Transferability of Privacy-related Behaviours to Shared Smart Home Assistant Devices

Lin, Vanessa Z.; Parkin, S.E.

DOI
10.1109/IOTSMS52051.2020.9340199

Publication date
2021

Document Version
Accepted author manuscript

Published in
2020 7th International Conference on Internet of Things

Transferability of Privacy-related Behaviours to Shared Smart Home Assistant Devices

Vanessa Z. Lin
University College London
London, UK
vanessa.lin.17@ucl.ac.uk

Simon Parkin*
TU Delft
Delft, Netherlands
s.e.parkin@tudelft.nl

***Abstract*—Smart assistant devices (such as Amazon Echo or Google Home) have notable differences to more conventional consumer computing devices. They can be used through voice control as well as physical interaction, and are often positioned as a shared device within a home environment. We conduct an exploratory online survey with 97 UK-based users of smart assistant devices, to examine the differences users perceive between smart assistants and more familiar devices (such as smartphones and computers), in terms of shared use dynamics, privacy-related behaviours, and privacy concerns. The survey explores typical usage, setup practices, perceived ease of use and control, privacy concerns for multiple users, shared usage of existing devices, and smart assistant privacy control usage. Approximately half of participants were unsure of where to access privacy settings on their smart home assistants; basic device controls and informal privacy controls saw general use. Those who had used privacy controls with previous devices used at least one smart assistant privacy control. Results have implications for supporting transferable privacy behaviours from computing devices to smart home devices, and improving privacy-related design for smart assistants.**

***Index Terms*—consumer Internet-of-Things, smart homes, privacy behaviours**

I. Introduction

Smart home voice assistants or smart speakers (from here on, *smart assistants*) are increasingly prevalent worldwide, even though they are a relatively new technology [1]. Such devices include, but are not limited to, the popular Amazon Echo and Google Hub [2], [13].

Within a smart home, where consumer Internet-of-Things (IoT) devices are used, these smart assistants learn on increasing amounts of data to become more useful ([15], [17], [21], [32], [37]). Smart assistants such as the Amazon Echo can gather audio data, location data, log queries, and access linked third-party apps [2]. They may also access, collect, and store financial data, purchasing data, and productivity data [2], [13].

Where there has been a focus in research on attacks exploiting weak device security, consumers often have incomplete or inaccurate threat models around smart assistants [1], [3], [23], [24], [38]. Many users lack understanding of how smart assistants function, how they integrate with other IoT devices, or how their information is processed and available privacy controls [24], [33], [38].

Critically, smart assistants can operate in highly personal and informal spaces like the home, where users may reasonably expect to relax their privacy behaviours, as opposed to more formal environments like the workplace [15], [17], [37]. Smart assistants are often shared amongst multiple users, where one user may be more knowledgeable about technology than others [15], [22], [29], [31].

Users may be familiar with privacy controls and threats around personal devices such as tablets, laptops, and mobile phones. However, the relative novelty of smart assistants as being a new, shared technology makes it potentially difficult for users to understand and be aware of not only their own privacy concerns, but their privacy concerns in regards to use of a highly-connected device shared with other users. It is reasonable to ask if existing privacy control usage and behaviours for non-'smart' devices influences adoption of privacy control usage in smart assistants [1], [24], [33], [38]. We explore whether the transfer of privacy-related behaviours (or lack thereof) can be identified. We consider further whether existing privacy behaviours for familiar devices such as computers and mobile phones are being translated to newer, unfamiliar classes of smart assistant devices and Internet-of-Things (IoT) devices.

Here we describe an exploratory survey of 97 UK residents (Section III) who own and share either an Amazon Echo or a Google Home smart assistant (these being among the most popular smart assistant devices). Survey results (Section IV) find that privacy control usage rates for smart assistants were generally low, with half of participants unsure of where to access privacy settings and reporting only use of simple informal privacy controls. Transferability of privacy-related behaviours between prior computing devices and newer smart home devices was generally in terms of adoption of available device privacy controls. Respondents who used privacy controls previously also used at least one smart assistant privacy control. We discuss implications and conclusions in Section V and Section VI respectively.

II. Background and Related Work

Related work spans a number of areas, characterising threats to the smart home and the smart assistant environment, the dynamics of a shared device environment, user perceptions for smart assistants, and user privacy concerns.

A. Smart assistant threats

Threats in a smart home environment may involve either external or internal adversaries, and sole or multi-user chal-

*Corresponding author. Portions of work conducted previously at UCL.

lenges. Smart assistants are interconnected within a smart home or device infrastructure, and may serve as a focal point to control other connected devices [37], [38]. Users may route control of connected devices through smart assistants [37]. There are gaps in the understanding of group privacy within the context of smart assistant environments [18]. The boundaries of privacy are blurred in this potentially shared, communal context —- for example, it is not clear how privacy violations are defined when related to guest users of a smart assistant [37]. Internal threats can often have more direct, realised effects than external threats [6], [25], [28], [31], [37] (such as a person being monitored or controlled by another). Existing privacy controls such as access controls, prevention of configuration changes, and parental controls for different users are often misunderstood and under-utilised [37]. Research also documents weaknesses and usability issues for such controls, such as navigating the complexity of privacy settings and whether feedback on device activity is communicated to all users of a shared device [28]. Thus, lack of user awareness and unintended sharing of information are ongoing concerns around smart assistants. Users of smart home devices may implement mitigations to address privacy concerns relating to external entities [14], where here we address individual capacity to control privacy relative to other users in the home by utilising existing knowledge about computing devices.

