Work in Progress: Towards Usable Updates for Smart Home Devices

Julie M. Haney and Susanne M. Furman

National Institute of Standards and Technology (NIST)**, Gaithersburg, MD, USA
{julie.haney, susanne.furman}@nist.gov

Abstract. ***Background.*** Smart home device updates are important tools for remediating security vulnerabilities.
Aim. We aim to understand smart home users' perceptions of and experiences with updates.
Method. We interviewed 40 smart home users and analyzed a subset of data related to updates. We are also planning a broader, follow-on survey.
Results. Users experienced inconsistency in update transparency and methods, were confused about how and if updates are applied, and seldom linked updates to security.
Conclusion. Our efforts will provide a new understanding of smart home updates from a usable security perspective and how those are similar/different to views on updates of conventional IT.

Keywords: Smart home · Updates · Cybersecurity · Usability.

1 Introduction

Internet of things (IoT) smart home updates are a critical mechanism by which manufacturers can distribute patches to remediate security vulnerabilities. Updates may be one of the few tools users have to secure their devices since other configurable security options are limited or unavailable. Unfortunately, technologists have found that update mechanisms may be inconsistent across devices [8]. Even among security professionals, the number one threat to IoT was viewed as "difficulty patching Things, leaving them vulnerable" [16]. Despite technology experts identifying issues, the user perspective on smart home updates has not yet been fully explored.

To better understand experiences and challenges with smart home updates, we analyzed a subset of data from a broader, in-depth interview study of 40 smart home users aimed at investigating general experiences with, perceptions of, and opinions about smart home devices, including aspects of privacy and security. This paper focuses on analysis of update-related data only. By exploring this subset of the interview data, we begin to gain insights into perceptions and

** Certain commercial companies/products are identified in this paper to foster understanding. This does not imply recommendation or endorsement by NIST.

usability of smart home updates, including what role, if any, users perceive updates as playing with the security of their devices. Preliminary analysis suggests that users experience inconsistency in update transparency and methods, as well as confusion about how and if updates are applied. More concerning, most study participants did not relate smart home device updates to security, so they might not have been as inclined to install updates immediately.

Since updates were not a major focus of the interview study, we wish to delve deeper into user update experiences and perceptions, especially on a per-device basis. To that end, we are planning a follow-up survey to gather responses from a broader population of smart home owners. When completed, we hope our research will have several contributions. We will provide novel insights into end user perceptions, experiences, and challenges with updates within the context of smart home devices from both a usability and security perspective. In addition to identifying similarities to prior research focused on updates of other types of computing devices, we hope to discover ways in which smart home device updates may be different or more challenging. Our results may also inform the design of smart home device update mechanisms and notifications to provide a more usable platform for deploying critical security patches when necessary.

2 Related Work

2.1 User Update Behaviors

While no prior studies have explored update behaviors for smart home technologies, researchers have investigated these behaviors for other information technology (IT). People delay software updates for a number of reasons, including a lack of awareness of the upgrade value; interruption of computing activities; and possible negative consequences of applying the update [6, 18]. Users may also have a difficult time understanding the relationship between software updates and security [6]. Ultimately, users must balance the risk and costs of updating against potential benefits [19].

2.2 IoT Updates

A number of critical security vulnerabilities for smart home devices have been identified in recent years, highlighting the need for timely updates [2]. However, there are unique challenges to IoT updates [9]. IoT manufacturers may be inexperienced with security feature and update mechanism design. Economic incentives for providing updates and long-term support for inexpensive and disposable devices may not exist, leaving devices vulnerable to attack. NIST discovered that information on IoT updates is not always readily available to consumers and that updates are not always done in a secure manner [8]. From a technology perspective, IoT devices are often memory, processor, and battery constrained, making updates more challenging to deploy while managing integrity and confidentiality of the updates and potential software dependencies [1, 11, 12].

Several researchers focused on security labels for IoT products. Emami-Naeini et al. [4] showed consumer openness to IoT privacy and security labels, including update information. Morgner et al. [15] investigated consumer preferences for security update information on mandatory IoT product labels. They concluded that security update labels, especially those focused on the availability period (how long the manufacturer guarantees to provide updates) may have a significant impact on consumer product selection.

