Giving Form to the Invisible: Can we make in-home network data traffic tangible to users?

Junginger Sabine[1], Tödtli Beat[2], Ulmer Tom[3]

[1]Lucerne University of Applied Sciences and Art, [2]Eastern Switzerland University of Applied Sciences, [3]Eastern Switzerland University of Applied Sciences

Sabine.junginger@hslu.ch
Beat.toedtli@ost.ch
Tom.ulmer@ost.ch

Abstract. Most people now connect to the Internet of Things (IoT) through a number of devices within the privacy of their homes. The data traffic generated by smart home and other connected devices remains invisible and intangible to everyday users. Is it possible to make these complex data flows somehow visible, and with that also accessible and graspable for users? Is there a path for everyday users to participate in desirable future developments, meaningful services, and relevant policies? If so, how do we go about conducting such user research? In this paper, we report and reflect on an experimental study conducted by an interdisciplinary research team with these questions in mind. We explore the possibilities and limitations of a non-intrusive, plug & play network monitoring device. Our findings point to opportunities for empowering participants in sensitive environments like the home and produce insights into how designers may collaborate with researchers in data analysis to make the invisible visible.

Keywords: User research, smart home, designing in the digital age, data visualization, user empowerment

1 Introduction and Background

For most people, the potential opportunity to participate in the evolution of the digital technologies and AI services they use in the privacy of their homes stretches beyond a strong interaction between designers and customers. The aim of designers here can no longer be to merely 'mine invaluable sources of information'. Rather, it is increasingly a task for designers to make the invisible visible and to make concepts graspable, so that users can engage in the discussions and developments, thereby giving them a voice in how, where, when and why products and services based on these technologies benefit them. But how might designers trained in products and services, but in hardly any of the new technologies, fill this role, or even approach the task? We provide an example of collaboration among designers, computer scientists and network data analysts looking to make an in-home data network accessible to users.

More and more people are installing smart devices in the sanctity of their homes, effectively connecting them to the IoT and exposing them to new vulnerabilities [1, 2, 3]. Most of the data-gathering activities of devices remain largely undetected by their users. Researchers have established that end users lack mental models when it comes to new IoT technologies, and so may fail to grasp their complexities and the attendant risks to privacy and security. Absent mental models, what do people make of the many devices they have in their homes? How may we arrive

at user-friendly, easy-to-use, and meaningful ways for non-expert users to learn about the network traffic in their homes? What would products and services that enable them to monitor and interpret in-home data traffic look like [2, 4]? How could we support them in taking deliberate actions and making informed decisions about their data sharing?

The quest for such products and services poses new demands and challenges because such user research depends on a combination of technical, quantitative, and qualitative methods. The user perspective so far has not received much attention. Answers to date involve elaborate, lab-like set ups in users' homes that constitute major intrusions of living spaces [4] and are highly impracticable. Most are so complicated as to limit studies to a few households and participants who are technically sophisticated [4, 5]. These studies have proven significant and insightful but have done little to explore what kind of information may be helpful to everyday users or how such information could be made available to lay people within the (data) confines of their homes. Furthermore, they cannot be scaled-up or replicated easily as they are costly. This paper reports on a pilot study that experimented with a non-intrusive, scalable approach to the capture of in-home data traffic.

1.1 Background

A recent review on definitions of the smart home by Marikyan, Papagiannidis & Alamanos [6] explains that the term 'smart home' is reserved for homes equipped with 'smart devices and sensors that are integrated into an intelligent system, offering management, monitoring, support, and responsive services and embracing a range of economic, social, health-related, emotional, sustainability and security benefits.' Such definitions may mislead users to assume they only need to be concerned about security and privacy risks in their homes if they consciously install advanced smart home devices such as, for example, voice assistants [6, 7, 8]. Given the range of 'smart' sensing and networking devices available today, almost any home network may require a certain degree of control and transparency over the data exchanged in- and outside this network [7, 9]. Lacking an awareness of vulnerabilities, users have even fewer opportunities to mitigate potential risks. The only way to learn about the presence of vulnerabilities is to make them visible in one way or another. Therefore, studies into user awareness of security and privacy risks must account for data traffic generated by an increasing number of sensing 'non-smart' home devices.

