An assessment of privacy policies for smart home devices

Timi Heino
University of Turku
Turku, Finland
tdhein@utu.fi

Sampsa Rauti
University of Turku
Turku, Finland
sjprau@utu.fi

Robin Carlsson
University of Turku
Turku, Finland
crcarl@utu.fi

ABSTRACT

Connected devices using the internet, such as smart home appliances, wearable technology, and other IoT devices, keep becoming more prevalent in our daily lives. At the same time, privacy of the IoT is still a great concern, and consumers need better ways to understand privacy issues clearly. We provide an overview of smart home device privacy policies in the context of the EU area and particularly Finland. In the current study, we analyze the privacy policies of mobile applications associated with 20 smart home devices, and assess these documents in terms of clarity and transparency. We find that the policies are frequently very vague about the third-parties involved, and often fail to clearly indicate whether the privacy policy applies to a specific device model, several models, associated mobile application, or company website.

CCS CONCEPTS

• **Security and privacy → Social aspects of security and privacy**.

KEYWORDS

IoT devices, smart home devices, privacy policies

ACM Reference Format:
Timi Heino, Sampsa Rauti, and Robin Carlsson. 2023. An assessment of privacy policies for smart home devices. In *International Conference on Computer Systems and Technologies 2023 (CompSysTech '23), June 16–17, 2023, Ruse, Bulgaria.* ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3606305.3606332

1 INTRODUCTION

IoT (Internet of Things) devices are becoming increasingly common in our everyday lives. According to recent estimates, there are currently over 15 billion IoT devices in use worldwide, and this number is expected to continue to grow in the coming years. These devices have the ability to connect to the internet and other devices, enabling them to collect and share data, automate tasks, and provide real-time information and feedback.

In the smart home environment, various IoT devices are becoming increasingly popular, offering a range of benefits to homeowners [4, 14]. Smart home technology enables automation of several tasks and data collection, providing convenience, energy savings, and improved security. Smart thermostats can learn the user's preferences and adjust the temperature accordingly, saving energy and money. Smart speakers enable hands-free control of IoT devices, as well as entertainment and information on demand. Smart locks can be used to monitor and control access to consumers' homes.

While these devices are very convenient, they also raise serious privacy concerns [8, 9, 11]. Privacy is essential for IoT devices in smart home settings because these devices are constantly collecting data about their users and potentially transmitting information to third parties. In many cases, this data can also include highly sensitive information like personal communication, biometric data, or data concerning health.

There is also a wide range of mobile applications provided by device manufacturers for conveniently controlling smart home appliances. In addition to data collection and third parties in IoT devices, these applications also process lots of data received from smart devices and potentially deliver this data to third parties [3]. In this paper, we concentrate on the privacy policies associated with smart home mobile applications.

There is a body of previous research on privacy policies for IoT devices. Paul et al. [6] provide an assessment of privacy policies of internet of things services, and found that most examined privacy policies informed users insufficiently. Similarly, Perez et al. [7] present an overview and analysis of privacy policies for consumer IoT devices, finding that documents are often long and vague, unnecessarily increasing the cognitive load for the user. Shayegh et al. [12] introduce an automatic approach to extract notice and choice statements from privacy documents to help users to make informed decisions and better understand privacy notices.

Our study contributes to the existing literature on IoT privacy policies by assessing the privacy policies for mobile applications provided by smart home device manufacturers. When analyzing these policy documents, our focus is specifically on what is said about personal data collection and sending data to third parties in the context of smart home mobile applications. Moreover, our study provides an overview of smart home privacy policies in the context of the EU and particularly Finland, as we focus on a group of popular smart home devices used by Finnish consumers. We provide a qualitative analysis of privacy policies of 20 smart home devices.

The rest of the paper is structured as follows. Section 2 introduces the research methods used in the study, explaining how the smart home IoT devices and the associated mobile applications were selected. It also discusses the method used to analyze the associated privacy policy documents. Section 3 presents the results of the study and evaluates whether the consumer can get a good understanding of what data is sent to third parties by the studied smart home mobile applications and who these data processors are.