Although the technical limitations of IoT updates and potential of labels have been discussed, to the best of our knowledge, no prior literature addresses potential usability issues with *smart home* updates through the eyes of consumers, a gap our study hopes to address. Lin and Bergmann [14] suggested that smart home devices should implement updates with little or no user intervention. Emami-Naeini et al. [4] interviewed smart home users, noting that most desired automatic updates because of convenience. However, they made no further observations for recommendations with respect to updates. Other researchers explored user perceptions of smart home privacy and security but did not discuss updates(e.g., [17, 21, 20].

3 Methodology

From February to June 2019, we interviewed 40 smart home users to understand their perceptions of and experiences with smart home devices. NIST's Research Protections Office approved the study. Prior to the interviews, we informed participants of the study purpose and how data would be protected with generic identifiers (e.g., P14_U) not linked to individuals.

3.1 Participant Recruitment and Demographics

We hired a consumer research company to recruit adult users of smart home devices from a database of individuals living in a large U.S. metropolitan area who had agreed to be contacted about research opportunities. To determine eligibility, prospective participants completed an online screening survey about their smart home devices, their role with the devices (e.g., administrator, user), and other demographic information. After reviewing the screening information, we selected participants if they were active users of at least two different types of smart home devices. In line with current interview compensation rates in our region, participants were given a $75 prepaid card.

Participants had diverse professional backgrounds with only eight in an engineering or IT field. Thirty-two of the 40 participants had installed and administered their devices (indicated with an A after the participant ID), and eight were non-administrative users of the devices (indicated with a U). Fifty-five percent were male and 45% were female. Seventy percent were between the ages of 30 and 49. Participants were highly educated with 45% having a master's degree or above and another 50% with a BS/BA. All but one participant had three or more individual smart home devices, with 38 having three or more different categories of devices.

3.2 Data Collection and Analysis

We developed a semi-structured interview protocol covering several topics: purchase and general use; installation and maintenance (including updates); privacy; security; and safety. In this paper, we focus only on data related to updates. An IoT content expert who had professionally worked on IoT security in addition to having an extensive, custom smart home, reviewed the interview questions to ensure the use of correct terminology and the consideration of appropriate aspects of smart home ownership. We piloted the interview with four smart home owners from our institution (two device administrators and two non-administrators/users) to determine face validity of questions and language. Based on feedback from the content expert, we added questions for potential "do-it-yourself" users who customize smart home software and hardware to their own specifications (e.g., via writing custom code). After the pilots, minor adjustments were made to to simplify the wording of several questions. Because modifications were minor, the pilot interviews were included in our analyzed data set. After the protocol was finalized, we collected data via 36 additional semi-structured interviews (40 interviews total including pilots) lasting on average 41 minutes. Interviews were audio recorded and transcribed.

We analyzed the interview data using both deductive and inductive coding practices. Initially, each member of the research team individually coded a subset of four interview transcripts using an *a priori* code list based on research questions and open coded for additional concepts as needed. We then met to discuss codes and develop a codebook. Coding then continued until all transcripts were coded by two researchers, who then met to examine and resolve differences in code application and identify relationships and central themes.

4 Methodology

From February to June 2019, we interviewed 40 smart home users to understand their perceptions of and experiences with smart home devices. NIST's Research Protections Office approved the study. Prior to the interviews, we informed participants of the study purpose and how data would be protected with generic identifiers (e.g., P14_U) not linked to individuals.

4.1 Participant Recruitment and Demographics

We hired a consumer research company to recruit adult users of smart home devices from a database of individuals living in a large U.S. metropolitan area who had agreed to be contacted about research opportunities. To determine eligibility, prospective participants completed an online screening survey about their smart home devices, their role with the devices (e.g., administrator, user), and other demographic information. After reviewing the screening information, we selected participants if they were active users of at least two different types of smart home devices. In line with current interview compensation rates in our region, participants were given a $75 prepaid card.

