Smart Home Device Loss of Support: Consumer Perspectives and Preferences

Julie M. Haney[0000−0002−6017−9693]* and Susanne M. Furman[0000−0002−7013−6603]*

National Institute of Standards and Technology, Gaithersburg MD 20899, USA
{julie.haney, susanne.furman}@nist.gov

Abstract. Unsupported smart home devices can pose serious safety and security issues for consumers. However, unpatched and vulnerable devices may remain connected because consumers may not be alerted that their devices are no longer supported or do not understand the implications of using unsupported devices. To investigate the consumer perspective on loss of manufacturer support, we conducted a survey of 412 smart home users. We discovered differences based on device category and provide insights into how user perspectives may relate to perceptions of smart home update importance, security, and privacy. Based on the results, we offer suggestions to guide the efforts of the smart home community to protect consumers from potentially harmful consequences of unsupported devices.

Keywords: smart home · internet of things· support · security · privacy.

1 Introduction

The Internet of Things (IoT) industry is a fast-growing, constantly evolving tech sector. This growth can be especially observed in the consumer smart home device market, with about half of all United States (U.S.) households using at least one device [23] and a projected annual growth rate of 14% [27]. There is a constant churn of both products and companies coming in and out of the market [25] [27], with manufacturers prioritizing their efforts on developing and releasing products with the newest technologies and features to maintain their competitive edge. This "planned obsolescence" – instilling in consumers the desire to own something newer, better, and sooner than necessary [16] [20] – is common in the IoT market.

Given the focus on innovation, there may be few economic incentives for providing updates (functional and security) and long-term support to IoT devices, particularly those considered low-end and disposable [12] [28]. Furthermore, because of the rapid evolution of technology and security threats and mitigations, manufacturers cannot "future-proof" products with long lifespans [14], such as smart appliances, door locks, or even single-function devices like lightbulbs or

* Designated as co-first authors

smart plugs. For example, current encryption algorithms may eventually become obsolete, but devices may not be able to accommodate future advances due to processing or memory limitations. Therefore, it is likely that many smart home devices will outlast manufacturers' support commitments.

Unsupported devices can pose serious safety and security issues for consumers, especially since smart home devices may have access to sensitive data or directly make changes to the home environment. As new security threats evolve, unsupported, connected devices will remain unpatched and vulnerable. Consumers may not be alerted that their devices are no longer supported or may not understand the implications of using unsupported devices [15]. In addition, consumers may unknowingly buy discontinued products that are vulnerable from the moment they are connected or soon after as end-of-life, but new-in-box smart home devices are currently being sold on popular online marketplaces. For example, when this paper was written, there were two active listings on an e-commerce site for a new smart hub, which was discontinued in 2018. Multiple smart televisions listed as discontinued on the manufacturer's website were available for purchase on a popular electronics retailer site without any warnings.

Despite the potentially harmful impacts on consumers, little is known about consumers' perspectives on the loss of manufacturer support for smart home devices and how they might best be informed of the safety and security implications. Our study begins to address these unknowns. This paper presents a subset of results focused on manufacturer support from a broader survey study to explore consumers' perceptions of and experiences with smart home updates. The survey involved participants who were active users of smart home devices in five categories of interest: virtual voice assistants, smart thermostats, smart security devices, smart environment sensors, and smart lighting. Related to manufacturer support, we sought to answer the following research questions:

RQ1: What are consumers' concerns regarding loss of manufacturer support for their smart home devices?
- (a) How do responses differ among device categories?
- (b) How do consumers' perceptions of the importance of smart home updates relate to their concerns for loss of support?
- (c) How do consumers' concern levels for smart home security and privacy relate to their concerns for loss of support?
- (d) Is there a relationship between concerns and consumers having prior Information Technology (IT) job experience?

RQ2: What actions, if any, would consumers take if their devices were no longer supported?
- (a) How do responses differ among device categories?