CompSysTech '23, June 16–17, 2023, Ruse, Bulgaria

ACM ISBN 979-8-4007-0047-7/23/06.
https://doi.org/10.1145/3606305.3606332

Table 1: The studied smart home devices

Device model	Category
Bosch AccentLine Series 8 HBG876EC6S	Oven
Bosch Serie 4 SMU4HAB48S	Dishwasher
Chromecast 3rd Generation	Streaming media adapter
Google Nest Hub 2nd Generation	Smart home hub
iRobot Roomba 980	Robot vacuum
LG FV90VNS2QE	Washing machine
LG InstaView GSX961MCCZ	Fridge freezer
Netatmo Smart Radiator Thermostats Starter Pack	Radiator Thermostats
Oral B iO Series 9S IO9BK	Electric toothbrush
Philips Hue Being 3261048P6	Ceiling light
Philips Hue Bridge	Network bridge
Ring Video Doorbell 3 RINGVD3	Doorbell
Samsung 9.1.4 HW-Q950	Speaker system
Samsung French Door RF24R7201SR	Fridge freezer
Samsung Nordic Home 25	Air source heat pump
Samsung UE55TU8072 55" 4K Ultra HD	TV
Siemens iQ300 SN43HW33VS	Dishwasher
Sonos Beam smart soundbar	Speaker system
Xiaomi Mi Robot Vacuum Mop Pro 26200	Robot vacuum
Yale Doorman V2N	Digital lock

Section 4 discusses the implications of our study ways to improve privacy policies. Section 5 concludes the paper.

2 METHODS

2.1 Selection of smart home devices and privacy policies

Different popular household devices and machines were considered. If a smart version of a device existed in addition to the traditional one, it was included in the study. Next, the corresponding devices were searched for on the website of Gigantti, the largest household electronics store in Finland. If a suitable device was not found on Gigantti's website, Verkkokauppa.com, another large electronics store, was used instead.

The selection criterion for choosing the devices among similar ones was their popularity. Thereby device categories were sorted by their popularity, and the first device was picked. If similar products were found to be equally popular, customer reviews were compared, and the device with most positive reviews was chosen. By assessing products this way, we aimed to ensure that the chosen products were widely used and research findings would have an impact on a larger group of consumers. In the end, 20 devices were selected for the study. The selected smart home devices are listed in Table 1.

Since the smart devices are controlled through mobile applications, application marketplaces were searched for the privacy policies of these applications. To find the mobile applications and their corresponding privacy policy documents, links to application marketplaces were searched on the product pages of the device retailer's website. The applications and their privacy policies were all found from Google's Play store.

2.2 Assessment of privacy policies

In previous literature, analysis of privacy policies has almost unanimously found them to be hard for consumers to understand [16]. In addition, oftentimes consumers solely glance through the policy without carefully perusing it [15]. Many studies have noted that privacy policies are sometimes intentionally vague [1, 5], and frameworks for identifying these unclear and unambiguous spots have been developed [13].

We studied the privacy policy documents of the smart home mobile applications to identify paragraphs where sharing personal data with third parties was discussed. Loosely based on the approach presented by Shvartzshnaider et al. [13], these excerpts from privacy policies were analyzed to identify vague points in the text where the privacy concerns – such as the nature of the shared data and the third parties receiving it – were not presented in sufficient detail.

3 RESULTS

The unclear and vague points of smart home application privacy policies are analyzed in this section. These unclarities are divided into four groups: 1) unclear privacy policy scope, 2) inadequate information about the transmitted personal data and third parties, 3) opt-out consent and sensitive personal data, and 4) unclear data retention period.

Unclear privacy policy scope

Table 2 shows the scopes of the analyzed privacy policies. Several problems with privacy policy scopes were identified in the current study. By looking at the table, we can see that the most privacy policy scopes are very generic, listing several different areas (mobile

Table 2: The scopes of the studied privacy policies of the smart home mobile applications