Participants had diverse professional backgrounds with only eight in an engineering or IT field. Thirty-two of the 40 participants had installed and administered their devices (indicated with an A after the participant ID), and eight were non-administrative users of the devices (indicated with a U). Fifty-five percent were male and 45% were female. Seventy percent were between the ages of 30 and 49. Participants were highly educated with 45% having a master's degree or above and another 50% with a BS/BA. All but one participant had three or more individual smart home devices, with 38 having three or more different categories of devices. Appendix B has more detailed demographics along with the types of devices owned by each participant.

4.2 Data Collection and Analysis

We developed a semi-structured interview protocol covering several topics: purchase and general use; installation and maintenance (including updates); privacy; security; and safety (Appendix A). In this paper, we focus only on data related to updates. An IoT content expert who had professionally worked on IoT security in addition to having an extensive, custom smart home, reviewed the interview questions to ensure the use of correct terminology and the consideration of appropriate aspects of smart home ownership. We piloted the interview with four smart home owners from our institution (two device administrators and two non-administrators/users) to determine face validity of questions and language. Based on feedback from the content expert, we added questions for potential "do-it-yourself" users who customize smart home software and hardware to their own specifications (e.g., via writing custom code). After the pilots, minor adjustments were made to to simplify the wording of several questions. Because modifications were minor, the pilot interviews were included in our analyzed data set. After the protocol was finalized, we collected data via 36 additional semi-structured interviews (40 interviews total including pilots) lasting on average 41 minutes. Interviews were audio recorded and transcribed.

We analyzed the interview data using both deductive and inductive coding practices. Initially, each member of the research team individually coded a subset of four interview transcripts using an *a priori* code list based on research questions and open coded for additional concepts as needed. We then met to discuss codes and develop a codebook. Coding then continued until all transcripts were coded by two researchers, who then met to examine and resolve differences in code application and identify relationships and central themes.

5 Preliminary Results

5.1 Update Modes and Notifications

The interviews revealed that update modes may vary from smart home device to device, with some updating automatically and others requiring users to manually initiate updates. In addition, participants discovered available updates in

different ways depending on the device. A participant who owned multiple devices said: *"Some of them notify me, others update automatically, and others I'll find out about either through an email or just because I'm kind of monitoring technology news in general"* (P15_A). Another commented:

> *"Some devices will send me a text message... saying that we're going to be updating a device at this time, and it will apply the updates automatically. Other devices, I need to go into their own specialty apps and check what firmware is running and then check for an update. Some devices, I actually have to go to a website and download something, and then my phone, for instance, will update the device"* (P11_A).

Smart home devices that notify users of available updates do so in a variety of ways. Notifications "pushed" to the device's user interface or via the companion app before or after update installation are most common. For example, an owner of a smart doorbell explained how she finds out about updates: *"I see an alert. It says, 'Your Ring doorbell has a new update. Do you want to allow it? Do you want to accept it?' "* (P36_A). Several participants received emails alerting them of available or just-installed updates. Some devices with screen interfaces, such as smart thermostats and televisions, displayed the update notification directly on the device itself. Other smart home owners did not receive push notifications to tell them updates were available. Rather, they had to manually open the companion app and check.

5.2 Update Purpose and Urgency

Participants most often viewed updates as fixing or adding non-security functionality. For example, one participant stated, *"I accept all updates because I believe they'll make things more functional, add new features that I didn't have before"* (P36_A). Interestingly, this perception led to mixed feelings regarding the urgency of applying updates. Several participants who had experienced issues with their devices believed updates were a high priority. A participant who owns a smart video doorbell and security cameras noted that smart home devices *"would have the highest priorities than any of the other apps on my phone... because that's the security of my home"* (P31_A). Another participant talked about experiencing frequent glitches with his devices. Therefore, he viewed regular updates to his devices as being critical:

> *"To me it's not a choice for, at least, internet of things. Sometimes for my computer, I don't update as soon as they tell me I should. I wait for a while to see if anybody reports bad bugs with the new update. I feel that I have to [for a smart home device] in order for it to work at its best"* (P13_A).