Efforts at providing users with the means to monitor their in-home data streams have focused on traffic generated by 'smart home devices' [10] in 'smart homes' [11]. Beyond specifically labelled smart home devices, most modern electronic devices can be equipped with additional functions for recording, receiving, and sending data. While some data needs to be protected from external access, meta-data on data collection and communication activities of home network devices should be available to the home network users in a transparent way. Ideally, users should be enabled to make informed decisions and take deliberate actions to adjust their own network traffic to their own privacy and security preferences. Ideally, information on their in-home data flow should be available in real-time so they can control which data their in-home network will share with specific providers and app services. But as the example of the GDPR shows, it is simply impractical for users to monitor every device activity, i.e., every refrigerator and every toaster. In theory, GDPR provides autonomy and control over data to users. In reality, most people give up on de-selecting the seemingly endless list of permission requests [12, 13].

Conducting research into people's homes and now into in-home networks and data traffic poses new ethical challenges as these are clearly highly sensitive research settings [16, 17]. Such settings even challenge our notion of 'vulnerable' research participants, as those who participate are inevitably becoming vulnerable, sometimes without realizing it until very late in the process. As one participant in this Network Traffic Analysis shared with us: "I realize now that it would be so easy for someone to access my system under the pretense of research." The participant emphasized that having been part of the initial in-home study for our project was a factor for allowing the research team to pursue follow-up studies.[1]

Current (in-) home network architectures are optimized for security, efficiency, and flexibility, but not for transparency of data traffic for users. Instead, these objectives often conflict with each other [10]. To change this, data needs to be gathered in an unobtrusive way and aggregated into meaningful information that users can act on. But even to get to the necessary insights poses new challenges for researchers: participants differ in age and technological enthusiasm and trust while the focus, by default, remains on technically literate users who can cope with elaborate lab-like arrangements in their homes for study purposes.

The issue of data legibility is related to but not identical to the challenge of making the intangible tangible and the invisible visible in a way that is meaningful and actionable to non-experts so they can become aware, make informed decisions, and take deliberate actions to minimize their privacy and security risks [10, 11]. Data visualization for users has gained new urgency [16] but presents new challenges. Though data visualizations have changed over time [17, 18], the needs of everyday users have yet to be addressed and considered in information visualizations of Big Data [16, 19].

There is a need for new methods to conduct research in the privacy of the home in ways that are less intrusive and reduce exposure of their data, their homes and their networks. Users also should also not need to adjust their everyday routines and practices around physical technical equipment and its requirements. In this context, limiting research to meta-data presents a way to maintain a high level of user privacy during ongoing research. But few users understand what meta-data is or can reveal. Users, in fact, continue to be treated more like subjects in these studies, with only a few benefitting directly from their participation. The question remains what kind of methods are suitable for researchers and users.

When looking at the IoT from the user perspective, these questions emerge:

> *Who tells me that the algorithms for filtering potentially sensitive devices ("design IoT Inspector such that it does not upload any traffic from devices that show signs of being general-purpose computing devices") really work?*
>
> *Maybe I have a different opinion than the algorithm. What is sensitive for the programmer (the project manager/designer/developer) and what for me?*
>
> *If I can then delete my data on a server (remotely) afterwards because they are too sensitive for me, then they have already been transferred and stored on a drive. I have to trust that, for example, if the data is backed up, the backups will*

[1] For more on this follow-up project see: Shorter et al (forthcoming). Lifting the Bonnet on Voice Recognition Technology: Designing the WordCloud, *Designing Interactive Systems Conference* (DIS) 2023.

also be deleted. How is it deleted? Permanent and irreversible (data shredder) or is it just a "deleted" flag set?

I can't control who has access (or had before deleting it). Even if the architecture is broken down completely transparently (if I can remember that), I have to trust the setup.

Due to the great public attention, such projects are always interesting for hackers. What if someone gained unauthorized access or exploited a vulnerability in the architecture and was able to sniff the traffic (without the knowledge of the project team)?