B. Shared use and management

Use of smart assistants depends on spatial and temporal factors, such as where the device is located and when in the day it is used [17]. Research into the social context of smart home devices notes a reliance on existing work or social relationships to determine who manages the technologies [15], adding that the amount of control given to a user is often determined by technical ability and device familiarity. Primary or more knowledgeable users may accommodate less technically capable users and guest users. In non-adversarial and generally cooperative households, shared privacy is usually protected by social norms and fostering of mutual trust [37]. Where there may be power imbalances between users [12] this may include malicious activity, such as in intimate tech-abuse and the threat of the "UI-bound," "authenticated but adversarial user" [11]. This raises issues around privacy violations for shared, and increasingly connected, devices.

C. User perceptions

Patterns in smart assistant adoption and studies of smart assistant users have found that users do not use existing privacy controls, liked to be early adopters, acknowledge the convenience vs. privacy tradeoff, and have an incomplete knowledge of the risks [1], [22], [31], [34], [37]. Both users and non-users may perceive that they have nothing to hide, and generally that data stored by a smart assistant is not sensitive [22], [24], [31], [37], though there is evidence that users do care about these issues [4].

Users may be unfamiliar with smart assistants and how to manage them. Many are uncertain of how data is collected, managed, and used [1], [24], [33], [38]. User familiarity, and thus knowledge, is heavily correlated to who sets up and configures the smart assistant [33]. Most efforts to encourage adoption of strong privacy practices rely on social triggers, though users may conversely feel obliged to share changes in privacy behaviours with others [7].

When facing difficulties in using a computing device, users may first seek informal help in social networks since official help sources are often limited in scope, cost, and time [29]. Informal controls include unplugging a device, muting it, disabling certain features, and non-technical behaviour changes such as not using the device in certain situations or placing it in different locations [1], [24], [37]. Critically, users may defer to past practices and similar situations, relating perceived risks to attacks on other devices and platforms [1], [22], [27], [31]. Characterising the transferability of past behaviour, and identifying contributing factors for privacy within shared use of smart assistants, would then be a useful direction in improving privacy design and secure use.

D. Privacy concerns

Users may prefer data collection to be in public rather than private spaces, and be highly uncomfortable with devices that collect biometric information [24], [26]. It is an interesting contradiction that users are generally trusting of their smart assistant provider, yet the same companies who make the devices are also considered to be a key potential threat to privacy [1], [38]. The novelty of smart assistants translates to little social support in the guise of informal help from social circles [29]. Therefore, the complexity and unfamiliarity of existing formal privacy controls imposes a burden of security fatigue from what is perceived as excessive measures towards protecting non-sensitive data [27]. Most shared environments raise neither a perceived need for access controls nor privacy issues, due to a social trust among multiple users in the shared smart assistant environment [37] — users may then be relying on trust rather than device configuration, despite advice to users to take steps to secure smart home devices.

E. Summary and research questions

This study explores the contextual dynamics behind privacy behaviours in previous devices, relative to newer, smart home assistant devices. There is an additional challenge of defining a means to monitor and measure the transfer of privacy behaviours across existing, familiar devices and emerging IoT devices such as smart assistants, which has not been adequately framed nor explored in previous work. We explore specific Research Questions (RQs):

- **RQ1.** Does prior experience of sharing or not sharing information through devices play a role in adoption of privacy-related controls with smart assistant devices?
- **RQ2.** Do users perceive opportunities to transfer their existing privacy-related behaviours to the context of using a shared smart assistant device? If so, what are the determining factors?

III. Methodology

With consideration of existing research (Section II) and our research questions (RQs) (Section II-E), we explore the RQs through an exploratory survey of smart assistant users. Given the overwhelming share of Amazon and Google in the smart assistant market [1], we focused on devices using the Amazon Alexa or Google Assistant smart assistant applications.

A. Survey design

In the survey design, Part I addresses RQ1 above (as in the first five of eight question groups below), identifying correlating factors that may contribute to responses in transferable privacy behaviours in Part II (the last three question groups), which moves focus to RQ2. Part II asks directly about transferable privacy behaviours from previous to current devices. Part I supports findings into these transferable changes, or lack thereof, by offering supplementary information and potential underpinning behavioural factors as supporting context.

The survey is made up of 42 mandatory questions divided into groups. Each question group contains a set of related questions. For each question group, there is a main question, the responses for which form a conditional variable that will be tested for significance. This significance refers to whether the factor assessed by this main question has an impact on users' transferable privacy behaviours in Part II. Other questions within a question group support the main question, to capture additional context into user behaviour and perceptions.

Question groups are: Device Information (Q1-Q3); Usage (Q4-Q7); Device Setup (Q8-Q11); Ease of Use and Perceptions of Control (Q12-Q14) (Q14 uses adjectives, as used elsewhere for authentication studies [20]); Privacy Concerns for Multiple Users (Q15-Q20); Previous Shared Device Usage (Q21-Q22); Previous Privacy Control Usage (Q23-Q26); Smart Assistant Privacy Control Usage (Q27-Q31). Survey questions can be found in the Appendix.

B. Participants

100 UK-resident smart assistant users were recruited on the Prolific survey platform. We employed an existing Prolific pre-screen question to filter only for users of a smart home assistant device. 100 complete, valid responses were recorded, where validity entails not failing both attention check questions embedded within the survey. The gender breakdown includes 62 female and 38 male participants, with an average age of 35 years (stdev = 10.949, all at least 18 years of age). We employed convenience sampling and did not control for gender or age distribution in this exploratory survey. Potential privacy-related issues relating to gender are discussed in, e.g., [31]. The average survey completion time was 11.5 minutes and participants were compensated with an average payment of £12.09/hour. We note that payment was configured at £10/hour, and participants tended to complete the survey under our 12 minute estimate (despite an initial configuration phase of 10 participants which aligned with this). 3 participants were excluded from analysis (23:F, 25:M, 30:F) as they reported using a device that was not a Google or Amazon device.

