PriCheck– An Online Privacy Assistant for Smart Device Purchases

Vera Volk
LMU Munich
Munich, Germany
veravolk.post@gmail.com

Sarah Prange
University of the Bundeswehr Munich
LMU Munich
Munich, Germany
sarah.prange@unibw.de

Florian Alt
University of the Bundeswehr Munich
Munich, Germany
florian.alt@unibw.de

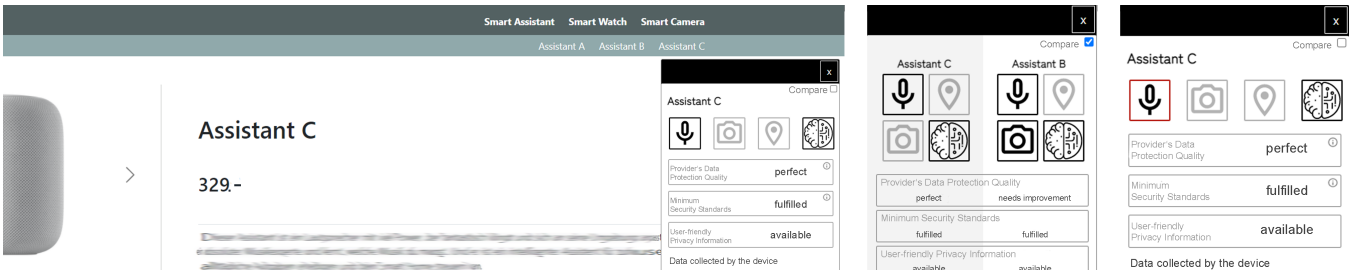

Figure 1: We present *PriCheck*, a browser extension with privacy-relevant information on smart devices (here: in an online shop). With *PriCheck*, users can learn about, e.g., built-in sensors and data collected by the device, and data policies. It also allows for comparison of two devices with each other, or with personal, preconfigured preferences. *PriCheck* supports informed purchase decisions for privacy preserving products.

ABSTRACT

In this paper, we present *PriCheck*, a browser extension that provides privacy-relevant information about smart devices (e.g., in an online shop). This information is oftentimes hidden, difficult to access, and, thus, often neglected when buying a new device. With *PriCheck*, we enable users to make informed purchase decisions. We conducted an exploratory study using the browser extension in a simplified (mock) online shop for smart devices. Participants chose devices with and without using the extension. We found that participants ($N = 11$) appreciated the usability and available information of *PriCheck*, helping them with informed decisions for privacy-preserving products. We hope our work will stimulate further discussion on how to make privacy information for novel products available, understandable, and easy to access for users.

CCS CONCEPTS

• **Security and privacy** → **Usability in security and privacy**; • **Human-centered computing** → *User studies.*

KEYWORDS

usable security, privacy, browser extension, smart devices

CHI '22 Extended Abstracts, April 29-May 5, 2022, New Orleans, LA, USA

ACM ISBN 978-1-4503-9156-6/22/04…$15.00
https://doi.org/10.1145/3491101.3519827

ACM Reference Format:
Vera Volk, Sarah Prange, and Florian Alt. 2022. *PriCheck*– An Online Privacy Assistant for Smart Device Purchases. In *CHI Conference on Human Factors in Computing Systems Extended Abstracts (CHI '22 Extended Abstracts), April 29-May 5, 2022, New Orleans, LA, USA.* ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3491101.3519827

1 INTRODUCTION

A growing number of smart devices is available on the consumer market. These devices can usually act *autonomous*, are *connected* to other devices and the Internet, and are *context-aware*, i.e. they can collect information about their environment through sensors [21]. While these features can serve a variety of application areas and provide great benefits to users (cf. [16] for an overview), they need to collect a plethora of data which can violate users' privacy, especially if they are unaware of whether and which data is being collected, and how it is processed. To allow users to protect their privacy, it is crucial to make them *aware* of data collection by smart devices [17] and how well this data is protected. This information is relevant in many scenarios (e.g., visiting a foreign smart home [20]), but should especially be available to inform users' *purchase decisions.*

