A Study of Privacy Policies across Smart Home Companies

Paul Biocco
NC A&T State University
1601 East Market Street
Greensboro NC 27401
pjbiocco@aggies.ncat.edu

Mahsa Keshavarz
NC A&T State University
1601 East Market Street
Greensboro NC 27401
mkeshavarz@aggies.ncat.edu

Patrick Hines
NC A&T State University
1601 East Market Street
Greensboro NC 27401
phines@aggies.ncat.edu

Mohd Anwar
NC A&T State University
1601 East Market Street
Greensboro NC 27401
manwar@ncat.edu

ABSTRACT

Smart home users have limited control over their own smart home data. With Zero-Conf setups, users are given default security with limited or no options to increase protection of their data. In this paper, we study a smart home user's ability to control their data. We create a rubric to measure the quality of privacy policies of smart home companies. From the perspective of a privacy-concerned smart home user, we reviewed the privacy policy of 13 smart homes companies. We find that in most cases users cannot opt-out of their information being collected. When there are opt-out options, often the process requires contacting the company directly, leaving the process in the hands of a company employee instead of the user. In addition, we find that often these privacy policies tend to be hard to read and comprehend. We have three recommendations: first, increase clarity of their privacy policy by reducing distributed information into user-consumable format (e.g., bullet points, visuals, etc.) instead of paragraphs. Second, separate the website's privacy policy from their devices and hubs to clarify what information the user is releasing about their home. Third, either allow a user to opt-out of data collection during registration or create a data donation program that users can opt into.

1. INTRODUCTION

Smart homes allow users to get optimal control over their environment. With smart technology increasing at a rapid rate, our homes are being filled with smart home appliances. Smart home technologies have improved home security, home automation, and home healthcare efforts. These technologies collect data such as one's activity levels, sleeping patterns or food intake behaviors through various smart devices and are able to share this information with health care providers or family members [3]. These devices interact with one another and display and analyze the data that they receive in order to provide home comfort services [26]. Although these services make life easier, they raise concerns about the violation of home data privacy. Disclosure of smart home data may allow large businesses to make complete profiles of their users for advertisement revenue or allow an attacker to interrupt normal behaviors. To better outline the data management procedures for users, privacy policy documents were created as an explanation of these procedures.

Privacy policies are standardized documents detailing the manner in which a company handles user information. In general, these documents as it relates to smart home devices are cumbersome to read and understand, and the opt-out procedures listed in them for users whom have data stored with the company are typically non-existent or tedious to execute. Given the verbosity of these privacy policies, it is possible for a company to not disclose what information is gained (through smart sensors and smart hubs) in anticipation that most users will overlook this explanation. A user may not want their detailed home information and daily activities in the hands of these companies.

To highlight this problem further, we created a privacy policy rating rubric for smart home company websites. We analyzed 13 different smart home company websites and rate their privacy policy in accordance with our rubric. Finally, we give recommendations on how to increase privacy policy clarity and provide options for smart home companies to collect data with user consent effectively.

The rest of our paper is organized into the following: section two covers privacy issues in smart homes, section three describes our study of the smart home companies' privacy policies, section four discusses the study results, and we conclude and discuss potential future works in section five.

2. PRIVACY ISSUES IN SMART HOMES

Privacy issues are not new to smart homes. McKenna et al. [16] identified privacy concerns about the authentication process of accessing smart home data. Attackers can illegally obtain unencrypted information generated by a smart home via wireless data intercept tools. Paetz et al. [19]found that home information can be stolen with eavesdropping attacks due to personal information leaks over radio-frequency protocols. Sanchez et al. [21] found that a user's activities and behavior may reveal sensitive information. While some individual entries of home data are not sensitive, in combination with other non-sensitive entries, personally identifiable information can be created. For example, the flow of data packets between the MAC address of a smart television and the access point of a smart hub would allow an attacker to guess when a user is active within the home.

Denning et al. [4]states that there are various threats emerging in smart homes due to swift and steady introduction of smart devices. Some attacks may require the attacker to be near the smart home, such as stealing home data through flaws in ZigBee and ZWaves[9; 15]. Other attacks, however, do not require proximity to their target, such as linking attacks. Konidala et al. [13] discussed several of these smart home attack vectors. For example, they explain how an insecure connection can leave smart homes vulnerable to replay, spoofing, and snooping

attacks. For example, these attacks can be executed against a smart refrigerator with a RFID reader-enabled display.