However, others thought updates to functionality were lower priority or unnecessary as long as the device appeared to be working properly. A participant described her indifference with respect to updates, *"I don't think that the end user actually really cares. As long as the thing works, it works"* (P40_U). Other participants did not feel they could properly assess the criticality of the up-

date because the manufacturer did not reveal the purpose of the update: *"The information on what the update achieves is unclear"* (P31_A).

5.3 Uncertainty about Update Status

Participants reflected that they may not observe update notifications, do not recall setting an option to automatically install updates, or are not sure if there are configurable options for setting update parameters. These inconsistencies may lead to a sense of uncertainty about whether their devices are being updated or even can be updated. One user remarked about his virtual assistant, *"I don't know when it's [virtual assistant] doing its updates. Like ever. They never ask me. They never prompt me"* (P7_A).

Some participants assumed that the lack of notifications meant that updates must be happening automatically. While possibly true with some devices, this assumption might be flawed for other products. A participant lamented, *"They don't notify me when there's an update. I guess I just kind of assume that they happen as they go. You would think that I'd get an email, but I guess I don't. That might be nice" (P23_A).*

Even though users may have an assumption of automatic updates, the uncertainty due to lack of notification leaves some with a sense of discomfort. For example, one participant stated: *"I'm assuming that updates are being done silently in the background. I don't really know, and it sort of gives the impression that you bought this thing and it's not evolving... that it's not expanding and getting new updates"* (P24_A).

5.4 Updates to Apps vs. Updates to Devices

In addition to uncertainty about update status, the interviews revealed that participants often conflated updates to smart home device companion app software (typically installed on a smartphone) with updates to device firmware. They did not realize that updates to apps were not necessarily accompanied by device updates and vice-versa. This was evidenced by participants referencing typical smartphone app update indicators when asked how they know smart home device updates are available. For example, a user of an Android-based phone explained, *"I get a notification. It doesn't say specifically which apps need to be updated. It just says 48 apps need to be updated. Then I go into Google Play, and see my apps, and individually determine which ones I want to update"* (P31_A).

5.5 Update Concerns

Even when update availability was visible, participants voiced concerns about updates causing issues or breaking functionality on their smart home devices. For example, one participant voiced frustration with updates to his smart televisions: *"I've had to reset my TVs many times because the software update didn't work or kind of messed things up"* (P10_A). Updates also have the potential to

invalidate previous user configuration settings or necessitate new ones: *"as they come out with updates, particularly significant updates that change the interface, for example, that might be cause for me to go back in and redo some of the settings"* (P15_A).

Two participants expressed concerns about a lack of updates should a manufacturer stop supporting a product. One of these commented,

> *"I would hope that over time the companies that support these devices would continue to update their firmware and basically make them more reliable. I think in some cases that's happened, but I think in other cases the devices just get abandoned"* (P11_A).

5.6 Relationship to Security

Although some updates can be a conduit to fix security vulnerabilities in smart home devices, study participants rarely linked updates to security, with only five mentioning updates in the context of security. Most discussed updates in terms of fixing functionality or adding features. When asked what mitigation actions they take to address any security concerns they might have, only three mentioned applying updates or upgrading products.

Interestingly, two participants recognized the importance of applying updates, but were also concerned about potential security-related consequences. One participant liked that updates to his devices could be done via the internet, but at the same time was concerned because *"it means that someone's reaching in... There's some kind of access from the outside"* (P26_A). Another saw potential for updates to weaken security:

> *"I guess one area where I would be worried about would be adding features that may threaten my privacy and security... I would want to know that the update also gave me the capability of disabling or turning off that feature I might be concerned about"* (P15_A).

6 Discussion

6.1 Comparison to Traditional Updates

We note similarities between our results and those from previous research studies in Related Work. Similarities included: a lack of awareness of the importance of applying updates; a lack of information about the update purpose hindering users' ability to weigh risk and cost against potential update benefits; concern about possible negative consequences of applying updates; and concern about surprise new features being added.