We address this need for easy access to information with *PriCheck*, a browser extension that can be used, e.g. in an online shop (cf. Figure 1). *PriCheck* provides a summary of privacy-relevant information to users so they can make informed purchase decisions and/or reconsider how, where and when to use the device. It also allows to directly compare the information across different devices as well as with personal preferences. In this paper, we present the functionalities and information of *PriCheck*. We conducted an exploratory study ($N = 11$) using a mock online shop with a set of typical smart home devices (e.g., smart speakers). Participants of our study were to choose devices with and without using the

extension following the think aloud method. We complemented the evaluation with semi-structured interviews and questionnaires. In this study, we investigated the following research questions:

> **RQ1 General Experience:** How do users use and perceive *PriCheck*?
> **RQ2 Decision Support:** Can *PriCheck* support users in their choice for privacy-preserving products?

We found that participants appreciated the usability and clear information of *PriCheck*. The comparison function facilitated participants' decision in favor of data protection and privacy. Based on our exploration, we discuss directions for future work and open challenges. We hope this work to inspire further research around how to make privacy-relevant information easy to use, understandable, and accessible to users in relevant moments.

2 BACKGROUND & RELATED WORK

Data collection is increasingly present in our daily lives. However, many users are unaware of this, which puts their privacy at risk and prevents them from acting according to their privacy needs [17]. Privacy notices are a common means to increase users' awareness and inform them about data policies, however these are not sufficient [5]. Especially in times with data collection being ubiquitously present, there is a need to rethink how to inform users. Prior research made several suggestions to make privacy-relevant information more accessible. One idea is to design policies to be more attractive and, hence, more understandable to users [14]. Many other approaches summarize privacy information to only display the core aspects. Examples include the privacy label [7, 13, 19], which is placed on device's packaging and mandatory in, e.g., the UK[1] and Singapore[2]. However, the device packaging is not always available to users (e.g., when shopping online). Other approaches such as *PriView* [20] or *PARA* [1] display privacy information on smart devices in users' vicinity in-situ by means of augmented reality. However, these approaches mainly target devices already being installed rather than the purchase decision. An example of a browser extension designed to help users protect their data online is the *Privacy Bird* [6]. The extension compares websites' privacy policies to users' personal privacy preferences and notifies them in case these are violated.

With *PriCheck*, we combine the ideas of accessible privacy information (e.g., in the form of a label) and put it into an online context (e.g., shopping), to foster informed purchase decisions. We used the Mozilla Foundation's **privacy not included* online guide[3] as source for information about devices that can be displayed in the browser extension. In this work, we present a prototype implementation and explore users' perceptions towards this idea.

3 IMPLEMENTATION

PriCheck is an extension for the Chrome web browser. It is implemented in Vanilla Javascript to ensure high compatibility. The information popup (cf. Figure 1) is accessible by clicking on the extension icon. The popup is added to a shop's webpage as inline frame and remains connected to the browser tab until it is closed using the x-button. The popup is movable to avoid occlusion of underlying content.

3.1 Functionality

The extension shows data protection information on the current device in an online shop. A comparison mode allows users to a) compare the information of two devices directly with each other and b) compare the devices with personal data protection preferences that can be configured in the extension's settings. A mismatch of preferences and data policies is highlighted in red (cf. Fig. 1, right).

3.2 Privacy Information

The extension shows the following information: device name, built-in sensors and functionality (cf. icons for microphone, camera, location, and artificial intelligence in Figure 1, black refers to "technology included", light gray to "not included"), manufacturer's data protection quality (needs improvement, average, or perfect), compliance with the minimum security standards (fulfilled or not fulfilled), and availability of user-friendly data protection information (available or not available). These items are taken from the Mozilla Foundation's **privacy not included* website. Detailed explanations around data protection quality and security standards can be accessed through the information (i) icon.