C. Ethics

The survey was approved through university research ethics committee review. The study was designed with consideration of the four principles of the ethical framework for ICT research described in the Menlo Report [8]: Respect for Persons, Beneficence, Justice, and Respect for Law and Public Interest. Use of closed questions prevented personally identifying information from being gathered, where we developed adjective-based questions to capture sentiment where appropriate. Study participation was voluntary, goals of the study were presented before the survey, and participants explicitly stated having understood the study conditions before proceeding to the survey. There was non-discriminatory selection of subjects, barring research pre-screening requirements, and fair compensation.

IV. Results

In this section we describe key results which emerged from analysis of the survey responses.

A. Device information and usage

In line with current market share information and projections, 74 respondents reported using a smart assistant running Alexa while the remaining 23 used a Google Assistant device. The majority of the devices were shared (61 for Amazon, 21 for Google), either with other members of the household or with guests, or both. The duration of ownership for both devices was mostly 1-3 years (61 respondents) or 3-12 months (24 respondents), with only one respondent reporting less than one month of ownership.

Users fall into three categories, a primary user, a secondary user, or a user within a shared dynamic of equal use. 83 of the 97 respondents were primary (52) or equal (31) users, noting that non-shared devices automatically followed that the respondent was a primary user. Most respondents acquired the device themselves and tended to be primary users.

Respondents generally had the impression that they had explicitly provided location, name, and telephone number data to their smart device, and that implicitly the device had access to linked account information, location, name, and telephone number. Notably, 20 respondents indicated that they had not explicitly provided any of the previously mentioned data, although 15 of those 20 stated that such data was instead implicitly given or inferred by the device. 12 respondents indicated that to the best of their knowledge, no information had been implicitly given to the smart assistant through linking accounts even though for each of them, their usage encompassed at least one activity that would provide linked account information, location, or name data.

B. Device setup

Device setup was defined as the process that included configuration, setting up a new account, or replacing a previous account on the smart assistant. Of the 97 responses, 74 respondents were involved in the setup of their smart assistant device, while 23 were not. Amongst the latter, reasoning for this was mostly that they were not the primary user, followed

Previous Device		Current Smart Assistant	
Device Type		**Software Type**	
Computer	43	Amazon Alexa	74
Smart TV	34	Google Assistant	23
Video Game Console	33		
Tablet	27		
Smart Assistant	7		
Phone	5		
Other Mobile Device	1		
Shared	54	**Shared**	82
Not Shared	43	**Not Shared**	15
Total	97	Total	97

TABLE I
BREAKDOWN OF SMART ASSISTANTS AND PREVIOUS DEVICES BY TYPE AND SHARED STATUS.

Privacy Control	**Have Owned Previous Shared Device**	**Have NOT Owned Previous Shared Device**
Incognito/Private/Guest Mode	50%	62.8%
Pausing Device History*	16.7%	4.6%
Clearing Device History	66.7%	67.4%
Application Locks or Restricting Functions*	29.6%	11.6%
Setting Account Passwords	77.8%	65.1%
Other Actions (Obfuscation)*	9.3%	2.3%
Other Actions (Hiding Data)*	16.7%	4.7%
Other Actions (Deleting Data)*	24.1%	4.7%
No Formal Privacy Control Use	11.1%	11.6%
Total Users	54	43

**Difference is a statistically significant multiple*

TABLE II
PERCENTAGE OF PRIVACY CONTROL USAGE ON PREVIOUS DEVICES.

by a belief that they had less technical experience compared to other shared users. Users who share their smart assistant device are split almost evenly into seeking online or IT staff help (32 respondents) versus asking other shared users or family members (33 respondents). Other research has found users consulting only family members for advice, but also a mix of different sources [30].

C. Ease of use and perceptions of control

Approximately half of respondents (48) believed they knew where to access privacy settings on their smart home device. Respondents generally agreed or strongly agreed that they felt comfortable and familiar using their device. When asked if they felt secure using the device, the majority answer was neutral but overall skewed towards agreement. When asked about control of personal privacy, these users gave a majority neutral response with even distribution of answers on each side. Users gravitated towards describing their device in positive terms of convenience rather than security. The terms "easy to use," "helpful," and "useful" each had over 80 responses, while "secure" and "transparent" only had 7 responses each. Privacy-related controls can potentially also be easy to use [1].

D. Privacy concerns for multiple users

20 of the 82 respondents sharing smart assistants noted that they have been in a situation where they had sensitive information that must be kept private from other users. The four most common types of information cited from available options were, in descending order, financial information, information about surprises or gifts, health information, and personal information including political preference, sexual orientation, and personal interests. Meanwhile, 21 of the 82 users of shared smart assistants indicated that they had been in a situation where they would have preferred to keep information private from other users but it was not mandatory.

All respondents reported a preference to have schedule information be kept public. Similarly, call history and buying recommendations are considered not too sensitive but are split evenly between preferences for being kept private and public.

E. Previous shared device and privacy control usage

As in Table I, 54 users had previously used a shared device, while 43 did not. 39 of the 54 respondents indicated that users were able to create an account on the device.

The most frequently used privacy controls in previous devices, whether shared or not, were configuring account passwords, clearing device history, and some version of 'incognito' or private browsing mode. This is correlated to familiarity, as respondents indicated a significant margin of familiarity with using these three popular controls over others.