Although similarities exist, we identified several differences in user experiences with smart home updates as compared to updates explored in prior studies. We did not find evidence of concerns about interruption, likely because users do not have the same kind of interactive sessions with smart devices as they would on a tablet, phone, or computer. Our findings additionally suggest that, because

devices are often controlled with a mobile companion app, some updates may be overlooked since several participants did not understand the difference between a phone update, an app update, and a device update. We also discovered that participants were concerned about manufacturers discontinuing product support (and therefore, no longer issuing updates) due to the dynamic smart home market. As opposed to updates for more-familiar and widely-used operating systems, applications, and hardware (e.g., those from Apple and Microsoft), our participants were often unaware if updates were available, how to configure automatic updates, or how to check update status. Confusion about update mechanisms may be amplified by the number of smart home devices users own, especially if the products are from various manufacturers with different update models and different modes of notification.

We also acknowledge that the update experience for smart home devices may necessarily have to be different than traditional IT updates because of processing/memory constraints and limited interactive interfaces. Therefore, more research is warranted to investigate a suitable, usable update interface that can accommodate device limitations.

6.2 Informing Usable Updates

Study results may inform more usable update interfaces and mechanisms. Although our focus was on home users, improved update usability can also be especially valuable for IoT administrators in organizations who have to maintain large numbers of devices.

Insufficient information about the purpose and benefit of updates may result in users lacking a sense of urgency about applying updates, especially if devices appear to be working fine. Users may also be uncertain about update status and availability. To help users make informed decisions, manufacturers could provide greater transparency of update purpose and importance of applying an update (perhaps via a criticality rating), which is in concert with Vaniea and Rashidi's recommendation for easy-to-find information on updates [19]. As also recommended by other standards and government organizations [9, 5, 3, 7], manufacturers could be more forthcoming about their update model and support so that users are aware of how update availability will be made known, what actions users should take to install updates, what update configuration and notification options (if any) are available, and how manufacturers will handle discontinuation of product support. Some of these update attributes were addressed in prior work on product labels [4, 15] and showed promise in impacting consumer purchase decisions and providing transparency. However, more research needs to be done to determine whether consumers would even read the labels.

In addition to lack of transparency, many of our participants expressed discomfort or frustration with updates and their ability to control them. Providing additional information on updates can help users feel more confident in their update decisions. In addition, manufacturers could provide options for users to configure automated updates (as recommended in [14]) with configurable notifications of success afterwards. Users could be given options to schedule if and

when they receive notifications. To mitigate concerns that updates might break the device or result in unwanted features or settings, devices could support a rollback mechanism, as recommended by others [8, 13, 19]. Users may then be more likely to install an update if they have a way out should there be a problem.

Although we identified issues related to lack of transparency, it must be noted that it is currently unclear as to whether or not consumers would actually read any additional information or in what format they would wish to receive the information. In addition, too much information could be overwhelming and result in user frustration or users just ignoring the information. Therefore, future research should be done to account for consumer preferences.

7 Limitations and Planned Future Work

In addition to typical limitations of interview studies (e.g., self-report and social desirability biases), our study results may have limited generalizability. Our sampling frame of mostly well-educated individuals living in a high-income region in the U.S. may not be fully representative of the global smart home user population. However, our participant population does appear to typify early adopters of smart home devices as identified in industry surveys (for example, [10]).

Our interview study was meant to be exploratory with a goal of identifying areas warranting additional investigation. As such, the interview protocol was broad in covering multiple aspects of smart home ownership and did not focus solely on updates. We also did not ask about updates on a per-device basis (just generally), so are not able to determine if there are different perceptions or experiences depending on the type of device and manufacturer and if some devices are doing a better job at updates than others.

In recognition that more research should be done to delve deeper into users' smart home update experiences, we are in the initial planning phase for an online, quantitative survey of a larger, more diverse sample of smart home users. In addition to asking more questions about perceptions of updates (e.g., importance, purpose), we will obtain per-device experiences and explore what kind of options, if any, users would like in order to gain greater insight and control of update mechanisms. We will also investigate users preferences for update-related information, e.g., what kind of information they would like to receive (if any at all) and desired formats and communication mechanisms.

