KEYWORDS

Internet of Things, Privacy, Privacy Policy, Visualization

ACM Reference Format:
Dipu Ram Roy, Jieqiong Zhao, Shijia Pan, and Shiwei Fang. 2025. Poster Abstract: *PrivacyVis*: Interactive Visualization Tool for Privacy Risks of Internet of Things Sensors. In *The 23rd ACM Conference on Embedded Networked Sensor Systems (SenSys '25), May 6–9, 2025, Irvine, CA, USA.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3715014.3724041

1 INTRODUCTION

The Internet of Things (IoT) has rapidly transformed everyday life, enabling seamless interaction with a wide range of devices, such as smart home appliances and security systems. These devices provide functionalities like voice command control, security surveillance, and in-home health monitoring, offering significant convenience and enhancing automation in the home environment. However, as IoT devices become increasingly integrated into daily routines, users are often unaware of the privacy implications associated with these technologies, especially as the complexity of such devices grows with the introduction of new sensor technologies.

The primary means users attempt to understand privacy implications is through privacy policies provided by manufacturers. Unfortunately, these policies are often lengthy, written in dense legal language, and difficult for lay people to interpret. As a result, many users struggle to comprehend the extent to which their personal data is collected, processed, and shared. Furthermore, IoT devices often operate in ways that are opaque to users, with data being continuously collected and processed in the background to ensure a seamless user experience. This lack of transparency, combined with the challenge of comprehending privacy policies, creates an information asymmetry between users and service providers, exacerbating the privacy knowledge gap. Consequently, users face significant challenges in making informed decisions about the privacy risks associated with IoT devices.

Previous research has explored methods to improve user engagement with privacy policies, acknowledging that most people do not read them [5]. Privacy Nutrition Labels [3] have attempted to summarize privacy policies, while annotated text privacy policies [6] allow users to find specific information about data use practice more easily. Poli-see [2] has explored visualization to inform users about data flow and usage. PrivaSee [7] explored using AR to highlight sensing areas. While these works have demonstrated better user engagement and understanding, they are more focused on non-IoT devices, which do not continuously record potentially privacy-intrusive data that IoT devices do.

We propose a novel approach to address these challenges through the development of an interactive web-based visualization tool – *PrivacyVis* – designed to enhance user comprehension of IoT device privacy risks. *PrivacyVis* provides an informative and expressive representation of the sensors involved in data collection, the subsequent processing steps, and the potential privacy risks associated with the use of these devices. With a straightforward, accessible interface, *PrivacyVis* empowers users with a deeper understanding of how their data is used and the privacy risks they might face. Our approach aims to bridge the information gap and help users navigate the complex privacy landscape of modern IoT technologies.

2 SYSTEM DESIGN

PrivacyVis is implemented as a web-based application that leverages React for efficient updates in response to user interactions and D3 for rendering a tailored graphical interface. It is designed to reveal potential privacy risks in IoT devices through three coordinated panels: (1) a Sankey Diagram (Figure 1 ⓐ) that provides an overview of potential risk pathways, illustrating the flow of data from sensors to processing stages and their associated privacy risks; (2) a Radial Bar Chart (Figure 1 ⓑ) that quantifies privacy risk across different categories, where higher values indicate a greater likelihood of privacy exposure; and (3) a Privacy Policy text panel (Figure 1 ⓒ) that displays the privacy policy of a hypothetical IoT device and highlights relevant content in colors corresponding to specific sensors and data processing.

Unlike previous works, our approach emphasizes the sensors used in IoT devices, visualizes the tasks performed on the collected data, and highlights the associated privacy risks. The **Sensor** component is specifically tailored to IoT devices, which are sensor-rich