We investigated (1) how to design a plug & play, user-friendly and self-installable data traffic monitoring device; (2) how might a minimally invasive/unobtrusive research approach to reduce the security and privacy risks to participants be conducted; (3) how can we visualize the data captured for users (i.e., non-experts) and make it understandable to them and (4) what insights into privacy and security issues can we gain from a user's perspective by presenting our findings to them employing semi-structured interviews. The study took place during the COVID-19 pandemic and the ability to capture network traffic remotely and without a physical visit turned out to be essential. It was further designed to be minimally intrusive to monitor users' in-home data traffic. We made use of Raspberry Pi 4 devices, compact full-fledged single-board computers, that were configured as network sniffing devices. Our requirements echo those established by DiCioccio et al [20]:

a. Ease of Use: In our case, the tool had to be simple to install, run and de-install by non-experts.
b. Portability: In our case, the tool needed to run on all home networks (WLAN and Ethernet).
c. Respect Users' Privacy: In our case, the sniffing tool does not collect any identifiable information, no data is transferred over the internet, no data is uploaded to an external server.
d. Light User Commitment: In our case, the installation, configuration, running, de-installation and returning of the device and its components had to be done in little time without drawing on the users' resources. The objective was to provide a plug & play experience.
e. Incentive for Participation: In our case, user incentives were to learn about what one can see and infer from the data traffic in their home networks and to receive a visualization and explanation from experts on their personal network data.

Method and Approach

To minimize risks of privacy and security for our participants, we opted to store data only locally and to require no personal contact or cloud storage. The approach is one where data is (securely) deleted after local processing. For this reason, we experimented with a remote and non-intrusive set-up.

Our participants self-installed a monitoring/recording device we had prepared and mailed to them together with an illustrated step-by step instruction. There was no change to their living environment. The data sniffing device then recorded the participant's home network traffic for one week and recorded it locally before participants de-installed the device following another step-by-

step set of instructions. The recordings were stored locally on the device without the need for personal contact or sending or storing them in a cloud that could be hacked or accessed by third parties. They then returned their device to the research team in a prepared, pre-stamped and pre-addressed return box. We produced individual charts for each home network as well as a comparison chart with the other participants home networks. From this, we were able to produce insights into individual participants' in-home network data traffic, which we were able to compare and contrast with that of other participants. All data and participants' information were anonymized and recordings were deleted after analysis. Next, we developed a semi-structured interview around our findings for their home using PowerPoint slides. We invited participants to meet with us individually online to share and discuss our findings with them, prompting participants first to estimate what the recordings would reveal about their in-home data network traffic. We recorded their answers before we shared with them the actual data we captured for their home. We chose this approach to get a better understanding of how aware people are of the connected activities in their homes.

This network data traffic study was embedded within a larger study into the user experience of voice assistants in the home, which was conducted with 31 Swiss-German households. Of those, 16 households consented to join the network traffic study. However, four of our participants experienced technical difficulties and one withdrew, allowing us to collect data from eleven households (of the remaining participants three were male, nine female).[2] Prior to the in-home study, participants were asked to rank their technology expertise on a scale from 1 to 6, where 1 stood for "I am a novice to digital technologies" and 6 stood for "I am an expert, no one fools me." The majority considered themselves as knowledgeable to very knowledgeable (Table 1). Participants were not compensated for this part of our study, which was approved by our university's Internal Review Board. Participants also had to inform and get consent from members in their household, as in-home studies involve everyone in a home. We tested the technical set-up as well as the visualization and presentation of the captured data with two people who were not involved in any part of the study and were non-experts.

Table 1. Participants in the study.

Male Participants	Technical Self Assessment on 1-6 Scale	Participated in Power Point semi-structured interview	Female Participants	Technical Self Assessment on 1-6 Scale	Participated in Power Point semi-structured interview
M1	5	no	F1	2	no
M2	**4***	**YES***	F2	2	no

[2] In one household, two people signed up independently; that is how the number adds up to 12 participants.

Male Participants	Technical Self Assessment on 1-6 Scale	Participated in Power Point semi-structured interview	Female Participants	Technical Self Assessment on 1-6 Scale	Participated in Power Point semi-structured interview
M3	**5**	**YES**	F3	6	no
M4	5	no	F4	**5***	**YES***
M5	**5**	**YES**	F5	5	no
M6	withdrew	no	F6	3	no
M7	6	no	F7	4	no
M8	5	no	F8	5	no
Total 8			**Total 8**		

* M2 and F4 shared a household. They did not install the mini-computer but were interested in learning about the general findings. (Data from VA-PEPR).

Key Findings

Our findings go beyond those we mention here. We present here a summary only of those most relevant to the DesForm Community and its conference theme. Overall, the understanding of basic concepts of networks such as ports and packages was low even for people who judged themselves to be experts. In contrast, the forms of visualizations we chose (such as chord diagrams, bar charts, time series or histograms (see Figure 1 & 2 as an example) were intuitively clear.