However, there is little focus on data sharing between smart home companies and consumers. Companies who offer smart home services can take data through their own smart hubs and devices despite the user's active consent. The users are not able to express their information sharing preferences or restrict how their data is used. Bai et al. [2] expressed concern over this problem. Zero-Conf configurations, which are default settings within a system that a user cannot change, are employed in smart homes which forces users to accept the vendor's policies. Users do not have the ability to control the data flow of their devices.

Technological glitches can also contribute to privacy breaches. In May 2018, an Amazon Echo smart home device (powered by the voice-command system "Alexa") recorded a conversation between a couple in Portland, Oregon and sent the raw audio to their employer without the couple's knowledge [14]. This was due to a mistake in the Echo's audio interpretation of their conversation, the device recognizing some early vocal segment as "Alexa," an activation word for the device. The device then began listening for a command and recognized "send message." In June 2017, a man in Cary, North Carolina also fell victim to an accidental recording by the Amazon Echo and Alexa [25]. During a personal conversation in his home, Alexa picked up on keywords that triggered its recording of an audio message and sent the message to the man's insurance agency listed in his contacts. The company called the man to alert him to the accidental sending. Though these mishaps seem like unlucky situations, this brings to light the concern of privacy.

3. A STUDY OF SMART HOME PRIVACY POLICY

Our purpose of this study is to understand the scope of how much control a user has over their own data in a smart home when they buy a third-party smart home product. We took the perspective of a home owner who wishes to have a smart home but has concern over how much data about their home is given to a third-party company. To accomplish this, we limited the scope of study to using only the smart home company's privacy policy and product descriptions. However, after reading several product manuals, we could not find significant information regarding privacy controls and chose to further limit the scope down to comparing only privacy policies.

We selected companies with high, medium, and low market shares in smart homes and judged their privacy policies based on a privacy policy rating rubric. The results are shown in Table 1.

For consistency, we created a judging criterion for privacy policies as it relates to a user's home data. In this rubric, we use the word "hub" and "device". We define a "hub" as a hardware which connects smart home appliances and controls data communication among them. This can be, but is not limited to, a smartphone application, a web application, or a separate computer. We define the "device" as a smart home appliance, which can gather and send information about an environment's state to a hub.

Privacy Policy Rating Rubric:

0: No privacy policy found on the company website.

1: Privacy policy on the company website does not include hubs or devices. Furthermore, there is no option stated to not to be tracked while visiting the company website.

2: Privacy policy on the company website does not include hubs or devices. However, the policy does state the option for not to be tracked while visiting the company website.

3: Privacy policy on the company website covers hubs and devices, but does not allow for opt-out.

OR

3: Privacy policy on the company website covers hubs, and devices, but the privacy policy only defines what the devices/hubs collect and does not tell the user if this information collected is accessible by the company.

4: Privacy policy covers hubs and devices. Allows for opt-out, but the process has significant complications, or requires third-party software.

Table 1. A list of smart home companies and their privacy policy rating according to our rubric along with an average privacy policy rating.

Company Name	Category	Privacy Policy Rating
Fibaro [8]	General	5
Iotas[12]	General	3
Sentri [22]	General	3
Nexia [18]	General	2
Avi-on [1]	General	5
Keen Home [11]	Climate Control	2
Ecovent [7]	Climate Control	3
Vivint.SmartHome [24]	Security	3
Ring [20]	Security	5
Ecobee [5]	Environment	3
Ecoisme [6]	Environment	5
Sonos [23]	Entertainment	3
Musaic [17]	Entertainment	3
Average Rating		3.461538

5: Privacy policy covers hubs and devices. Allows for opt-out options but requires direct contact with company in a time-gated way (i.e., you must wait for an email response or fill out a support ticket).

OR

5: Privacy policy covers hubs and devices. It allows partial opt-out of home information.

6: Privacy policy covers hubs and devices, but requires additional configuration of the hub and/or browser to apply.

7: Privacy policy covers their hubs and devices, allows for opt-out immediately within the site, but finding the settings within the site/portal is difficult.

8: There is privacy policy on hubs and devices and allows opt-out immediately within the site. Finding the privacy settings is easy.

9: Privacy policy includes hubs and devices and allows opt-out during registration and is immediately made clear. Options to change settings are also within the profile.