4 EXPLORATORY STUDY

To answer our research questions, we conducted an exploratory user study using the *PriCheck* prototype and a simple mock online shop. The study took place remotely and participants took part at home on their private computers.

4.1 Apparatus

The study was conducted remotely using Zoom as a video conferencing tool and two major components: 1) a (mock) online *shop* that was available online, and 2) the *PriCheck extension* that we made available to participants as zip-file to be installed manually and locally in their Chrome browser. We assisted them if necessary. The *shop* included nine sample smart devices from three categories (smart assistant, smart watch, and smart surveillance camera), represented with two pictures, name, price, a short description and technical facts (e.g., battery performance). The questionnaires were also made available online using a survey tool. The sessions were audio- and video-recorded.

4.2 Study Design

We conducted a within subjects study with two independent variables: shopping WITHOUT EXTENSION and WITH EXTENSION. All participants conducted the tasks in this order (i.e., first shopping without extension, then using *PriCheck*) to capture their intuitive device choice first. They were asked to think aloud while browsing the shop and filled a NASA-TLX questionnaire [12] (in the "raw" version [11]) after every task to assess perceived workload. For using *PriCheck* (shopping WITH EXTENSION), we also asked participants to fill the SUS questionnaire [4] to assess perceived usability. We

[1] https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security/consultation-on-the-governments-regulatory-proposals-regarding-consumer-internet-of-things-iot-security#designing-a-security-label, last accessed December 23, 2021
[2] https://www.csa.gov.sg/Programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/about-cls, last accessed December 23, 2021
[3] https://foundation.mozilla.org/en/privacynotincluded/about/why/, last accessed December 23, 2021

concluded with semi-structured interviews and questionnaires on demographics, affinity for technology (ATI scale [8]), and general privacy concerns (using the 10-item IUIPC questionnaire [15]).

4.3 Procedure

We conducted two pilot tests to make sure the procedure runs smoothly and tasks are clear. In particular, after the pilots, we removed any device and manufacturer names from the shop to avoid participants being influenced by brand preferences. Results from the pilots are not reported. The final procedure was as follows:

(1) **Installation & Setup.** After participants gave consent for participation, they installed the extension locally in their Chrome web browser and accessed our mock online shop.
(2) **Choice without extension.** To assess participants' general decision factors, we asked them to choose one device per category without using the extension. We asked them to think aloud and afterwards fill the Raw-TLX [11].
(3) **Choice with extension.** Next, participants used *PriCheck* to again choose one device per category while thinking aloud (note that we did not change the shop, nor the available devices to capture potential reconsiderations). After they completed the task, we asked them to fill the Raw-TLX [11] and SUS [4] questionnaire.
(4) **Questionnaire & Interview.** We complemented the session with a semi-structured interview about participants' experience with *PriCheck*, prior purchase decisions, and general feedback on the extension[4]. Finally, participants filled the ATI [8] and IUIPC [15] scale and demographic questions, including a question on smart devices they already own.

4.4 Recruitment & Participants

We recruited 11 participants via university mailing lists and social media. Participants needed access to a Chrome browser on a desktop computer. A session took around 60 minutes. Participants were reimbursed with a 10€ online shopping voucher or study credits.

Participants (9 identified as female, 2 as male) were on average 21.69 years old ($SD = 2.23$). Using the ATI-Scale [8], we measured participants technological affinity on a scale from 1 (low) to 6 (high), which was rather high ($M = 4.28$, $SD = 0.70$). They were also generally concerned about privacy according to the IUIPC questionnaire [15]. On a scale from 1 to 7, they rated their wish for *control* ($M = 5.56, SD = 0.80$), general *awareness* ($M = 6.36, SD = 0.53$), and perception of data *collection* ($M = 5.50, SD = 1.10$). All participants owned a smartphone, seven a smart TV, five a smartwatch, three a smart speaker, one mentioned a smart household appliance and one smart lights.