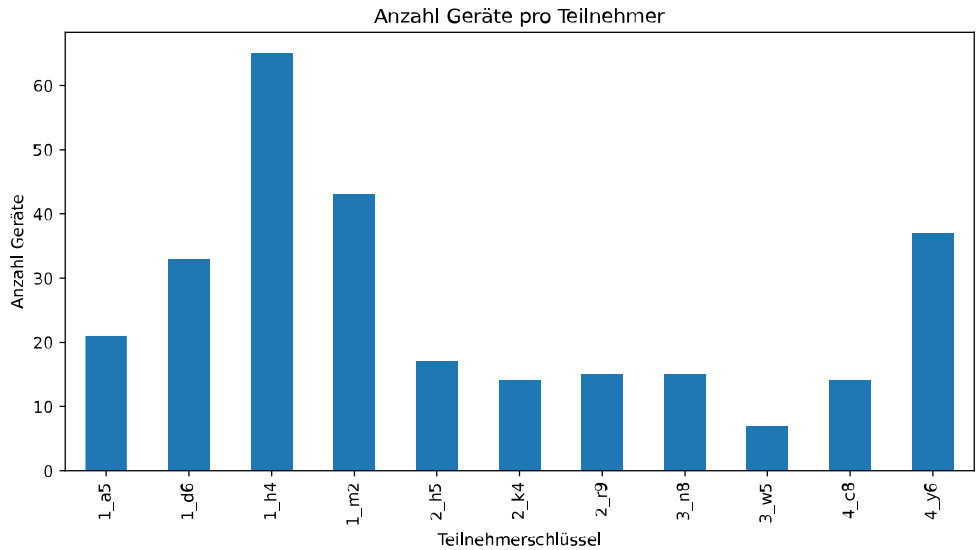

Fig. 1. Number of devices per household for each of the eleven participants: Do I have more or fewer than other participants? (Source: VA PEPR).

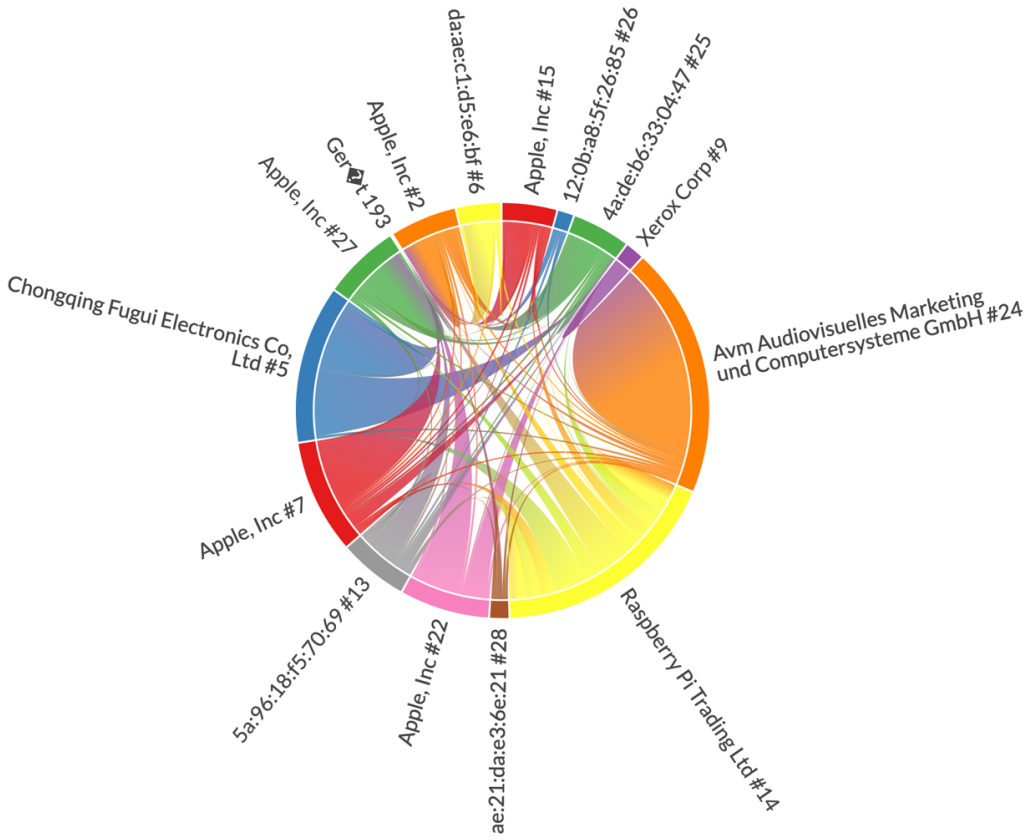

Fig. 2. What devices in your home are sending and receiving – from where to where? (Source: VA PEPR).