A notable observation is that respondents used more formal privacy controls on previous non-shared devices than their previous shared devices. Comparing the former to the latter, this includes comparisons of 36 reports to 26 for Clearing Device History, 42 to 35 for Setting Account Passwords, and 13 to 4 for Deleting Data. One can argue that this can be caused by shared devices perceived as having less sensitive information, such as a Smart TVs (34 respondents) or Video Game Consoles (33). Previous shared devices also include computers (43 respondents), tablets (27), and phones (5).

For users who had not previously owned a shared device, when asked about their use of formal privacy controls on non-shared devices, these are illustrated in the right-hand column of Table II. Similar to users who previously had owned a shared device, the distribution of privacy controls strongly favours use of clearing history, configuring passwords, and some form of 'incognito' or private browsing mode.

There were statistically significant differences in the usage rate of users who had and had not owned a shared device previously. Privacy control usage was compared across previous non-shared devices that encompass both of these groups of users, so users who had not previously shared devices would not be impacted by having a smaller range of available privacy controls. Significantly enough, respondents who owned a previous shared device had around 4x higher usage of clearing history, 3x higher usage of using application locks or feature restrictions, 4x higher usage of other methods to obfuscate data, and 6x higher usage of other methods to delete data. In comparing IoT device owners to non-owners,

Privacy Control	Users	User Usage Rate: Users Owned Previous Shared Device	User Usage Rate: Have NOT Owned Previous Shared Device
Amazon Households or Voice Authentication	16	18.5%	14%
Pause History	5	3.7%	7%
Clear History	14	9.3%	20.9%
Autodeletion of Voice Records After Set Duration	3	5.6%	0%
Mute Device	15	24.1%	4.7%
Unplug Device	18	27.8%	7%
Play Sound When Device is Listening	18	13%	25.6%
Application Lock or Feature Restriction	11	5.6%	18.6%
Disable Features	11	13%	9.3%
Account Lock or Voice Authentication	7	9.3%	4.7%
Child Safe Mode	9	9.3%	9.3%
Guest Mode	3	5.6%	0%
Simple Use Other Devices	5	5.6%	4.7%
No Smart Assistant Privacy Control Use	37	40.7%	34.9%

TABLE III
SMART ASSISTANT PRIVACY CONTROL USAGE.

Williams et al. found owners less likely to configure privacy-related settings [35].

F. Smart assistant privacy control usage

60 of 97 respondents reported using some form of privacy control for their smart assistant. 6 of these 60 respondents stated they did not use any privacy control but confirmed that they had used Amazon Households or Voice Authentication, which implies a point of potential confusion. Referring to Table III, 37 respondents did not use any form of privacy control, despite all but two of these were in a shared environment. Experience with a previous shared device was not a significant factor of smart assistant privacy control use, with both groups comparatively likely to not use privacy controls.

Of the smart assistant privacy controls offered, respondents favoured informal controls of muting or unplugging the device. The formal built-in controls or playing a sound when the device is listening, voice authentication, and Amazon households were around equally as popular overall. Unlike traditional privacy control usage in the previous section, there were no strongly favoured smart assistant privacy controls.

Finally, we queried participants directly on why they do not use smart assistant privacy controls. Past research has identified three reasons: unfamiliarity of privacy control use or setup, a lack of awareness that such controls exist, and not considering data to be sensitive (as in Section II). There was no single overwhelming reason provided by the respondents, who were free to select all reasons that applied. 23% responded that they did not know how to use, setup, or access such controls, 29% were not aware that such controls existed, and 29% did not consider their data sensitive enough to warrant using privacy controls. Finally, 18% stated that they did not realise that they wanted to use the privacy controls now. For context, IoT devices and controls may be less familiar than more established technologies such as laptops [35].

G. Transfer of privacy control adoption

Here we consider transferability of privacy behaviours to be where a respondent used at least one sort of privacy control previously, and now uses at least one smart assistant privacy control. 57 respondents managed to transfer some semblance of privacy control usage; 25 did not transfer any privacy control usage; 12 used no privacy controls across previous devices and smart assistants; 3 moved from no privacy controls to using controls with smart assistants. This does not indicate the extent of behaviour transfer; nuanced metrics of transferability across device classes are regarded as future work.

V. DISCUSSION

To revisit RQ1 (Section II-E), respondents who previously used shared devices tended to adopt informal privacy controls at a much higher rate than respondents who had never previously shared a device (Table II). Overall, respondents with previous shared device experience adopted a higher rate of privacy control usage on smart assistants (Table III). A remaining question is if informal privacy controls are more relevant in shared settings; informal methods like hiding a device screen or unplugging the device are potentially more effective at hiding information from internal, shared users rather than malicious, third-party external adversaries (similar to 'holistic security management' of physical spaces [9]). Manufacturers and policymakers could identify privacy controls which can support socially acceptable behaviours, while recognising the role of trust between users [19].

Regarding RQ2, half of respondents reported knowing how to access privacy settings for their smart assistant device. A lack of access to these settings would constitute a significant obstacle to using privacy controls beyond those which are informal or provided directly as an option during setup. Users who cited reasons for not using any smart assistant privacy controls noted foremost a lack of awareness that such controls existed, which may be influenced by not being able to easily access privacy settings. Privacy-related behaviours may be prompted if relevant information is provided with the device [10], with support to identify how to manage related concerns (where here respondents resorted to informal controls).