10: Privacy policy states that no data is ever collected about the site and devices.

When creating this rubric, we considered two primary features. First, we considered the disclosure of what data about the user's home is given by the user to the company. Second, we considered the ability to opt-out of data collection. We decided that, from the consumer's standpoint, it was worse to be given no information about home data privacy than to be told explicitly they have no option to opt-out. When the user is informed that their home data will be retained, a consumer can still choose not to use the product. However, if there is no policy disclosure, this choice cannot be made.

4. DISCUSSION

When reading privacy policies of smart home companies, we observed that most commonly there was no opt-out policy. Most of the time reasons were not given, but some products were designed to function with device information as a requirement to how the product works, such as Sonos. Other times, such as in the case of Ring, they refuse to let the user opt-out because they have additional services they provide for payment beyond their standard package. In addition, most privacy policies used vague wording, failing to disclose what smart home data is being collected. Most of the websites have opt-out options for third-party disclosure, but for our rating system we prefer that the smart home company to not collect data after an opt-out to be given a higher rating.

While most of these privacy policies were rated poorly, there were a few privacy policies with notable positive characteristics. In this section, we will outline a few companies' privacy policies.

Fibaro: This general smart home company sells motion sensors, flood sensors, and hubs. Though this company collects a significant amount of information, they have a very clear opt-out section called "The Right of Access to the Content of Your Data and Other Rights" [8]. However, this company requires a support ticket to be emailed, leaving it up to the them to delete information in a timely manner.

Keen Home: This company primarily sells smart vents for climate control. Keen Home's privacy policy for their main site applied to the website only. The policy explicitly states the following at the start of their privacy policy: "This policy explains how Keen Home's website collects and uses information, and it explains how we use and protect that information. A separate policy covers Keen Home's Smart Vents" [11]. Unfortunately, we could not find this separate policy within the site after searching. This policy, if it exists, has either been buried within the site, or it can only be found after the user has purchased a smart vent.

Ecobee: This company's privacy policy clearly states what data is collected, but does not state that if a user's home data is accessible by the main company. However, they have a "donate your data" model, which allows a user to opt-in to giving their home data to third-party research facilities [5]. This sort of model would be a better privacy-preserving option for companies to let users share their information.

Iotas: While this company did not have a clear opt-out agreement, there was one notable feature which was applied to third parties [12]. During registration, they allow for the user's information to be withheld from third-party distribution. If this was applied to not only third-party distribution but also to the main company, this would be a significant option for a privacy-concerned user.

While this rubric thoroughly covers the ability of a user to opt-out of information collection, this rubric has limitations in judging the overall criteria of a privacy policy. Other factors such as accessibility within the website, information collected, and readability, are also critical parts in judging the overall quality of a privacy policy. In addition, it is important that users read the privacy policy just as much as the privacy policy is readable. Rating rubrics such as the one provided would best be applied by a neutral third-party, potentially integrated into a privacy policy tool such as Polisis [10].

5. CONCLUSION AND FUTURE WORKS

Overall, beyond simple disclosure we found two strong configurations companies can use to ethically collect data. They can opt-out of information collection during registration as shown by Iotas, create a "donate your data" program as shown by the Ecobee. Additional recommendations would include increasing the clarity of privacy policy improving clarity by using concise language and bullet points. In addition, there should also be a secondary privacy policy that applies to only the devices and hubs, such as what Keen Home provided. This secondary privacy policy should also be available and visible on the product's page.

In the future, we plan to expand upon the rubric outlined in this paper by factoring in accessibility, readability, and content collection. To ensure that our rubric is accurate as possible, we plan to create a user study which will consider our expanded range of topics. We plan to test privacy policy observing how

long it takes a user to access a privacy policy and compare it to how long it takes to find a product. Other potential fields of research may include privacy option accessibility within devices and hubs. In addition, expanding Bai et al.'s work in Zero-Conf setups to include smart home devices and hubs would also be a strong consideration.

6. REFERENCES

[1] AVI-ON. (2015). "Privacy Policy". http://avi-on.com/privacy-policy/, Retrieved May 25, 2018.

[2] BAI, X., XING, L., ZHANG, N., WANG, X., LIAO, X., LI, T., & HU, S.-M. (2016). "Staying secure and unprepared: understanding and mitigating the security risks of Apple ZeroConf," In Security and Privacy (SP), 2016 IEEE Symposium on IEEE, 655-674.