Users are looking for comparisons with others: Participants asked for cross-participant visualizations because they felt that this allowed them to compare their own household with others. Lacking mental models and any understanding of what 'normal' behavior is, the participants had trouble interpreting and judging the absolute values we presented for their in-home network (e.g., the number of open ports per device or network activity). It emerged that concepts relative to other households were significantly more intuitive than the absolute numbers. (See Fig.3 as an example). A wish for a clear point of orientation was noticeable. Immediate questions that arose were often of the type "Is it good or bad that I have less (or more) of ... than the others?"

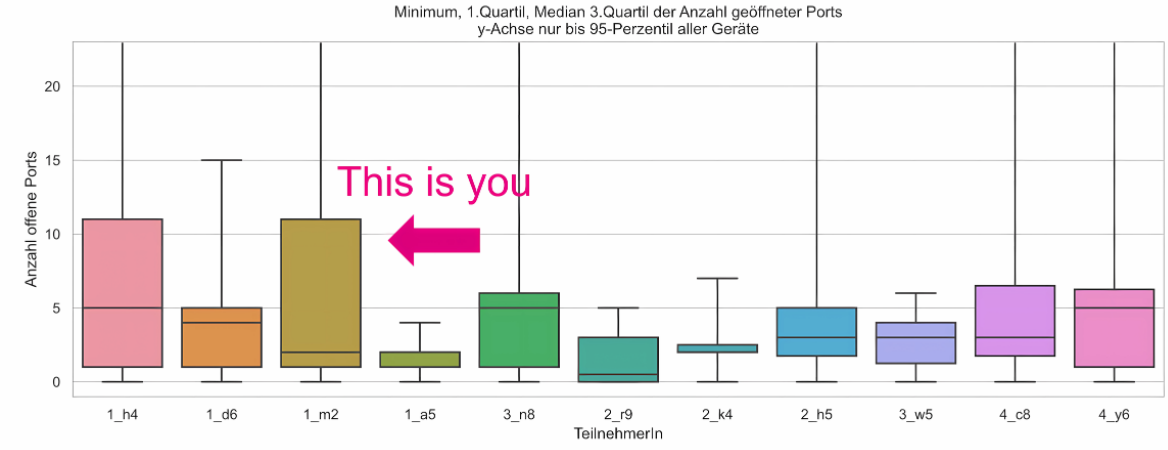

Fig. 3. How many open ports does your household have in comparison to other participants? Participants found it helpful to compare their situation with that of others (Source: VA PEPR).

Though we could not answer these questions in a definite fashion, it underlined the value of such visualizations when the goal is to enable users to frame questions around their own home network and the attendant privacy and security risks. This aligns with the study by Krsek et al. [21], which explored the social influence personal and non-personal on the behavior of users in best practices around security and privacy. They suggest that the difficulty of gathering the meta-data that is needed to show end-users personalized peer recommendations might be overcome by deploying non-personal social influence suggestions into 'existing or fabricated privacy setting interfaces.'

Our interviewees struggled to account for all the devices in their home networks the data sniffer picked up. They had either under- or over-estimated the number of devices, by 30-50%. In our view, this is linked with the concepts users have of a smart home as outlined by Marikyan et al [6]. Once they sat down with us, they realized that their children's iPads and the phones used by guests logging into the home network were all part of it, too. Unlike Huang et al. [4] who consciously excluded some devices in the home out of concern for abuse and ethical violations, we think that users need to be able to account for all the devices in their home network. This would give all household members a much better picture of their privacy and security risks. Homes are co-lived, co-shared and co-worked in, they are the best places for open data. Yet, the social aspects of the smart home have not found their way into services and applications yet. Applications are still built around one-user, one-password per account. Our study shows that everyone (or at least every adult) in a home should have the ability to see all the devices in the network to have a chance at transparency. This may require a rethinking along with new technological and regulative approaches.