The privacy controls reported as being used the most across shared and non-shared devices that were not a smart assistant, were passwords, clearing history, and an 'incognito' or private mode. There are no clear equivalent smart assistant privacy controls that dominate usage in the same way as these three popular privacy controls. Mobile and Internet skills can translate into good IoT skills [5], implying a missed opportunity to leverage knowledge of these more familiar controls in a smart home context. Participants tended to use more formal, built-in privacy controls on non-shared devices. and a mix of both formal and informal controls with shared smart assistants. Manufacturers could portray and promote smart assistant privacy controls in ways that would leverage users' existing familiarity with passwords, clearing history, or privacy-preserving usage modes. This could include framing

features to be more recognisable, or explaining privacy controls in familiar formats (such as an app-based data collection audit [37]) or terms familiar to users (where improvements have been seen doing this for private browsing modes [36]). Arguably, instructions provided with devices border on misleadingly minimal [16].

A. Limitations

Due to our closed survey design, participants could not express open-ended responses. The survey was designed iteratively, informed by prior user studies, to collate and best identify appropriate potential user responses. This included categorical and meaningful "Other" options designed to capture non-specific answers. The survey did not engage individuals whose privacy concerns may mean they would not adopt a smart assistant device at all. Similarly, the survey may capture generally amiable device use, with limited use of privacy controls and high levels of trust [19]. This contrasts with shared spaces of monitoring or control (as in tech-abuse [28]), which may arguably benefit most from analysing use of privacy controls.

VI. Conclusions

We conducted an exploratory qualitative survey study of 97 smart assistant owners. We found among our participants that most smart assistant devices were shared and perceived to be in environments where social trust enforced privacy-respecting behaviour more than adoption of privacy controls.

Privacy control usage rates for smart assistants were generally low, with half of participants unsure of where to access privacy settings and reporting only use of simple informal privacy controls, though use of built-in Amazon Households and Google's Voice Authentication were seen. Thus, reported transfer of privacy-related behaviours between prior computing devices and newer smart home devices was generally low in adoption rates of available privacy controls. As a simple measure, users who used privacy controls previously also used at least one smart assistant privacy control.

Our results indicate that the transferability of privacy behaviours across shared smart devices may be difficult to predict. Future work will develop a measure of transferability of privacy-related skills across different device platforms.

References

[1] Abdi, N., Ramokapane, K.M., Such, J.M.: More than smart speakers: security and privacy perceptions of smart home personal assistants. In: Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019) (2019)

[2] Amazon: Alexa features @ amazon.com (last viewed 2nd November 2020), https://www.amazon.com/b?ie=UTF8&node=17934672011

[3] Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J.A., Invernizzi, L., Kallitsis, M., et al.: Understanding the Mirai botnet. In: 26th USENIX security symposium (USENIX Security '17). pp. 1093–1110 (2017)

[4] Barbosa, N.M., Park, J.S., Yao, Y., Wang, Y.: "What if?" predicting individual users' smart home privacy preferences and their changes. Proceedings on Privacy Enhancing Technologies **2019**(4), 211–231 (2019)

[5] de Boer, P.S., van Deursen, A.J., Van Rompay, T.J.: Accepting the Internet-of-Things in our homes: The role of user skills. Telematics and informatics **36**, 147–156 (2019)

[6] Bowles, N.: Thermostats, locks and lights: Digital tools of domestic abuse. https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html (2018), accessed: 03-07-2019

[7] Das, S., Dabbish, L.A., Hong, J.I.: A typology of perceived triggers for end-user security and privacy behaviors. In: Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019) (2019)

[8] Dittrich, D., Kenneally, E., et al.: The Menlo Report: Ethical principles guiding information and communication technology research. Tech. rep., US Department of Homeland Security (2012)

[9] Dourish, P., Grinter, R.E., De La Flor, J.D., Joseph, M.: Security in the wild: user strategies for managing security as an everyday, practical problem. Personal and Ubiquitous Computing **8**(6), 391–401 (2004)

[10] 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. pp. 1–12 (2019)

[11] Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T., Dell, N.: "A stalker's paradise" how intimate partner abusers exploit technology. In: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. pp. 1–13 (2018)

[12] Geeng, C., Roesner, F.: Who's in control? interactions in multi-user smart homes. In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. pp. 1–13 (2019)

[13] Google Store: Google nest compatible smart home devices (last viewed 2nd November 2020), https://store.google.com/us/magazine/helpful_home?srp=/us/product/google_home_learn

[14] Haney, J.M., Furman, S.M., Theofanos, M.F., Fahl, Y.A.: Perceptions of smart home privacy and security responsibility, concerns, and mitigations. In: Symposium on Usable Privacy and Security (2019)

[15] J Kraemer, M., Flechais, I., Webb, H.: Exploring communal technology use in the home. In: Proceedings of the Halfway to the Future Symposium 2019. pp. 1–8 (2019)

[16] Kaaz, K.J., Hoffer, A., Saeidi, M., Sarma, A., Bobba, R.B.: Understanding user perceptions of privacy, and configuration challenges in home automation. In: 2017 IEEE Symposium on Visual Languages and Human-Centric Computing (VL/HCC). pp. 297–301. IEEE (2017)

[17] Kawsar, F., Brush, A.B.: Home computing unplugged: why, where and when people use different connected devices at home. In: Proceedings of the 2013 ACM international joint conference on Pervasive and ubiquitous computing. pp. 627–636 (2013)

[18] Kraemer, M.J., Flechais, I.: Researching privacy in smart homes: A roadmap of future directions and research methods. In: Living in the Internet of Things: Cybersecurity of the IoT. IET (2018)