4.5 Limitations

Our sample is biased towards young, female students. However, this age group belongs to the early adopters of smart devices in Germany[5]. Second, our mock online store included only few information about (real) devices. It did not cover potential other decision factors, such as the manufacturer or reviews from other buyers. However, this allowed participants to focus on privacy-relevant information as provided by *PriCheck*. Lastly, privacy preferences tend to differ from real life behavior (cf. the "privacy paradox" [9]). It remains to be investigated how *PriCheck* can support decisions under real conditions such as, e.g., spending actual money.

[4]The full interview guide is available in the supplementary material of this paper.
[5]https://de.statista.com/statistik/studie/id/41155/dokument/smart-home-report/, last accessed March 01, 2022

4.6 Qualitative Data Analysis

We applied thematic analysis following Braun and Clarke [2, 3]. First, we transcribed all sessions (think aloud and interviews). Next, two researchers independently went through two sample transcripts and applied open coding to establish an initial code book. They applied this code book to half of the remaining transcripts each. New codes and potential disagreements were discussed throughout the analysis process. Hence, we do not report measures of inter-rater agreement [18]. We provide the final code book in the supplementary material of this paper. Quotes were translated from German.

5 RESULTS

5.1 RQ1: General Experience

All participants ($N = 11$) were generally positive and agreed that they would use *PriCheck* for future purchases, e.g.:

> *"I found it very practical and clear."* (P11)

Participants appreciated *PriCheck* to simplify ($N = 6$) and inform ($N = 5$) their choice:

> *"(...) you can see what information these devices collect and then I think you can better assess what and how much information is collected from you (...)"* (P1)

PriCheck also fostered new considerations such as, e.g., where to use the device:

> *"So maybe I wouldn't put the camera in my living room, but only use it in the garden (...) And that influences my decision."* (P2)

Moreover, the usability of *PriCheck* was considered as *very good* with a value of 86.59 ($SD = 6.15$) out of 100 according to the SUS score [4]. Moreover, participants perceived a medium workload in both tasks (browsing with and without *PriCheck*), compared to other computer tasks [10] (Raw-TLX score WITHOUT EXTENSION: $M = 49.77, SD = 12.94$, Raw-TLX score WITH EXTENSION: $M = 47.0, SD = 14.60$). Paired t-tests show that there is a significant difference in physical demand ($t_{10} = -2.50, p = 0.031$). The perceived higher physical demand when using the extension could be due to the fact that participants sometimes had to move the browser extension to see the text behind it. We found no significant differences in the other dimensions.

Participants also raised some suggestions for improvement, especially for the comparison feature ($N = 6$) to, e.g., be able to compare more than two devices:

> *"With the comparison, I actually find it very cool that you [see the devices] directly next to each other. What does one have, what has the other? But I don't think it's bad either to be able to compare all three (...)."* (P7)

Two participants suggested other information to be displayed such as, e.g., data processing procedures or options to opt out.

5.2 RQ2: Decision Support

In our study, participants chose three devices in each task, without and with using *PriCheck*. Only one participant chose the same three devices in both tasks, but the vast majority ($N = 10$) of participants changed at least one decision for a device when using *PriCheck* in the second task. In particular, six participants changed their mind about one device, three changed two devices, and one participant chose different devices in all three categories in the second round.