Device model	Reported privacy policy scope
Bosch AccentLine Series 8 HBG876EC6S Bosch Serie 4 SMU4HAB48S	Mobile app, website, services
Chromecast 3rd Generation Google Nest Hub 2nd Generation	Mobile app, devices, website, services
iRobot Roomba 980	Mobile app, devices, website, communication with iRobot
LG FV90VNS2QE LG InstaView GSX961MCCZ	Mobile app, devices, website, services, communication with LG
Netatmo Smart Radiator Thermostats Starter Pack	Devices, website, software, services
Oral B iO Series 9S IO9BK	Mobile app, devices, website, services, 3rd party partners
Philips Hue Being 3261048P6 Philips Hue Bridge	Mobile app, devices, website, social media, communication with Philips
Ring Video Doorbell 3 RINGVD3	Mobile app, devices, website, social media sites, services
Samsung 9.1.4 HW-Q950 Samsung French Door RF24R7201SR Samsung Nordic Home 25 Samsung UE55TU8072 55" 4K Ultra HD	Mobile app
Siemens iQ300 SN43HW33VS	Website
Sonos Beam smart soundbar	Devices, software, website, services, offline actions (like visiting the store)
Xiaomi Mi Robot Vacuum Mop Pro 26200	Devices and services
Yale Doorman V2N	Mobile app, devices, software, website, services

application, devices, vendor website etc.) to which the policy is applied. Terms such as "services" and "software" are very non-specific and undermine the goal to transparently inform the customer.

Almost in all cases, the mobile application associated with the smart home devices does not have a separate privacy policy, which usually makes it very difficult to differentiate the third-party data collection in the mobile application and the data collection happening elsewhere. For example, the privacy of the company website is often discussed in the same privacy policy as the privacy of the IoT device and the related application, and the fact that the text often keeps alternating between the application and website does not help. When this is the case, it is often impossible for the user to know whether the third-party analytics mentioned in the policy document, for example, pertain to the IoT device, associated mobile application or simply company website. As an example, the Sonos speaker system had a generic privacy policy, where the use of Google Analytics was mentioned without clearly indicating whether this third party is present in the mobile application, on the company website or possibly both. As we can see in Table 2, Samsung was the only vendor clearly discussing the mobile application in its own privacy policy.

Moreover, several device models of the same manufacturer often have a common privacy policy, which makes it difficult for the user to get a good understanding of the privacy of a specific device model, as the functionalities provided by the models and their privacy implications vary. The device model also has a direct impact on what kind of data the related mobile application potentially leaks to third parties.

Finally, the mobile application and the smart home device itself are not clearly separated in the privacy policies in terms of third parties. To some extent this is understandable as these two effectively function as a whole but it would still be beneficial for the user to understand what kind of information collection by third parties they consent to by installing and using the application. This helps the user to make the important decision whether to use the mobile application at all. Therefore, it would be recommendable for manufacturers to consider this distinction.

Inadequate information about the transmitted personal data and third parties

Under the GDPR, companies and organizations are required to disclose to users what third parties receive personal data from them and what personal data is being shared. By learning these details, individuals can better appreciate how their personal data is being used and what parties can access it. Only then can a consumer make a truly informed decision about whether to provide their personal data to the IoT device manufacturer.

Third parties were not always mentioned in the studied privacy policies. For example, in the privacy policy for Philips Hue Being ceiling light, it was mentioned that personal information is shared with third parties, but these third parties were not further specified. Therefore, the user cannot get a good understanding of what kinds of data specific third parties receive and who they are. Even when the third parties are mentioned, the previously discussed issue with the privacy policy scopes often caused problems when trying to understand which third parties were present. For instance, the Ring doorbell listed Google Analytics, Google Firebase, Mixpanel, Optimizely, and Heap Analytics as third parties, but it remains unclear whether these third parties collect data in the associated Always Home application, or only on the company website. For

the same reason, it remains a mystery what personal information is collected by the application. Xiaomi had similar issues, as it was not clear which product the generic privacy policy was referring to when discussing shared personal data and third parties involved. Samsung also has a common privacy policy concerning several device models, although the mobile application and its privacy is discussed more clearly.

Opt-out consent and sensitive personal data

When smart home IoT devices collect sensitive personal data, there is always the question whether the user truly makes the conscious decision to accept the data collection. For instance, the robot vacuums of iRobot create and store a machine-generated map of the floor plan that the robot is cleaning [2]. This raises several concerns regarding the data privacy in users' homes. At least for the iRobot Roomba 980 vacuum cleaner we studied, the user has to actively opt out by switching the map data collection off from the mobile application. Under the GDPR, however, consent must be specific, unambiguous and informed, and the opt-in approaches are considered the best way to obtain such consent. At least for most privacy critical data collection functionalities in the devices, device manufacturers should consider using the opt-in approach when obtaining consent in a way that adequately informs the user of the specific data collection functionality.

