Protected at home? User mental models of home network privacy and privacy tool coverage beliefs

Michelle McDowell
eyeo GmbH
Max Planck Institute for Human Development
Harding Center for Risk Literacy

Felix Rebitschek
Harding Center for Risk Literacy
Brandenburg Medical School Theodor Fontane
Max Plank Institute for Human Development

Simon Overell
eyeo GmbH

Abstract

The present study explores user mental models of how data flows between multiple users and multiple devices on shared home networks, including user awareness of the entities that can see and connect information and activities, and the privacy implications of cross-device linkage for individuals and other household members. The study also explores how well participants believe they are protected from tracking on their home network and what misconceptions they hold about the coverage of device- or network-level privacy tools. Findings from a qualitative interview and drawing exercise are expected to characterise potential gaps and misconceptions users hold about privacy at home and the extent to which current privacy-regulating behaviours and tool usage match their coverage expectations. Results are anticipated to provide design evidence for network-level privacy tools.

1 Introduction

Paradoxically, the home is a space in which individuals report the strongest subjective sense of privacy and desire for personal control over their data, yet it exposes one of the most information-rich sources of observation available to third parties [17]. In 2015, Kang et al. [5] reported that lay internet users held simple and incomplete mental models about how the internet works and the entities who had access to their personal data and communications. Over 10 years later, the ecosystem has changed markedly. The mechanisms by which users can be tracked, the number of entities involved in data collection, sharing and storage, and the number of devices users now connect to home networks has increased [2,4,7,10]. In addition, cross-device tracking from the interconnection of multiple personal and shared devices on shared networks has privacy implications not only for individuals but other household members.

A recent review of privacy and security issues in home network environments concluded that user perceptions of the more complicated data flows in multi-user homes and the implications of interactions between multiple users and devices is understudied [10]. Most recent work has focused on smart devices, IoT and smart homes more broadly [1, 17], yet the privacy concerns users hold differ by device type (e.g., smart home devices, smartphones) and privacy concerns increase when multiple as opposed to single devices are interconnected [14]. Users express concern about the negative impacts of cross-device tracking on information leakage in other contexts (e.g., online behavioural advertising at work related to home usage) as well as information exposure related to other network members [6, 11, 15].

When it comes to protective actions, there are few accessible network-level privacy tools available to lay users and those that exist can present technical barriers [8,9]. The use of device-level privacy tools and settings is more prevalent, and users report taking a range of privacy-regulating and privacy protection behaviours – even those who report being dismissive about their online privacy [3, 13]. However, misconceptions about the purpose and capabilities of privacy protection tools are widespread [8, 13, 16], and while some users layer or combine tools, their expectations about how they combine to offer enhanced protection is often overestimated, false, or simply undeliverable [13]. Indeed, a greater number of browser extensions may actually *increase* tracking through improved identifiability via browser fingerprinting [12]. Beliefs about the additive protection of multiple device- or network-level privacy tools on individual and shared devices within home networks and in combination with privacy-regulating behaviours has not been explored, particularly in terms of how comprehensively users perceive these actions to cover personal and collective household privacy.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2024.
August 11–13, 2024, Philadelphia, PA, United States.

The present research will fill this gap by idenfiying what users understand about the privacy threats associated with the connection of multiple devices on shared home networks, awareness of the implications for the privacy of individuals and other household members, and perceptions about the capability of privacy protecting tools and behaviours to cover against privacy threats.

1.1 Research Questions

RQ1: What are participants' mental models of how data flows within and out of their home network and the entities that can see their information and activities?
RQ2: What do participants understand about how data is tracked across devices and persons within the home network and what consequences do they perceive for their privacy and that of other household members?
RQ3: How well do participants believe they are protected from tracking on their home network and what misconceptions do they hold about the coverage of device- or network-level privacy tools?
RQ4: What would people expect a privacy solution to cover across their home network?

2 Methodology

Participants. Approximately 20-25 participants who have two or more devices connected to their home WiFi network will be recruited to participate in a semi-structured interview. Of these, at least 12 will report living in a household with more than one person who regularly uses the internet at home and around half will report using at least one privacy product on a personal device (e.g., tracker blocker, DNS filter, browser with built-in privacy protections). The study focuses on US participants because protection from home-network tracking depends largely on users' own knowledge and tool use rather than comprehensive privacy regulations (e.g., GDPR). Recruitment is conducted via Prolific with participants receiving $.10USD for completing a pre-screener to identify eligibility and $17USD for for those who complete the interview. Interviews are expected to be completed by July 2026.