Decision Factors without PriCheck. Prior to using *PriCheck* (i.e., during the first task), participants mentioned design ($N = 11$), functionality ($N = 11$), price ($N = 10$), and price performance ratio ($N = 3$) as main factors for device choice:

> *"I want to choose [device] C here (...) I wouldn't choose A as it would be too expensive for me, (...). I don't like the design of [device] B and I wouldn't wear it. [Device] C is a good combination."* (P5)

However, few ($N = 3$) participants mentioned data protection as crucial factor, were generally skeptical of smart devices ($N = 1$), or weighed functionality against privacy ($N = 1$):

> *"Smart devices, I'm very skeptical about that. The question is: Do you actually need that in life?"*(P1)

> *"I also like that it records sound. However, I also find it kind of creepy. Then you have this ulterior motive to eavesdrop on someone."* (P1)

> *"I would hesitate between camera C and camera A. Simply because I'm not sure to what extent I personally would like to have a camera on my house now."* (P7)

Decision Factors with PriCheck. Using *PriCheck*, participants increasingly based their decision on information presented in the extension, such as data protection ($N = 11$), the data collected ($N = 5$) and other details presented ($N = 5$). As before, functionality ($N = 6$), design ($N = 2$) or price ($N = 1$) were mentioned. However, these factors were often evaluated in connection with data protection, e.g.:

> *"It could be that I would choose [device] A in this case, despite the price differences, because at least the data protection is better."* (P10)

A comparison was also made between the quality of data protection and the data collected, e.g.:

> *"They are all the same in terms of data protection quality. (...) watch A also collects (...) voice recordings (...). And it also collects contacts, what I don't like."* (P9)

Decision Factors for own devices. In the interviews, we asked participants which factors played a role in the purchase of their own smart device(s) (e.g., smartphones). They mentioned functionality ($N = 8$), price ($N = 4$), design ($N = 4$), price-performance ratio ($N = 2$), or the brand ($N = 2$). Other reasons were the intended use, quality and the advertising ($N = 1$ each). Only three participants stated that they paid attention to data protection and policies. Two participants retrieved information on data protection only after the purchase. No participant claimed to have actively dealt with the data protection guidelines of the individual manufacturers, but rather concluded data protection aspects from previous knowledge and the functionality of the device:

> *"I haven't done a lot of research. I may have drawn conclusions. The best example: This has a face recognition system, hence it records the face's data. It has a fingerprint scanner, so my fingerprint is recorded, but otherwise I did not specifically inform myself (...)."* (P2)

Most participants ($N = 8$) stated that they did not pay attention to data protection as they believed to be unable to avoid data collection in the first place. They also found it difficult to even find the relevant information, e.g.:

> *"(...) most of the time it doesn't even say on the website. And until you (...) looked for all information, it feels like a year had passed. That's why I don't look at it like that, even if I personally think it's a shame."* (P3)

Impact of PriCheck. Participants confirmed that they found *PriCheck* useful ($N = 10$) and it supported their decision ($N = 5$). The comparison feature was mentioned as particularly helpful ($N = 8$) as it saves time ($N = 4$), e.g.:

> *"The structure was especially great because (...) I always looked at the same place, what I wanted to compare and I could easily move between the products."* (P9)

Many participants ($N = 6$) appreciated the additional information about devices. However, there were also concerns about the quality of this information ($N = 2$) and one was overwhelmed by the larger amount of information:

> *"I don't know whether it [the extension] made it easier for me, because it offered a lot of information that is of course useful (...). But then you would have a lot more input, you have to process a lot more, compare a lot more, in order to then make decisions."* (P5)

5.3 Further Use Cases

While many participants would actually use *PriCheck* for online shopping ($N = 8$), especially for complex technical devices, they could imagine further use cases. Participants liked the condensed presentation of information and the comparison option and would like to see a similar tool for other topics such as fake news, sustainability, grocery shopping and other non-technical contexts.

6 DIRECTIONS FOR FUTURE RESEARCH

6.1 Decision Factors

PriCheck fostered decision change, mostly in favor of higher quality in data protection and policies of devices and providers. Other factors that were mentioned included the design and functionality of devices. However, real life purchase decisions might be more complex due to a plethora of other factors such as, e.g., the price or existing infrastructure. It remains to be investigated how *important purchase decision factors can be identified, and how they can be targeted by future mechanisms.* For instance, users' preferences for privacy, but also design and functionality, could serve as a basis for (automatic) device recommendations.