[19] Kraemer, M.J., Lyngs, U., Webb, H., Flechais, I.: Further exploring communal technology use in smart homes: social expectations. In: Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems. pp. 1–7 (2020)

[20] Krol, K., Parkin, S., Sasse, M.A.: Better the devil you know: A user study of two captchas and a possible replacement technology. In: NDSS Workshop on Usable Security (USEC). vol. 10 (2016)

[21] Kumar, D., Shen, K., Case, B., Garg, D., Alperovich, G., Kuznetsov, D., Gupta, R., Durumeric, Z.: All things considered: an analysis of IoT devices on home networks. In: 28th USENIX Security Symposium (USENIX Security '19). pp. 1169–1185 (2019)

[22] Lau, J., Zimmerman, B., Schaub, F.: Alexa, are you listening? privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. Proceedings of the ACM on Human-Computer Interaction **2**(CSCW), 1–31 (2018)

[23] Lin, H., Bergmann, N.W.: IoT privacy and security challenges for smart home environments. Information **7**(3), 44 (2016)

[24] Malkin, N., Deatrick, J., Tong, A., Wijesekera, P., Egelman, S., Wagner, D.: Privacy attitudes of smart speaker users. Proceedings on Privacy Enhancing Technologies **2019**(4), 250–271 (2019)

[25] Matthews, T., O'Leary, K., Turner, A., Sleeper, M., Woelfer, J.P., Shelton, M., Manthorne, C., Churchill, E.F., Consolvo, S.: Stories from survivors: Privacy & security practices when coping with intimate partner abuse. In: Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems. pp. 2189–2201 (2017)

[26] Naeini, P.E., Bhagavatula, S., Habib, H., Degeling, M., Bauer, L., Cranor, L.F., Sadeh, N.: Privacy expectations and preferences in an IoT world. In: Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017). pp. 399–412 (2017)

[27] Parkin, S., Krol, K., Becker, I., Sasse, M.A.: Applying cognitive control modes to identify security fatigue hotspots. In: Twelfth Symposium on

Usable Privacy and Security (SOUPS 2016) — Workshop on security fatigue (2016)
[28] Parkin, S., Patel, T., Lopez-Neira, I., Tanczer, L.: Usability analysis of shared device ecosystem security: Informing support for survivors of IoT-facilitated tech-abuse. In: Proceedings of the New Security Paradigms Workshop. p. 1–15. ACM (2019)
[29] Poole, E.S., Chetty, M., Morgan, T., Grinter, R.E., Edwards, W.K.: Computer help at home: methods and motivations for informal technical support. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. pp. 739–748 (2009)
[30] Redmiles, E.M., Malone, A.R., Mazurek, M.L.: I think they're trying to tell me something: Advice sources and selection for digital security. In: 2016 IEEE Symposium on Security and Privacy (SP). pp. 272–288. IEEE (2016)
[31] Sambasivan, N., Checkley, G., Batool, A., Ahmed, N., Nemer, D., Gaytán-Lugo, L.S., Matthews, T., Consolvo, S., Churchill, E.: "Privacy is not for me, it's for those rich women": Performative privacy practices on mobile phones by women in south asia. In: Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018). pp. 127–142 (2018)
[32] Shouran, Z., Ashari, A., Priyambodo, T.K.: Internet of things (IoT) of smart home: privacy and security. International Journal of Computer Applications **182**(39), 3–8 (2019)
[33] 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 (SOUPS 2019) (2019)
[34] Westin, F., Chiasson, S.: Opt out of privacy or "go home" understanding reluctant privacy behaviours through the FoMO-centric design paradigm. In: Proceedings of the New Security Paradigms Workshop. pp. 57–67 (2019)
[35] Williams, M., Nurse, J.R., Creese, S.: Privacy is the boring bit: user perceptions and behaviour in the internet-of-things. In: 2017 15th Annual Conference on Privacy, Security and Trust (PST). pp. 181–18109. IEEE (2017)
[36] Wu, Y., Gupta, P., Wei, M., Acar, Y., Fahl, S., Ur, B.: Your secrets are safe: How browsers' explanations impact misconceptions about private browsing mode. In: Proceedings of the 2018 World Wide Web Conference. pp. 217–226 (2018)
[37] Zeng, E., Mare, S., Roesner, F.: End user security and privacy concerns with smart homes. In: Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017). pp. 65–80 (2017)
[38] Zheng, S., Apthorpe, N., Chetty, M., Feamster, N.: User perceptions of smart home IoT privacy. Proceedings of the ACM on Human-Computer Interaction **2**(CSCW), 1–20 (2018)

APPENDIX: SURVEY QUESTIONS

Device Information

Q1. Do you use an Amazon Alexa device, Google Assistant device, or other smart speaker device? If you use more than one, please select the one you use most frequently.