References

1. Bauwens, J., Ruckebusch, P., Giannoulis, S., Moerman, I., Poorter, E.D.: Over-the-air software updates in the internet of things: An overview of key principles. IEEE Communications Magazine **58**(2), 35–41 (2020)
2. Consumer Product Safety Commission: Status report on the Internet of Things (IoT) and consumer product safety. https://www.cpsc.gov/s3fs-public/Status-Report-to-the-Commission-on-the-Internet-of-Things-and-Consumer-Product-Safety.pdf (2019)

3. Department for Digital, Culture, Media and Sport: Code of practice for consumer IoT security. https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security (2018)
4. Emami-Naeini, P., Dixon, H., Agarwal, Y., Cranor, L.F.: Exploring how privacy and security factor into IoT device purchase behavior. In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. ACM (2019)
5. ETSI: TS 103 645 Cyber security for consumer internet of things. https://www.etsi.org/newsroom/press-releases/1549-2019-02-etsi-releases-first-globally-applicable-standard-for-consumer-iot-security (2019)
6. Fagan, M., Khan, M.M.H., Buck, R.: A study of users' experiences and beliefs about software update messages. Computers in Human Behavior **51**, 504–519 (2015)
7. Fagan, M., Megas, K.N., Scarfone, K., Smith, M.: NISTIR 8259 foundational cybersecurity activities for IoT device manufacturers. https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf (2020)
8. Fagan, M., Yang, M., Tan, A., Randolph, L., Scarfone, K.: Draft NISTIR 8267 Security review of consumer home Internet of Things (IoT) products. Tech. rep., National Institute of Standards and Technology (2019)
9. Federal Trade Commission: Internet of things privacy and security in a connected world. https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf (2015)
10. GfK: Future of smart home study global report (2016), https://www.gfk.com
11. Gupta, H., Oorschot, P.C.V.: Onboarding and software update architecture for IoT devices. In: 17th International Conference on Privacy, Security and Trust (PST). pp. 1–11 (2019)
12. Hernández-Ramos, J.L., Baldini, G., Matheu, S.N., Skarmeta, A.: Updating IoT devices: challenges and potential approaches. In: 2020 Global Internet of Things Summit (GIoTS). pp. 1–5. IEEE (2020)
13. IoT Security Foundation: Secure design best practice guides. https://www.iotsecurityfoundation.org/wp-content/uploads/2019/11/Best-Practice-Guides-Release-2.pdf (2019)
14. Lin, H., Bergmann, N.: IoT privacy and security challenges for smart home environments. Information **7**(3), 44 (2016)
15. Morgner, P., Mai, C., Koschate-Fischer, N., Freiling, F., Benenson, Z.: Security update labels: Establishing economic incentives for security patching of IoT consumer products. In: Proceedings of the 2020 IEEE Symposium on Security and Privacy. pp. 429–446. IEEE (2020)
16. SANS Institute: Securing the Internet of Things survey. https://www.sans.org/reading-room/whitepapers/covert/paper/34785 (2014)
17. Tabassum, M., Kosinski, T., Lipford, H.R.: "I don't own the Data": End user perceptions of smart home device data practices and risks. In: Fifteenth Symposium on Usable Privacy and Security (2019)
18. Vaniea, K., Rader, E., Wash, R.: Betrayed by updates: How negative experiences affect future security. In: Proceedings of the 2014 SIGCHI Conference on Human Factors in Computing Systems (CHI 14). pp. 2671–2674 (2014)
19. Vaniea, K., Rashidi, Y.: Tales of software updates: The process of updating software. In: Proceedings of the 2016 SIGCHI Conference on Human Factors in Computing Systems (CHI 16). pp. 3215–3226 (2016)
20. Zeng, E., Mare, S., Roesner, F.: End user security and privacy concerns with smart homes. In: Thirteenth Symposium on Usable Privacy and Security (2017)

21. Zheng, S., Apthorpe, N., Chetty, M., Feamster, N.: User perceptions of smart home IoT privacy. In: Proceedings of the ACM on Human-Computer Interaction (2018)

A Interview Questions

SECTION A: TERMINOLOGY

1. You may have heard the term "internet of things," or IoT for short. Can you talk a little about what you think the internet of things is?
2. You may have heard the term "smart devices." What about devices makes them "smart?"
3. What does it mean to have a smart home?
4. What do you think is the relationship, if any, between the internet of things and smart devices?