SenSys '25, Irvine, CA, USA

ACM ISBN 979-8-4007-1479-5/25/05
https://doi.org/10.1145/3715014.3724041

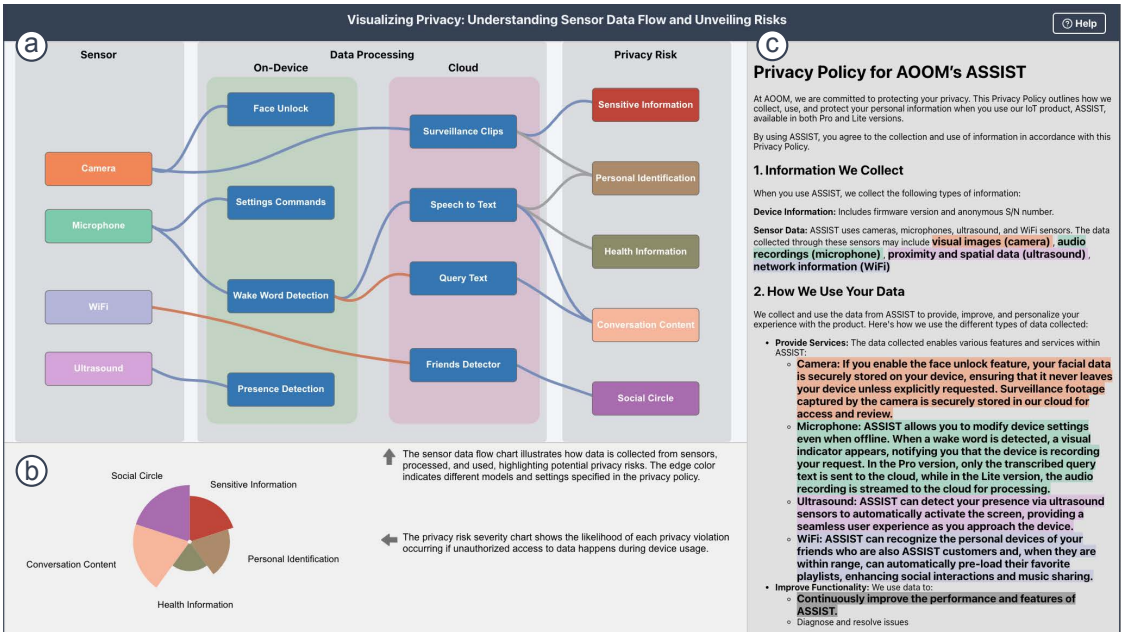

Figure 1: Privacy Policy Visualization Website. The visualization comprises three coordinated views: ⓐ a Sankey Diagram that maps the flow of data from sensors through processing stages to their associated privacy risks; ⓑ a Radial Bar Chart that quantifies privacy risks across different categories, with higher values indicating greater exposure likelihood; and ⓒ a Privacy Policy text panel that presents the privacy policy with highlighted text corresponding to specific privacy risk categories.

but often lack clear visibility for users. While sensors such as cameras and microphones are familiar to many users, others like WiFi [1] and vibration [4] remain less well-known, creating an additional barrier to comprehending their potential privacy risks. To increase user awareness, we introduce the **Data Processing** component, which illustrates the tasks performed on the data collected by these sensors. We also employ color encoding to convey the risk levels associated with **On-Device** versus **Cloud**-based processing within the **Data Processing** component. This distinction is increasingly important, as devices may default to one or the other, even if they perform the same functions.

Understanding the privacy risks tied to data processing can be challenging for users. While it may be clear how data is processed, the specific privacy risks associated with that processing are often unclear. For instance, users might recognize that recordings of conversations can expose content but may not realize that these recordings could also be used for identification or health assessments. To further assist users, we provide concrete examples of these risks in **Privacy Risk** component, helping them recognize the potential privacy concerns linked to their data. Additionally, we introduce an assessment of the likelihood of privacy leakage, acknowledging that while data extraction may be possible in some cases, the likelihood of such occurrences can vary. This helps users better assess the potential risk of privacy breaches tied to their data. Our visualization approach enhances user awareness of data privacy concerns by externalizing the relationships between an IoT device's sensors, data processing flows, and potential privacy risks while linking them to relevant privacy policy descriptions.

3 CONCLUSION AND FUTURE WORK

We introduce, *PrivacyVis*, a visualization tool designed to address the challenges of understanding privacy risks in IoT devices. Our approach has the potential to bridge the information gap between users and service providers, fostering more informed decisions about privacy in an increasingly connected world. Looking ahead, we plan to expand the scope of *PrivacyVis* by incorporating additional privacy risk factors, such as data sharing with third-party services. We also intend to conduct user studies to evaluate its effectiveness in enhancing user understanding and decision-making regarding the privacy of IoT devices. By integrating user feedback and iteratively refining the design, we aim to enhance the tool's usability and ensure it aligns with the evolving needs of lay users.

REFERENCES

[1] Shiwei Fang, Tamzeed Islam, Sirajum Munir, and Shahriar Nirjon. 2020. Eyefi: Fast human identification through vision and wifi-based trajectory matching. In *2020 16th International Conference on Distributed Computing in Sensor Systems (DCOSS)*. IEEE, 59–68.

[2] Wentao Guo, Jay Rodolitz, and Eleanor Birrell. 2020. Poli-see: An interactive tool for visualizing privacy policies. In *Proceedings of the 19th Workshop on Privacy in the Electronic Society (WPES'20)*. ACM, New York, 57–71.

[3] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W Reeder. 2009. A "nutrition label" for privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS '09)*. ACM, New York, Article 4, 12 pages.

[4] Shijia Pan, Mostafa Mirshekari, Jonathon Fagert, Ceferino Gabriel Ramirez, Albert Jin Chung, Chih Chi Hu, John Paul Shen, Pei Zhang, and Hae Young Noh. 2018. Characterizing human activity induced impulse and slip-pulse excitations through structural vibration. *Journal of Sound and Vibration* 414 (2018), 61–80.

[5] H Jeff Smith, Tamara Dinev, and Heng Xu. 2011. Information privacy research: An interdisciplinary review. *MIS Quarterly* 35, 4 (2011), 989–1015.

[6] Shomir Wilson, Florian Schaub, Frederick Liu, Kanthashree Mysore Sathyendra, Daniel Smullen, Sebastian Zimmeck, Rohan Ramanath, Peter Story, Fei Liu, Norman Sadeh, and Noah A. Smith. 2018. Analyzing privacy policies at scale: From crowdsourcing to automated annotations. *ACM Transactions on the Web (TWEB)* 13, 1, Article 1 (2018), 29 pages.

[7] Yue Zhang, Shangjie Du, Jiqing Wen, Robert Likamwa, Shiwei Fang, and Shijia Pan. 2024. Poster: PrivaSee: Augmented Reality-Enabled Privacy Perception Visualization for Internet of Things. In *Proceedings of the 22nd Annual International Conference on Mobile Systems, Applications and Services*. 694–695.