Unclear data retention period

The GDPR requires that device manufacturers include information about data retention in privacy policy documents. The privacy policy should provide clear information about how long the user's personal data will be retained – for example, the retention period of cookies. The retention period should always reflect the purpose for which the data is being retained and should not be longer than needed. Almost all of the studied privacy policy documents stated that data is stored "as long as necessary", which is not very helpful for users. The privacy policy of Netatmo Smart Radiator Thermostats appeared to be the only one providing completely sufficient information about data retention in terms of exact time intervals.

4 DISCUSSION

We have presented a study of privacy policy documents of mobile applications for smart home devices. In particular, we discussed how they describe personal data sent to third parties. We have seen that at many points, the studied policies addressed the issue of third-party analytics inadequately and vaguely. Third-party data leaks to analytics companies are a significant security threat in the context of smart home IoT devices. Various analytics services collect data from smart home devices to analyze user behavior and preferences and to further develop their products. However, sharing of data without informing the user sufficiently can result in serious privacy risks.

The key findings of the current study can be summarized as follows:

- The scopes of the studied privacy policies were constantly found to be unclear. It was not clear at all times whether the privacy policy document was referring to a specific model of smart device, several device models, the associated mobile application, the company website or all services of the company.
- Third parties involved in data collection were not always mentioned at all. It was also unclear what information was shared with specific third parties and in which parts of the system (e.g. in the smart device or in the mobile application) information collection took place.
- There were also apparent shortcomings in the practices such as using an opt-out approach for privacy critical data collection functionality (e.g. a robot vacuum collecting sensitive map data of the user's home).
- In many cases, the retention period of the collected personal data was left unclear.

To mitigate the privacy risks caused by the data sent to third-party analytics companies, IoT device manufacturers have to keep track of what kind of personal data their devices and associated applications are collecting and sharing. While this analysis may lead to removal of some analytics services – which can nowadays be unintentionally added when using many development environments and frameworks – it is also very important to transparently report the use of third-party services in privacy policy documents. This includes clearly stating which third parties receive personal data, what categories of personal data are involved, how this data is being processed, and how long it is stored. As we have seen, manufacturers should also pay special attention to clearly indicating which device model, application, or web service the privacy policy is discussing at each specific point.

The current study has shown that at many points, privacy policies of smart home IoT devices and their applications are vague and inform users insufficiently about sharing personal data to third parties. To improve their privacy policies, the device manufacturers should use clear and concise language, avoid complicated legal jargon and vague expressions that may confuse users. Providing comprehensive information is also important. The privacy policy should clearly and transparently discuss how personal data is collected, how and why it is processed, which third parties it is shared with, and for how long it is stored.

As we have seen, it would also be important to have consumers consent by opting in when the most critical privacy issues, such as collecting map data of their home, are concerned. Later on, it is also important to allow consumers to take control of their own personal data by giving them the choice to opt out of specific data collection and sharing practices. This not only makes the data collection more controllable but also adds transparency of privacy issues. Finally, ready-made templates or checklists could be a good idea to help writing privacy policy documents (see also [10]). This would at least help in avoiding such problems as forgetting important matters like data retention periods.

5 CONCLUSION

As stated by many studies, privacy in the IoT environment is an area where many privacy issues are still inadequately addressed [6]. As we have seen, this is also clearly reflected in many unclarities and ambiguities present in smart home privacy policy documents. It is also very difficult for consumers to perceive the scopes of privacy

policy documents, as several different products and services such as the smart device, mobile application and website are being discussed in a disorganized and vague manner. Our results highlight the need for device manufacturers to pay closer attention to the clarity, transparency and completeness of their privacy policy documents in the smart home setting.

ACKNOWLEDGMENTS

This research has been funded by Academy of Finland project 327397, IDA – Intimacy in Data-Driven Culture.