6.2 Information & Data Sources

Participants described our *PriCheck* implementation as helpful and would like to use it. For our study, we only implemented *PriCheck* for a mock online shop. Adjustments would still be necessary to enable use in common online shops. In particular, the extension would need to automatically adapt to the current web page or shop. It could, e.g., search for known device names within an arbitrary page and adapt content accordingly. Moreover, the information to be displayed in the extension would need to be acquired. Ideally, this would happen automatically via, e.g., the manufacturers themselves. Another option could be to crowd-source privacy-relevant information and make it available to users of *PriCheck*. Some participants even questioned the information being displayed. Hence, it would be essential to find means to *verify and only provide trusted information* in *PriCheck*.

6.3 Modalities & Interaction

With *PriCheck*, we provide privacy-relevant information in a browser, which is useful for, e.g., online shopping to support users in context. Another means to display information in-situ is augmented reality. For instance, *PARA* [1] shows information on devices including options to turn off data collection and processing completely. *PriView* [20] visualizes types of sensors as well as the range of data collection. An interesting direction for future research is to look into ideal *modalities for privacy-relevant* information, to make sure the information is available to users in relevant moments (e.g., when being in vicinity of potential privacy intrusion [20], or during a purchase decision). This possibly includes means for *interaction* to, e.g., choose information that is being displayed, access more detailed information, or even directly control data collection and processing for devices that are already installed.

7 CONCLUSION

In this work, we present *PriCheck*, a browser extension that supports users in making informed decisions for the purchase of smart devices, with a focus on privacy-relevant information. Participants of our exploratory user study found the provided information useful, appreciated the comparison feature, and confirmed that *PriCheck* supported their decisions. We conclude with directions for future research that we hope to stimulate further discussions around making privacy information about ubiquitous computing available devices, understandable, and easy to access for users.

ACKNOWLEDGMENTS

We thank all participants for their time and valuable feedback on *PriCheck*. This research was funded by dtec.bw – Digitalization and Technology Research Center of the Bundeswehr [Voice of Wisdom].

REFERENCES

[1] Carlos Bermejo Fernandez, Lik Hang Lee, Petteri Nurmi, and Pan Hui. 2021. *PARA: Privacy Management and Control in Emerging IoT Ecosystems Using Augmented Reality.* Association for Computing Machinery, New York, NY, USA, 478–486. https://doi.org/10.1145/3462244.3479885

[2] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3, 2 (2006), 77–101. https://doi.org/10.1191/1478088706qp063oa

[3] Virginia Braun and Victoria Clarke. 2012. Thematic analysis. (2012).

[4] John Brooke. 1995. SUS: A quick and dirty usability scale. *Usability Eval. Ind.* 189 (11 1995).

[5] Lorrie Faith Cranor. 2012. Necessary but not sufficient: Standardized mechanisms for privacy notice and choice. *J. on Telecomm. & High Tech. L.* 10 (2012), 273. https://fpf.org/wp-content/uploads/2013/07/Cranor_Necessary-But-Not-Sufficient1.pdf

[6] Lorrie Faith Cranor, Praveen Guduru, and Manjula Arjula. 2006. User Interfaces for Privacy Agents. *ACM Trans. Comput.-Hum. Interact.* 13, 2 (jun 2006), 135–178. https://doi.org/10.1145/1165734.1165735

[7] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. 2019. Exploring How Privacy and Security Factor into IoT Device Purchase Behavior. In *Proc. of the CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. ACM, New York, NY, USA, Article 534, 12 pages. https://doi.org/10.1145/3290605.3300764

[8] Thomas Franke, Christiane Attig, and Daniel Wessel. 2019. A Personal Resource for Technology Interaction: Development and Validation of the Affinity for Technology Interaction (ATI) Scale. *International Journal of Human–Computer Interaction* 35, 6 (2019), 456–467. https://doi.org/10.1080/10447318.2018.1456150 arXiv:https://doi.org/10.1080/10447318.2018.1456150