Discussion

Our findings indicate that there is no normal for users when it comes to their in-home traffic. Yet, they are eager to understand what a normal network state is in terms of their usage of data, data traffic flows, number of connected devices, and risks they take with respect to their privacy and security. When we were able to present the findings for an individual household, the bars, levels, and numbers meant little to our participants until we were able to show them how they compared to the other 10 participants in the study. This points to an opportunity for home networking providers to improve their products by providing users with such orientation and baselines.

When participants were able to see visualizations of their own network traffic – the number of devices they had in their homes versus those of others; the level of data traffic activities; the days their data networks and/or individual devices were most active; the actual devices (i.e., partner's iPhone; Airbnb guest's phone) that contributed to their data traffic; the open ports of their devices, etc. they started to ask questions and reflected on their in-home networks. They affirmed our hypothesis that when we make the invisible visible, we provide people with the means to engage in the conversation around these new technologies. This outcome resulted despite our admittedly clumsy and rather basic visualizations. We consider it a key challenge for the DesForm Community to engage in further research and development of user-friendly, appropriate visualizations that consider the human experience. At this point, no such visualizations exist, or at least are not readily or easily available to non-expert users.

Data collection needed only a minimal support effort, and where we received any data, it was mostly complete and extending over the full data-gathering period. This indicates that our

single-board computer might scale well to tens of participants. Most of the participants did not experience any technical difficulties with our single-board computer and the self-installation procedure, but we did not receive data from 4 out of 11 participants. We do not know if these four tried the installation but were not able to provide data, or if they simply were no longer willing to share. We will follow up on this. The research team was able to reduce exposure risks of participants to privacy and security during this research by avoiding any 'middling' technology, i.e., external server, or internet transfer.

Conclusion

As reported above, research into user homes and home network data inevitably involve sensitive research settings. We run into the issue of privacy in the home because making network traffic transparent possibly exposes people in a household to different privacy risks. Our effort to test the potential for a remote and non-intrusive plug-and-play data monitoring solution still generated ethical questions. In these sensitive settings, new methods are needed to generate relevant and meaningful information for users who ultimately need to be able to assess and manage their privacy and security risks. One challenge we find emerging here is the tension that arises in the hands-off approach by researchers that leaves participants in control of their data and insists of a non-intrusive research method. The method entails participants never even meeting the researchers in person (though they are in contact online, via Messenger app and email) and it is difficult to engage users in such a way as to enable them to contribute to future desirable outcomes for their home networks. In the latter, participants take on a more active role and that role in turn requires closer engagement with the researchers, possibly limiting the ability to be non-intrusive.

Our approach and methods depended on interdisciplinary collaboration. We would not have been able to conduct this experiment within any one of our disciplines and depended on this collaboration that brought together data analytics, network analysis and human-centered design. Our methods allowed us to get a basic understanding of how home network users think of their data streams. We found that from a user's perspective, an analytical approach is not sufficient to explore the possibilities and opportunities for how users may engage in security and privacy risk assessment and risk management. Instead, a more cultural approach is needed [22, 23]. Here, we see a greater role for speculative design and the use of *provotypes* as methods to explore meaningful and user-friendly monitoring solutions [24, 25]. These may also be able to point to alternative business models to those that exist today. Research into smart home devices – which are more like consumer products – has embraced methods of co-designing [11]. But so far, few studies into the privacy and security risks of home networks and home network traffic involve such methods. This, we argue, is also owing to the fact that the design and computer-human-interaction research communities are not yet collaborating often enough. Users tend to be at a loss when confronted with data visualizations (of packets and ports) generated from the transport layer. We are still lacking suitable truly informative visualizations for the non-technically, non-data inclined. We did not have enough time in our project to get to these. Nevertheless, discussions with users about privacy, data protection and device activities were easily initiated based on our data presentation. We are thus encouraged and not as pessimistic as Forget et al. about engaging users [27].

6 Limitations of the Study

As pointed out by DiCioccio et al. (2013), it is difficult to get representative results from a few homes. Our participants were also part of a voice assistant study and smart speakers may have different preferences and attitudes to privacy [20]. Nonetheless, with eleven participating households, we have begun to identify measurement points inside the homes that are meaningful to home network owners and users. And with only three completed semi-structured interviews, the findings must remain preliminary. Nonetheless, we were still able to get thick data [26] and with that, glean important insights relevant to privacy and security issues from a user perspective. An important factor was that the one-week data network analysis was embedded within a four-week ethnographic in-home-study, which was also conducted remotely.