SECTION B: PURCHASE & GENERAL USE

[Review list of smart home devices before beginning this section.]

5. Who was involved in the decision to purchase the smart home devices?
6. What are the reasons the smart home devices were purchased?
   - How did you (or a household member) learn about the devices before buying them?
7. What hesitations, if any, did you have about getting the devices prior to purchase?
8. For what purposes do you use your smart home devices?
9. How do you access the devices – remotely with an app, while physically in the home, or both?
   - *If using a virtual assistant:* How do you access your devices using [insert assistant name]?
   - *If using a hub:* Do you use the hub app to access your devices, or do you use an individual app specific to each device?
10. How do others in your household use the smart home devices?
11. What do you like most about the devices? What are the benefits, if any, of having these devices?
12. What do you like least or dislike about the devices?
13. How have your opinions or expectations of the devices changed, if at all, from the time you first used them until now?
14. What concerns, if any, do you have about the devices?
15. In what ways, if any, have you changed your behaviors because of your smart home devices?
16. In what ways, if any, have you become reliant on your smart home devices?
17. What do the other members of your household think about the smart home devices?
18. Have you had visitors to the home who have had to use the smart home devices?
    - *If yes:* How did they use the devices? What did they think?

19. What smart home devices, if any, have you had in the past, but are no longer using?
    - What are the reasons for no longer using this device?
20. What kinds of things would you like to be able to do with your devices, but haven't, don't know how, or are not sure that you can?
21. What devices would you like to get in the future? For what reasons?

SECTION C: INSTALLATION/TROUBLESHOOTING

22. Who installed the smart home devices?
23. Who administers (configures or maintains) the smart home devices?

For Installers:

24. In general, what was your experience with the installation of the devices?
    - What went well?
    - What didn't go as well?
25. Have you ever had to reinstall a device? If so, what were the reasons for the reinstallation?
26. *If have more than one device:* What has been your experience adding additional devices to the home?

For DIYers:

27. In the screening questionnaire you indicated you build your own or create extensions for your smart home devices and platforms. Can you briefly summarize what you've done?

For Administrators:

28. What configuration changes, if any, have you made to the devices since installation?
    - *If participant makes configuration changes:* How often do you make changes?
29. How do you know that updates are available or needed?
30. How are updates done on your device - automatically or do you have to initiate them?
    - *If manual initiation:* How often do you check for updates?
    - How do you decide whether to update or not update?

For Everyone:

31. How do you try to figure out how to do something new with your devices?
    - What sources do you consult or use?
    - *If have a voice assistant:* What has been your experience, if any, adding new skills to your voice assistant?
32. What kinds of problems, if any, have you encountered while using your smart home devices?
    - How did you go about trying to resolve those problems?

SECTION D: PRIVACY

33. What type of information, if any, do you think the devices are collecting?
    - Which of this information, if any, would you consider to be personal?
34. Where do you think the information goes?
35. In what ways, if any, does your device or the device manufacturer provide a means to control or manage what information is collected and how it is shared?
36. What are your concerns, if any, about how information is collected, stored, and used and who can see that information?
    - In what ways, if any, have you acted to minimize or alleviate some of those concerns?
    - What kinds of actions would you like to be able to take to address your concerns, but haven't, don't know how, or are not sure that you can?
37. Who do you think is responsible for protecting the privacy of information collected by your smart home device?