REFERENCES

[1] Benjamin Andow, Samin Yaseer Mahmud, Wenyu Wang, Justin Whitaker, William Enck, Bradley Reaves, Kapil Singh, and Tao Xie. 2019. PolicyLint: Investigating Internal Privacy Policy Contradictions on Google Play.. In *USENIX Security Symposium*. 585–602.

[2] Anna Chatzimichali, Ross Harrison, and Dimitrios Chrysostomou. 2020. Toward privacy-sensitive human–robot interaction: Privacy terms and human–data interaction in the personal robot era. *Paladyn, Journal of Behavioral Robotics* 12, 1 (2020), 160–174.

[3] Timi Heino, Robin Carlsson, Sampsa Rauti, and Ville Leppänen. 2022. Assessing discrepancies between network traffic and privacy policies of public sector web services. In *Proceedings of the 17th International Conference on Availability, Reliability and Security*. 1–6.

[4] Ruqaiya Khan, Vinod Kumar Shukla, Bhopendra Singh, and Sonali Vyas. 2021. Mitigating Security Challenges in Smart Home Management Through Smart Lock. In *Data Driven Approach Towards Disruptive Technologies: Proceedings of MIDAS 2020*. Springer, 61–71.

[5] Thomas B Norton. 2016. The non-contractual nature of privacy policies and a new critique of the Notice and Choice Privacy Protection Model. *Fordham Intell. Prop. Media & Ent. LJ* 27 (2016), 181.

[6] Niklas Paul, Welderufael B Tesfay, Dennis-Kenji Kipker, Mattea Stelter, and Sebastian Pape. 2018. Assessing privacy policies of internet of things services. In *ICT Systems Security and Privacy Protection: 33rd IFIP TC 11 International Conference, SEC 2018, Held at the 24th IFIP World Computer Congress, WCC 2018, Poznan, Poland, September 18-20, 2018, Proceedings 33*. Springer, 156–169.

[7] Alfredo J Perez, Sherali Zeadally, and Jonathan Cochran. 2018. A review and an empirical analysis of privacy policy and notices for consumer Internet of things. *Security and Privacy* 1, 3 (2018), e15.

[8] Alfredo J Perez, Sherali Zeadally, and Nafaa Jabeur. 2017. Investigating security for ubiquitous sensor networks. *Procedia computer science* 109 (2017), 737–744.

[9] Sampsa Rauti, Samuli Laato, and Tinja Pitkämäki. 2021. Man-in-the-Browser Attacks Against IoT Devices: A Study of Smart Homes. In *Proceedings of the 12th International Conference on Soft Computing and Pattern Recognition (SoCPaR 2020) 12*. Springer, 727–737.

[10] Mark Rowan and Josh Dehlinger. 2014. A privacy policy comparison of health and fitness related mobile applications. *Procedia Computer Science* 37 (2014), 348–355.

[11] Eryk Schiller, Andy Aidoo, Jara Fuhrer, Jonathan Stahl, Michael Ziörjen, and Burkhard Stiller. 2022. Landscape of IoT security. *Computer Science Review* 44 (2022), 100467.

[12] Parvaneh Shayegh and Sepideh Ghanavati. 2017. Toward an approach to privacy notices in IoT. In *2017 IEEE 25th International Requirements Engineering Conference Workshops (REW)*. IEEE, 104–110.

[13] Yan Shvartzshnaider, Noah Apthorpe, Nick Feamster, and Helen Nissenbaum. 2019. Going Against the (Appropriate) Flow: A Contextual Integrity Approach to Privacy Policy Analysis. In *Proceedings of the AAAI Conference on Human Computation and Crowdsourcing*, Vol. 7. 162–170.

[14] Benjamin K Sovacool and Dylan D Furszyfer Del Rio. 2020. Smart home technologies in Europe: A critical review of concepts, benefits, risks and policies. *Renewable and sustainable energy reviews* 120 (2020), 109663.

[15] Nili Steinfeld. 2016. "I agree to the terms and conditions":(How) do users read privacy policies online? An eye-tracking experiment. *Computers in human behavior* 55 (2016), 992–1000.

[16] Stephanie Winkler and Sherali Zeadally. 2016. Privacy policy analysis of popular web platforms. *IEEE Technology and Society Magazine* 35, 2 (2016), 75–85.