Study design and procedure. Following questions to obtain socio-demographic and background information, participants are asked about their home internet set-up, including the devices they have connected and other household members who use the internet at home. After being given the opportunity to familiarise themselves with the online sketching software Miro, participants are guided through the drawing exercise. Similar to Kang et al. [5], users are first prompted to explain how they think the internet works while at home using their home WiFi network. Subsequent questions ask participants to imagine how information flows, what other entities may be able to see their connections and activities, how other devices they connect at home fit into their model, information flow between devices and how other members of the household fit into their model. Participants are asked if they take any actions to prevent others from seeing their activities, and if so, to explain how this works. Participants are asked to think aloud as they complete the drawing task.

After participants complete the drawing task, they are asked about how they use their devices and what they do to protect their privacy while on their home network. Participants who indicated using privacy protection tools explain how they use their privacy protection tools, on which devices, what they believe these tools protect them from, and their perception of the level of privacy protection these tools offer across their home network as a whole. Participants who do not indicate using any tools are asked for their general perceptions of online privacy at home, and awareness of privacy protection tools. All participants are asked for their perspectives on what privacy protection at home would look like for them.

To identify what users understand about how devices can be linked across a home network, participants are asked for their perspective on how different devices within their home may be perceived by entities outside the home as well as the activities of other members within the household and what that means to them when it comes to their privacy. To conclude the interview, participants are asked to imagine that their home router came with a feature that would protect the privacy of everyone in the household when connected to the home WiFi. Participants are asked to share their expectations of what they would expect that feature to do.

Ethics. Participants consent to the study, including the purpose, usage and storage of audio and visual recordings. Personally identifiable information is anonymised. Approval was obtained from an independent Institutional Review Board.

Data analysis. Qualitative analysis of participants' think-aloud protocols and diagrams follow an inductive process to identify recurring themes and differences across mental models. The process is iterative; an initial analysis codes a sample of the participant transcripts to generate a set of initial codes that is applied and revised based on subsequent transcripts. An independent coder will code a sample of the interviews to establish good inter-coder agreement. We expect to identify the dimensions on which participant's mental models vary, including the entities that they are aware of and gaps in understanding of cross-device linkage on the home network.

3 Anticipated Contribution

The present research is anticipated to expose gaps in user awareness and comprehension of privacy-relevant issues related to connecting multiple devices on shared home networks, an understudied area in user privacy perception research [10]. Results from this study are expected to guide the design and communication of network-level privacy tools to increase user comprehension of the privacy protections that can be achieved across devices on the home network.

References

[1] Noah Apthorpe, Yan Shvartzshnaider, Arunesh Mathur, Dillon Reisman, and Nick Feamster. Discovering Smart Home Internet of Things Privacy Norms Using Contextual Integrity. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 2(2):1–23, July 2018. http://arxiv.org/abs/1805.06031.

[2] Justin Brookman, Phoebe Rouge, Aaron Alva, and Christina Yeung. Cross-Device Tracking: Measurement and Disclosures. *Proceedings on Privacy Enhancing Technologies*, 2017(2):133–148, April 2017. https://petsymposium.org/popets/2017/popets-2017-0020.php.

[3] Jessica Colnago, Lorrie Cranor, and Alessandro Acquisti. Is There a Reverse Privacy Paradox? An Exploratory Analysis of Gaps Between Privacy Perspectives and Privacy-Seeking Behaviors. *Proceedings on Privacy Enhancing Technologies*, 2023(1):455–476, January 2023. https://petsymposium.org/popets/2023/popets-2023-0027.php.

[4] Federal Trade Commission. Cross-Device Tracking: An FTC Staff Report - January 2017. Technical report, January 2017. https://www.ftc.gov/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017.

[5] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. "My data just goes everywhere": User mental models of the internet and implications for privacy and security. In *Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security*, SOUPS '15, pages 39–52, USA, July 2015. USENIX Association. https://www.usenix.org/conference/soups2015/proceedings/presentation/kang.

[6] Predrag Klasnja, Sunny Consolvo, Jaeyeon Jung, Benjamin M. Greenstein, Louis LeGrand, Pauline Powledge, and David Wetherall. "When I am on Wi-Fi, I am fearless": Privacy concerns & practices in everyday Wi-Fi use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '09, pages 1993–2002, New York, NY, USA, April 2009. Association for Computing Machinery. https://dl.acm.org/doi/10.1145/1518701.1519004.