SECTION E: SECURITY

38. What are your concerns, if any, about the security of your devices?
    - In what ways, if any, have you acted to minimize or alleviate some of those concerns?
    - What kinds of actions would you like to be able to take to address your concerns, but haven't, don't know how, or are not sure that you can?
39. What restrictions, if any, are placed on who in your home can use the devices and what they can do?
40. How do you authenticate to or get into any apps associated with the device?
    - What issues or problems, if any, have you experienced with authentication?
41. Does more than one person in your household use an app to access the same device?
    - Does more than one person use the same account and authentication to access the app?
    - What concerns, if any, do you have with multiple people having access to the app?
42. Who do you think is responsible for the security of your smart home devices?

SECTION F: SAFETY

43. In what ways, if any, do you think the devices contribute to safety?
44. In what ways, if any, do you think the devices might pose a safety risk?

SECTION G: CONCLUSION

45. Is there anything else you'd like to add related to anything we've talked about?

B Participant Demographics

ID	Gen	Age	Ed	Occupation	Device Type				
					Sec	Ent	Env	Appl	Asst
P1_A	F	50-59	M	Liaison	X		X		X
P2_A	M	30-39	M	Lead engineer	X	X	X		X
P3_A	F	40-49	M	Professor	X	X	X	X	X
P4_A	M	60+	M	Retired	X	X			
P6_U	F	30-39	B	Events manager	X	X	X	X	X
P7_A	M	30-39	B	Software engineer	X	X	X	X	X
P8_A	M	30-39	B	Federal employee	X	X	X	X	X
P9_A	F	30-39	M	Educationist	X	X	X		X
P10_A	M	30-39	B	Computer scientist	X	X	X	X	X
P11_A	M	50-59	M	Electrical engineer	X	X	X		X
P12_U	F	30-39	M	Administrative assistant	X	X	X		X
P13_A	M	50-59	M	Manager, cognitive scientist	X	X	X	X	X
P14_U	F	40-49	H	Information specialist	X	X	X		X
P15_A	M	30-39	B	Computer scientist	X	X	X		
P16_A	M	40-49	M	Research chief	X	X	X		X
P17_A	F	30-39	M	Systems engineer	X	X	X	X	X
P18_A	M	30-39	B	Business consultant	X	X	X		X
P19_A	M	50-59	B	Retail services specialist	X	X	X	X	X
P20_A	F	30-39	B	Administrator		X			
P21_U	F	18-29	B	Human resources manager	X	X	X	X	X
P22_A	M	30-39	B	Executive admin assistant	X	X	X	X	X
P23_A	F	40-49	M	Community arts specialist	X	X	X		X
P24_A	M	40-49	B	Operational safety analyst		X	X		X
P25_A	M	30-39	B	Program management analyst	X	X	X	X	X
P26_A	M	30-39	B	Analyst	X	X	X		X
P27_A	F	40-49	M	Program coordinator	X	X	X	X	X
P28_A	F	50-59	B	Consultant	X		X		X
P29_A	M	18-29	M	Events coordinator	X	X	X		X
P30_U	F	18-29	B	Event planner	X	X	X		X
P31_A	F	30-39	M	Lobbyist	X	X	X		X
P32_A	M	30-39	B	Health educator		X	X	X	X
P33_A	M	18-29	B	Senior technology analyst	X	X	X		X
P34_A	M	40-49	B	Financial analyst	X	X	X	X	X
P35_A	M	40-49	M	Accountant	X	X	X	X	X
P36_A	F	30-39	B	Project manager	X	X	X		X
P37_A	F	40-49	M	Assistant principal	X	X	X		
P38_U	F	60+	M	Special educator		X	X		X
P39_U	M	60+	M	Retired		X	X		X
P40_U	F	30-39	C	Customer service rep	X	X	X		X
P41_A	M	40-49	B	Security	X	X	X		X
				Total	**35**	**38**	**38**	**15**	**36**

Table 1. Participant Demographics. ID: A - smart home administrators/installers, U - smart home users; Gen (Gender); Ed (Education): M - Master's degree, B - Bachelor's degree, C - some college, H - High school; Device Type: Sec - Home security, Ent - Home entertainment, Env - Home environment, Appl - Smart appliance, Asst - Virtual assistant