Acknowledgments

The research results presented in this paper are part of a project funded by Swiss National Science Foundation (http://dx.doi.org/10.13039/501100001711) under grant number SINERGIA CRSII5 189955. Special thanks go to Aurelio Todisco and Michelle Murri from the VA PEPR Team, whose logistical and personal support of participants contributed to the in-home study and network data analysis. Finally, we are grateful for the feedback received from the anonymous DesForm reviewers.

References

1. N. Apthorpe, D. Y. Huang, D. Reisman, A. Narayanan, and N. Feamster. Keeping the Smart Home Private with Smart(er) IoT Traffic Shaping. In Proceedings on Privacy Enhancing Technologies Symposium (PETS), 2019.

2. Dudhe, P. V., Kadam, N. V., Hushangabade, R. M., & Deshmukh, M. S. Internet of Things (IOT): An overview and its applications. In *2017 International conference on energy, communication, data analytics and soft computing (ICECDS)* pages 2650{2653. IEEE, 2017.

3. https://www.cbc.ca/news/science/pringle-smart-home-privacy-1.5109347.

4. Danny Yuxing Huang, Noah Apthorpe, Frank Li, Gunes Acar, and Nick Feamster. IoT Inspector: Crowdsourcing Labeled Network Traffic from Smart Home Devices at Scale. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. 4, 2, Article 46 (June 2020), 21 pages. https://doi.org/10.1145/3397333.

5. Seymour, W., Kraemer, M.J., Binns, R. and Van Kleek, M. (2020). 'Informing the Design of Privacy-Empowering Tools for the Connected Home', In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. Association for Computing Machinery, New York, NY, USA, 1–14. Retrieved February 10, 2023, from https://doi.org/10.1145/3313831.3376264.

6. Marikyan, D., Papagiannidis, S., Alamanos, E. (2019). 'A systematic review of the smart home literature: A user perspective,' Technological Forecasting and Social Change, Volume 138, 2019. Pages 139-154, https://doi.org/10.1016/j.techfore.2018.08.015.

7. Liao, Y.; Vitak, J.; Kumar, P.; Zimmer, M.; Kritikos, K. (2019). ‚Understanding the Role of Privacy and Trust in Intelligent Personal Assistant Adoption', Proceedings, Information in Contemporary Society, 2019.

8. Angelini M., Catarci T., Mecella M., Santucci G. (2018) The Visual Side of the Data. In: Flesca S., Greco S., Masciari E., Saccà D. (eds) A Comprehensive Guide Through the Italian Database Research Over the Last 25 Years. Studies in Big Data, vol 31. Springer, Cham. Retrieved Feburary 10, 2022 from https://doi.org/10.1007/978-3-319-61893-7_1.

9. Radhika Garg and Hua Cui. 2022. Social Contexts, Agency, and Conflicts: Exploring Critical Aspects of Design for Future Smart Home Technologies. ACM Trans. Comput.- Hum. Interact. 29, 2, Article 11 (April 2022), 30 pages. DOI:https://doi.org/10.1145/3485058.

10. C. Pappas, T. Lee, R. M. Reischuk, P. Szalachowski and A. Perrig, "Network Transparency for Better Internet Security," in *IEEE/ACM Transactions on Networking, vol. 27, no. 5*, pp. 2028-2042, Oct. 2019, doi: 10.1109/TNET.2019.2937132.

11. Tabassum, M.; Kosiński, T.; Frik, A.; Malkin, N.; Wijesekera, P.l; Egelman, S.; Lipford, H. R. (2019). ‚Investigating Users' Preferences and Expectations for Always-Listening Voice Assistants', *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 2019*.

12. Oksana Kulyk, Nina Gerber, Annika Hilt, Melanie Volkamer, Has the GDPR hype affected users' reaction to cookie disclaimers?, Journal of Cybersecurity, Volume 6, Issue 1, 2020, tyaa022, https://doi.org/10.1093/cybsec/tyaa022.

13. Froomkin, A. Michael and Arencibia, Phillip J. and Colangelo, Zak, Safety as Privacy (January 30, 2022). Available at SSRN: https://ssrn.com/abstract=4021420 or http://dx. doi.org/10.2139/ssrn.4021420.