[3] BAUER, K.A. (2001). "Home-based telemedicine: a survey of ethical issues," Cambridge Quarterly of Healthcare Ethics 10, 2, 137-146.

[4] DENNING, T., KOHNO, T., & LEVY, H.M. (2013). "Computer security and the modern home," Communications of the ACM 56, 1, 94-103.

[5] ECOBEE. (n.d). "Privacy Policy," https://www.ecobee.com/legal/use/, Retrieved May 25, 2018.

[6] ECOISME. (n.d). "Privacy Policy," https://ecoisme.com/privacy, Retrieved May 25, 2018.

[7] ECOVENT. (n.d). "Privacy Policy," https://www.ecoventsystems.com/privacy, Retrieved May 25, 2018.

[8] FIBARO. (n.d). "Privacy policy and cookies," https://www.fibaro.com/en/privacy-policy/, Retrieved May 25, 2018.

[9] FOULADI, B. & GHANOUN, S. (2013). "Honey, I'm Home!!, Hacking ZWave Home Automation System," Black Hat.

[10] HARKOUS, H., FAWAZ, K., LEBRET, R., SCHAUB, F., SHIN, K.G., & ABERER, K. (2018). "Polisis: Automated Analysis and Presentation of Privacy Policies Using Deep Learning," arXiv preprint arXiv:1802.02561.

[11] HOME, K. (n.d). "Privacy Policy," http://www.nexiahome.com/privacy-policy, Retrieved May 25, 2018.

[12] IOTAS. (n.d). "Privacy Policy," http://www.iotashome.com/policies/privacy-policy/, Retrieved May 25, 2018.

[13] KONIDALA, D.M., KIM, D.-Y., YEUN, C.-Y., & LEE, B.-C. (2011). "Security framework for RFID-based applications in smart home environment," Journal of Information Processing Systems 7, 1, 111-120.

[14] LALIBERTE, M. (2017). "Cary man says 'Alexa' disclosed private conversation," WRAL, https://www.wral.com/cary-man-says-alexa-disclosed-private-conversation/16745480/ Retrieved May 25, 2018.

[15] LOMAS, N. (2015). "Critical Flaw identified In ZigBee Smart Home Devices".

[16] MCKENNA, E., RICHARDSON, I., & THOMSON, M. (2012). "Smart meter data: Balancing consumer privacy concerns with legitimate applications," Energy Policy 41, 807-814.

[17] MUSAIC. (n.d). "Privacy Policy," http://www.musaic.com/en-wo/privacy-policy, Retrieved May 25, 2018.

[18] NEXIA. (n.d). "Privacy Policy," http://www.nexiahome.com/privacy-policy,Retrieved May 25, 2018.

[19] PAETZ, A.-G., DÜTSCHKE, E., & FICHTNER, W. (2012). "Smart homes as a means to sustainable energy consumption: A study of consumer perceptions," Journal of consumer policy 35, 1, 23-41.

[20] RING. (2018). "Privacy Notice," https://shop.ring.com/pages/privacy, Retrieved May 25, 2018.

[21] SANCHEZ, I., SATTA, R., FOVINO, I.N., BALDINI, G., STERI, G., SHAW, D., & CIARDULLI, A. (2014). "Privacy leakages in Smart Home wireless technologie," In Security Technology (ICCST), 2014 International Carnahan Conference on IEEE, 1-6.

[22] SENTRI. (2015). "Privacy Policy," http://hello.sentri.me/legal/, Retrieved May 25, 2018.

[23] SONOS. (2018). "Privacy Policy," https://www.sonos.com/en-us/legal/privacy, Retrieved May 25, 2018.

[24] VIVINT.SMARTHOME. (2018). "Privacy Policy," https://www.vivint.com/company/policies/privacy, Retrieved May 25, 2018.

[25] WAMSLEY, L. (2018). "Amazon Echo Recorded And Sent Couple's Conversation - All Without Their Knowledge," NPR, Retrieved May 25, 2018.

[26] ZHANG, M., LIU, Y., WANG, J., & HU, Y. (2016). "A New Approach to security Analysis of Wireless Sensor Networks for Smart Home Systems," In Intelligent Networking and Collaborative Systems (INCoS), 2016 International Conference on IEEE, 318-323.