- Amazon Alexa (Echo, Echo Dot, Echo Plus, Echo Studio)
- Google Assistant (Google Home, Google Home Mini, Google Nest Mini)
- Other

Q2. Do you share the use of <*device*> with other people? Please choose all that apply: [Yes, in a shared household | Yes, with guests | No]

Q3. How long have you been using <*device*>? [Less than 1 month | 1-3 months | 3-12 months | 1–3 years | More than 3 years]

Usage

Q4. Are you the main user of <*device*>? [Yes, I use it the most | No, I am not the main user | No, there is no primary user as usage is shared somewhat equally]

Q5. What do you use <*device*> for? Please create a new list on the right of all answers that apply, in order of most frequent to least frequent use. [Shopping | Personal Finances and Banking | Controlling Smart Home Devices (i.e. Thermostat, Lights, Speakers) | Play Games | Playing and Controlling Music | Watch or Stream Media/Radio/TV | Question and Answer Queries (i.e News, Weather, What's Nearby, Recipes) | Scheduling/Productivity (i.e. Calendar, Alarms, Timers, Notes) | Fitness | Calling and Messaging | Other (Recreation) | Other (Productivity)]

Q6. To the best of your knowledge, which of the following types of information have you directly and explicitly provided to <*device*>, through either voice queries or through configuring settings? * Please choose all that apply: [Location | Full Name | Telephone Number | Address | Health Data | Financial Data | Other Personal Data | Other Non-Personal Data | I have not directly provided any of the above]

Q7. To the best of your knowledge, what types of information do you think you may have provided indirectly? This means information that <*device*> gathers indirectly through linking other accounts rather than your directly providing it through voice queries of configuring settings. * Please choose all that apply: [Location | Full Name | Telephone Number | Address | Health Data | Financial Data | Linked Amazon or Google Account (i.e. Purchasing Data) | Linked App Data (i.e. Spotify, Uber, Netflix) | Linked Smart Home Device Usage Data (i.e Thermostat, Alarm System) | Other Personal Data | Other Non-Personal Data | I have not indirectly provided any of the above]

Device Setup

Q8. To the best of your knowledge, who purchased <*device*>, or how did you come to acquire it? [Myself | Partner | Family Member | Friend | Acquaintance or Colleague | Company or Workplace | A Gift | Provided as part of service subscription, contract, or came with something else]

Q9. Were you involved in the setup of <*device*>? [Yes | No]

Setup involves configuring your device out of the box, setting up a new account onto your device, or replacing a previous account with a new one.

Q10. Since you answered NO above, do any of the following suitably describe why? *Please choose all that apply: [I am not the primary user | I will not use it frequently | I do not own the smart assistant | I believe I have relatively less technical expertise than the person(s) I share this device with | Setup and technical support were already included before I acquired or started using it | I am content with the defaults and am not interested enough to set it up | I dislike using <*device*>]

Q11. Do you rely on another user that shares the device for technical help when adjusting settings, resolving usage problems, or using <*device*>? [Yes | No, if I don't know how to do it then I don't use it | No, I will seek outside help via online or IT staff | No, I will seek outside help from a family member or friend]

Ease of Use & Perceptions of Control

Q12. Are you familiar with where to access privacy settings for <*device*>? [Yes | No]

Q13. Having a shared <*device*> I can say that I feel [OR **Q13B.** If I were to share usage of my device, I think that I would feel]:

(rated on a five-point scale, from Strongly Disagree to Neutral to Strongly Agree)

Am Comfortable Using it
Am Familiar with Using its Functions
Feel Secure Using it
In Control of My Privacy

Q14. Please select all the phrases that apply. <*device*> is: * Please choose all that apply:

NOT CLEAR	TRANSPARENT
CONFUSING	EASY TO USE
NON-SECURE	INTUITIVE
CONFUSING	SECURE
LIMITED FEATURES	HELPFUL
INTRUSIVE	LEARNING
USELESS	USEFUL

Privacy Concerns for Multiple Users

Q15. Have you ever been in a situation where you HAVE to keep certain pieces of information private from other users? [Yes | No]

(IF 'Yes' to Q15) **Q15Y.** In the situation above, which type(s) of information did you feel you MUST keep private from other users? For multiple answers, please rank from most sensitive to least sensitive.

- My Personal Information (i.e. sexual preference, political preferences, personal interests)
- Personal Information about Other Users
- Surprises or Gift Information (i.e. surprise presents for other users, planning events without another user's knowledge)
- Financial Information
- Work Product
- Health Information
- There are underage users who preferably should not access my information for purchases or mature content

Q16. Have you ever been in a situation where you would PREFER to keep certain pieces of information private from other users? Only answer this

question if the following conditions are met: Answer was NOT 'No' at Q2. (Do you share the use of <*device*> with other people?) [Yes | No]
(IF 'Yes' to Q16) **Q16Y.** In the situation above, what type(s) of information would you have PREFERRED to keep private from other users? For multiple answers, please rank from most sensitive to least sensitive. [*same options as Q15Y)* | Miscellaneous]
Q17. Whether the device is shared or not, please describe the sensitivity level of the following types of information: * Please choose the appropriate response for each item: (For the responses below, participants select from a Likert Scale of 1. Not Sensitive At All or Already Public, 2. Not Really Sensitive, 3. Neutral, 4. Sensitive, and 5. Highly Sensitive) [My schedule | My call history | My search history | Buying recommendations | Access to my Amazon, Google, or device account | Access to connected devices | Health Information]

Please give your best general (average) answer.
Q18. Whether <*device*> is shared or not, what information would you NOT mind being made available to other potential users? *Please choose all that apply: [My schedule | My call history | My search history | Buying recommendations | Access to my Amazon, Google, or device account | Access to connected devices | Health Information | Other Personal Information | Other Usage Information | Other Productivity or Work Product | None of the above should be made available for other users]
Q19. Which user(s) do you share <*device*> with? Please choose all that apply: [My partner or spouse | Other adult family member I share the home with | Child I share the home with | A friend | A close friend | A work or school colleague | An invited guest | I do not share <*device*> with anyone else]
(IF last option selected for Q19) **Q20.** For each user selected above, which piece(s) of your personal data would you NOT mind that person having access to via <*device*>: (For each user selected in Q19, participants checked the boxes below if applicable) [*same options as Q17)* | None of the above should be made available for other users]