14. Jenny Waycott, Greg Wadley, Stefan Schutt, Arthur Stabolidis, and Reeva Lederman. 2015. The Challenge of Technology Research in Sensitive Settings: Case Studies in 'Sensitive HCI'. In *Proceedings of the Annual Meeting of the Australian Special Interest Group for Computer Human Interaction (OzCHI '15).* Association for Computing Machinery, New York, NY, USA, 240–249. DOI:https://doi.org/10.1145/2838739.2838773.

15. Jenny Waycott, Hilary Davis, Anja Thieme, Stacy Branham, John Vines, and Cosmin Munteanu. 2015. Ethical Encounters in HCI: Research in Sensitive Settings. In *Proceedings of the 33rd Annual ACM*

Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA '15). Association for Computing Machinery, New York, NY, USA, 2369–2372. DOI:https://doi.org/10.1145/2702613.2702655.

16. T. Catarci, M.F. Costabile, S. Levialdi, C. Batini, Visual query systems for databases: a survey. *J. Vis. Lang. Comput. 8 (2),* 215–260 (1997).

17. Angelini M., Catarci T., Mecella M., Santucci G. (2018) The Visual Side of the Data. In: Flesca S., Greco S., Masciari E., Saccà D. (eds) A Comprehensive Guide Through the Italian Database Research Over the Last 25 Years. Studies in Big Data, vol 31. Springer, Cham. Retrieved Feburary 10, 2022 from https://doi.org/10.1007/978-3-319-61893-7_1.

18. Grover, S., Park, M.S., Sundaresan, S., Burnett, S., Kim, H., and Nick Feamster (2013). Peeking Behind the NAT: An Empirical Study of Home Networks, IMC'13, October 23–25, 2013, Barcelona, Spain. Retrieved February 10, 2023 from http://dx.doi.org/10.1145/2504730.2504736.

19. Perkhofer, L.M., Hofer, P., Walchshofer, C., Plank, T. and Jetter, H.-C. (2019), "Interactive visualization of big data in the field of accounting: A survey of current practice and potential barriers for adoption", Journal of Applied Accounting Research, Vol. 20 No. 4, pp. 497-525. https://doi.org/10.1108/JAAR-10-2017-0114.

20. Lucas DiCioccio, Renata Teixeira, and Catherine Rosenberg. 2013. Measuring home networks with homenet profiler. In Proceedings off the 14th international conference on Passice and Active Measurement (PAM'13). Springer-Verlag Berlin, Heidelberg, 176-186. Httpas://doi.org/10.1007/978-3-642-36516-4_18.

21. Krsek, Isadora, Kimi Wenzel, Sauvik Das, Jason I. Hong, and Laura Dabbish. "To Self-Persuade or Be Persuaded: Examining Interventions for Users' Privacy Setting Selection." In CHI Conference on Human Factors in Computing Systems, 1–17. New Orleans LA USA: ACM, 2022. https://doi.org/10.1145/3491102.3502009.

22. Radhika Garg and Hua Cui. 2022. Social Contexts, Agency, and Conflicts: Exploring Critical Aspects of Design for Future Smart Home Technologies. ACM Trans. Comput.- Hum. Interact. 29, 2, Article 11 (April 2022), 30 pages. DOI:https://doi.org/10.1145/3485058.

23. S. Rayner and R. Cantor. How fair is safe enough? the cultural approach to societal technology choice. Risk analysis, 7(1):3{9, 1987.

24. Sanders, L. (1992). 'Converging Perspectives: Product Development for the 1990s', Design Management Journal, Fall 1992: 49-54.

25. https://www.forbes.com/sites/forbesfinancecouncil/2017/10/ 19/on-building-a-faster-horse-design-thinking-for- disruption/, accessed February 10, 2022. https://foundation.mozilla.org/en/insights/privacy-included/, accessed February 10, 2023.

26. Geertz C. Thick description: The interpretation of cultures *The Interpretation of Cultures*. London: Harper Collins; 1973:3–1.

27. A. Forget, S. Pearman, J. Thomas, A. Acquisti, N. Christin, L. F. Cranor, S. Egelman, M. Harbach, and R. Telang. Do or do not, there is no try: user engagement may not improve security outcomes. In Twelfth Symposium on Usable Privacy and Security (SOUPS 2016), pages 97{111, 2016}.