[9] Nina Gerber, Paul Gerber, and Melanie Volkamer. 2018. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security* 77 (2018), 226–261. https://doi.org/10.1016/j.cose.2018.04.002

[10] Rebecca Grier. 2015. How high is high? A metanalysis of NASA TLX global workload scores, In Proceedings of the Human Factors and Ergonomics Society Annual Meeting. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 59. https://doi.org/10.1177/1541931215591373

[11] Sandra G. Hart. 2006. Nasa-Task Load Index (NASA-TLX); 20 Years Later. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 50, 9 (Oct. 2006), 904–908. https://doi.org/10.1177/154193120605000909

[12] Sandra G. Hart and Lowell E. Staveland. 1988. Development of NASA-TLX (Task Load Index): Results of Empirical and Theoretical Research. In *Human Mental Workload*, Peter A. Hancock and Najmedin Meshkati (Eds.). Advances in Psychology, Vol. 52. North-Holland, 139–183. https://doi.org/10.1016/S0166-4115(08)62386-9

[13] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W. Reeder. 2009. A "Nutrition Label" for Privacy *(SOUPS '09)*. Association for Computing Machinery, New York, NY, USA, Article 4, 12 pages. https://doi.org/10.1145/1572532.1572538

[14] Agnieszka Kitkowska, Mark Warner, Yefim Shulman, Erik Wästlund, and Leonardo A. Martucci. 2020. Enhancing Privacy through the Visual Design of Privacy Notices: Exploring the Interplay of Curiosity, Control and Affect. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. USENIX Association, Berkeley, CA, USA, 437–456. https://www.usenix.org/conference/soups2020/presentation/kitkowska

[15] Naresh K. Malhotra, Sung S. Kim, and James Agarwal. 2004. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research* 15, 4 (2004), 336–355. https://doi.org/10.1287/isre.1040.0032 arXiv:https://doi.org/10.1287/isre.1040.0032

[16] Davit Marikyan, Savvas Papagiannidis, and Eleftherios Alamanos. 2019. A systematic review of the smart home literature: A user perspective. *Technological Forecasting and Social Change* 138 (2019), 139 – 154. https://doi.org/10.1016/j.techfore.2018.08.015

[17] Karola Marky, Sarah Prange, Florian Krell, Max Mühlhäuser, and Florian Alt. 2020. "You Just Can't Know about Everything": Privacy Perceptions of Smart Home Visitors. In *19th International Conference on Mobile and Ubiquitous Multimedia*. Association for Computing Machinery, New York, NY, USA, 83–95. https://doi.org/10.1145/3428361.3428464

[18] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. 2019. Reliability and Inter-Rater Reliability in Qualitative Research: Norms and Guidelines for CSCW and HCI Practice. *Proc. of the ACM on Human-Computer Interaction (HCI)* 3, CSCW, Article 72 (Nov. 2019), 23 pages. https://doi.org/10.1145/3359174

[19] Pardis Emami Naeini, Yuvraj Agarwal, Lorrie Faith Cranor, and Hanan Hibshi. 2020. Ask the Experts: What Should Be on an IoT Privacy and Security Label? *ArXiv* abs/2002.04631 (2020), 1–18.

[20] Sarah Prange, Ahmed Shams, Robin Piening, Yomna Abdelrahman, and Florian Alt. 2021. *PriView– Exploring Visualisations to Support Users' Privacy Awareness*. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3411764.3445067

[21] Manuel Silverio-Fernández, Suresh Renukappa, and Subashini Suresh. 2018. What is a smart device? - a conceptualisation within the paradigm of the internet of things. *Visualization in Engineering* 6, 1 (5 2018), 1–10. https://doi.org/10.1186/s40327-018-0063-8