Previous Shared Device Usage A shared device is a device shared amongst several people, i.e. a shared home computer, a shared game console, a smartphone used by you and your partner, a work tablet shared with your colleague, etc.
Q21. Have you ever used a shared device other than your current <*device*>? [Yes — No]
(IF 'Yes' to Q21) **Q21Y.** Which shared devices have you used before? *Please choose all that apply: [Phone | Computer | Tablet | Video Game Device (Xbox, Playstation, Wii, etc.) | Smart Television | Smart Assistant | Other (Mobile Device) | Other (Non-mobile Device)]
(IF 'Yes' to Q21) **Q22.** Which actions are other users able to do on the shared device(s) you have used other than your smart speaker device(s)? *Please choose all that apply: [Use the device | Change data on the device | View data on the device | Access and modify settings on the device | Create an account on the device]

Previous Privacy Control Usage The following section asks about privacy control usage for shared device(s) you have used previously or are using now, that is NOT <*device*>.
(IF 'Yes' to Q21) **Q23A.** To the best of your knowledge, which privacy controls have you previously used on a SHARED device other than your smart speaker device(s)? *Please choose all that apply: [Incognito/Private/Guest Mode | Pausing Device History | Clearing Device History | Application Locks or Restricting Access to Certain Functions | Setting Account Passwords | Other Actions to Obfuscate Data | Other Actions to Hide Data | Other Actions to Delete Data | I have not done any of the above]
Q23B. To the best of your knowledge, which privacy controls have you used before on a NON-SHARED device (a personal device which you do not share with anyone)? *Please choose all that apply: [*(same options as in Q21)* | I have not used a device solely owned by me]
(IF 'Yes' to Q21) **Q24.** On the shared device(s) you've used previously, have you deliberately done any of the following more than once to maintain your privacy from other users? *Please choose all that apply:

- Deliberately use device only when no one else is around or when unmonitored
- Physical privacy screen
- Hide or physically block screen
- Hiding the device or blocking access to the device
- Other methods to hide current use or activity
- Other methods to hide past usage history or activity
- I have not done any of the above

Q25. (Attention check question)
Q26. Which privacy controls would you consider yourself to be familiar with? *Please choose all that apply: [*(same as Q21, except last option, as below)* | I am not familiar with any of the above]
Q26A. For each privacy control selected above, please indicate your level of familiarity with each: (For every response selected in Q26, participants rank from Not Familiar (1) to Familiar (3) to Very Familiar (5) on a Likert Scale)

Smart Assistant Privacy Control Usage
Q27. Do you use (or are part of) Amazon Households, Google Voice Match, or any other type of software that supports managing multiple users? [Yes | No | I don't know what that is | I've heard of it but have not used it]
Q28. Which privacy controls do you use with <*device*>? * Please choose all that apply: [Pause Search History | Clear Search History — Automatic data deletion after a certain period of time | Mute <*device*> | Unplug <*device*> | Play a sound when <*device*> is listening | Controlling Access to Certain Skills | Disabling Features | Account Lock or Voice Authentication | Child-safe Mode | Guest Mode | Simply Use Other Devices | I do NOT use any privacy controls]
(IF any option other than last option selected for Q28) **Q29A.** For each of the privacy controls selected above, please state whether it is easy or intuitive to use, or not: (For the answers chosen in Q28, participants state whether it is 'Easy and Intuitive to Use' OR 'Easy nor Intuitive to Use')
(IF any option other than last option selected for Q28) **Q29B.** For each of the privacy controls selected above, please rate your level of satisfaction for each on the following scale: Dissatisfied - does not deliver the privacy that you seek; Neutral - delivers adequate privacy but could do better; Very Satisfied - effectively delivers the privacy you seek

(For the answers chosen in Q28, participants rank on a Likert Scale their satisfaction from Dissatisfied (1) to Neutral (3) to Very Satisfied (5).)
(IF only the last option was selected for Q28) **Q30.** If you do NOT use any of the privacy controls listed above, why do you think that is? Please select the best response(s) that apply: *Please choose all that apply: [I do not know how to use these controls | I was not aware that these controls existed | I do not consider my data on <*device*> to be particularly sensitive | I did not realize that I wanted to use these controls until now]
Q31. Which privacy control(s) would you like to use or see in the device? Please create a list on your right, ordered from highest to lowest preference.

- Guest Account or Incognito/Private Mode (i.e. allowing visitors or guests to use the smart assistant without using your linked account information)
- Voice Commands to Pause Search History (i.e. when shopping for a surprise birthday gift)
- Voice Commands to Clear Search History (i.e. to stop previous search history from being used in recommendations)
- Automatic Data Deletion (<*device*> only stores information for a set duration i.e. 3 months)
- Automatic Data Deletion of Guest Users (i.e. <*device*> will recognize guest users and not store their data)
- Automatic Data Deletion of Underage Users (i.e. device will recognize children and not store their data)
- Offer a Range of Default Privacy Settings (i.e. from Very Private to Normal) so you can quickly set up different privacy presets
- Locks for Certain Skills (i.e. a lock for playing games or checking bank statements)
- Account Lock or Voice Authentication (i.e. requiring a passcode or voice authentication to use your account)
- Child-Safe Mode (i.e. parental controls or preventing access to certain features)
- Other Desired Function (Concerning Storage of Personal Information)
- Other Desired Function (Concerning Processing of Personal Information)
- Other Desired Function (Concerning Transparency and Usability of Personal Information)

Closing
Finally, how confident are you in the correctness of the answers you've provided? [Not Very Confident — Relatively Confident — Very Confident] Thank you for participating in this study.