[7] Konrad Kollnig, Anastasia Shuba, Max Van Kleek, Reuben Binns, and Nigel Shadbolt. Goodbye Tracking? Impact of iOS App Tracking Transparency and Privacy Labels. In *2022 ACM Conference on Fairness Accountability and Transparency*, pages 508–520, June 2022. http://arxiv.org/abs/2204.03556.

[8] Maryam Mehrnezhad, Kovila Coopamootoo, and Ehsan Toreini. How Can and Would People Protect From Online Tracking? *Proceedings on Privacy Enhancing Technologies*, 2022(1):105–125, January 2022. https://petsymposium.org/popets/2022/popets-2022-0006.php.

[9] Alexandra Nisenoff, Ranya Sharma, and Nick Feamster. User Awareness and Behaviors Concerning Encrypted DNS Settings in Web Browsers. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 3117–3133, 2023. https://www.usenix.org/conference/usenixsecurity23/presentation/nisenoff-awareness.

[10] Nandita Pattnaik, Shujun Li, and Jason R. C. Nurse. A Survey of User Perspectives on Security and Privacy in a Home Networking Environment. *ACM Comput. Surv.*, 55(9):180:1–180:38, January 2023. https://dl.acm.org/doi/10.1145/3558095.

[11] Sarita Schoenebeck, Cami Goray, and Yasemin Gunal. Algorithmic Self-Diagnosis from Targeted Ads. *Proc. ACM Hum.-Comput. Interact.*, 9(2):CSCW028:1–CSCW028:19, May 2025. https://dl.acm.org/doi/10.1145/3710926.

[12] Oleksii Starov, Pierre Laperdrix, Alexandros Kapravelos, and Nick Nikiforakis. Unnecessarily Identifiable: Quantifying the fingerprintability of browser extensions due to bloat. In *The World Wide Web Conference*, WWW '19, pages 3244–3250, New York, NY, USA, May 2019. Association for Computing Machinery. https://dl.acm.org/doi/10.1145/3308558.3313458.

[13] Peter Story, Daniel Smullen, Yaxing Yao, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. Awareness, Adoption, and Misconceptions of Web Privacy Tools. *Proceedings on Privacy Enhancing Technologies*, 2021(3):308–333, July 2021. https://petsymposium.org/popets/2021/popets-2021-0049.php.

[14] Maximiliane Windl, https://orcid.org/0000-0002-9743-3819, View Profile, Magdalena Schlegel, https://orcid.org/0009-0003-5615-8173, View Profile, Sven Mayer, https://orcid.org/0000-0001-5462-8782, and View Profile. Exploring Users' Mental Models and Privacy Concerns During Interconnected Interactions. *Proceedings of the ACM on Human-Computer Interaction*, 8(MHCI):1–23, September 2024. https://acm-stag.literatumonline.com/doi/abs/10.1145/3676504.

[15] Yuxi Wu, Sydney Bice, W. Keith Edwards, and Sauvik Das. The Slow Violence of Surveillance Capitalism: How Online Behavioral Advertising Harms People. In *2023 ACM Conference on Fairness Accountability and Transparency*, pages 1826–1837, Chicago IL USA, June

2023. ACM. https://dl.acm.org/doi/10.1145/3593013.3594119.

[16] Yuxi Wu, Panya Gupta, Miranda Wei, Yasemin Acar, Sascha Fahl, and Blase Ur. Your Secrets Are Safe: How Browsers' Explanations Impact Misconceptions About Private Browsing Mode. In *Proceedings of the 2018 World Wide Web Conference*, WWW '18, pages 217–226, Republic and Canton of Geneva, CHE, April 2018. International World Wide Web Conferences Steering Committee. https://dl.acm.org/doi/10.1145/3178876.3186088.

[17] Shuning Zhang, Shixuan Li, Haobin Xing, Jiarui Liu, Yan Kong, Xin Yi, Kanye Ye Wang, and Hewu Li. "Privacy across the boundary": Examining Perceived Privacy Risk Across Data Transmission and Sharing Ranges of Smart Home Personal Assistants. In *Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems*, CHI '26, pages 1–26, New York, NY, USA, April 2026. Association for Computing Machinery. https://dl.acm.org/doi/10.1145/3772318.3790455.