RQ3: How would consumers prefer to be notified about loss of support?

Our study makes several contributions. We develop a better understanding of smart home device support loss from the perspective of consumers, discovering differences in consumers' perceptions and actions based on device category. We also provide insights into how these perspectives relate to perceptions of smart

home security, privacy, and updates. Based on the results, we offer suggestions to guide efforts of smart home stakeholders – manufacturers, standards developers, regulators/oversight organizations, and consumer advocacy groups – to inform and protect consumers from physical safety and online security consequences of unsupported, connected devices.

This paper is organized as follows. In section 2 "Methodology," we describe our survey development, data collection and analysis process, and limitations of the study. In section 3 "Participants and Devices" we provide an overview of the survey respondents, their demographics, and the types of devices they owned. We present our findings in section 4 "Results." Finally, in section 5 "Discussion and Related Work," we situate our study within prior literature and other related industry and government efforts and offer suggestions on how consumers may be better informed and empowered when their smart home devices lose support.

2 Methodology

2.1 Survey Development

Because of the diversity of smart home devices, we focused the survey on five device categories of interest:

- ***virtual voice assistants/smart speakers***, e.g., Amazon Echo/Alexa, Google Home, Apple HomePod
- ***smart thermostats***, e.g., Nest, Ecobee
- ***smart security devices***, e.g., cameras, door locks
- ***smart environment sensors***, e.g., smoke/leak detectors
- ***smart lighting***, e.g., light bulbs, lighting systems

We selected these categories since they are among the most popular in U.S. households [23] [29], represented varying levels of sophistication, and were likely to elicit a range of consumer security and privacy concerns [30] [34] [35].

Survey questions were informed by our research questions and prior work on software and IoT updates (e.g., [9] [17] [31]). To ensure survey content and construct validity, an IoT security expert, a survey methodologist, and two individuals representative of our target survey population provided feedback used to refine the survey. Appendix A contains the survey questions relevant to this paper, which included select one answer, select all that apply, and Likert scale formats. To explore potential differences between device categories, for some survey items, participants answered the same question for all categories they owned. In these cases, a matrix of items was presented to the participant. Only those device categories the participant owned were displayed in the matrix. Figure 1 shows an example question of this type as displayed for a participant who owned devices in all categories.

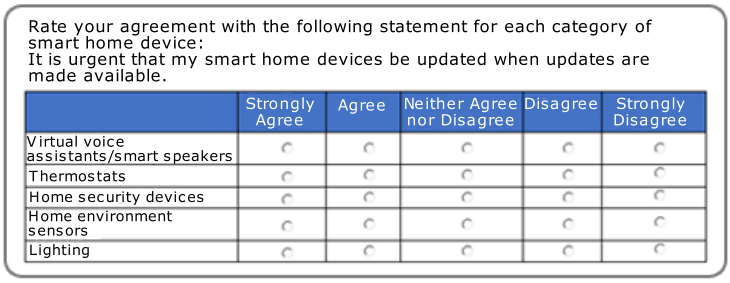

Fig. 1. Example question with multiple device categories

2.2 Data Collection

The study was approved by our institution's Research Protections Office, and the survey was fielded for two weeks in April 2021. On the first screen of the survey, participants were provided with an information sheet describing the study and how their data would be protected. Survey responses were collected without personal or machine identifiers. After finishing the survey, participants received $12.50.

We hired an independent research company that utilized the Prodege non-probability, online opt-in sample panel to recruit a demographically diverse set of participants. With millions of panelists and thousands of demographic and behavioral attributes, Prodege allowed for granular demographic targeting and recruitment that could be adjusted on a daily basis to fill gaps in desired demographics as the survey timeframe progressed. Prodege also had a smart home ownership attribute that facilitated efficient sample targeting. To be eligible for the survey, participants had to be adults living in the U.S. who were active users and administrators of smart home devices in at least two of the five device categories of interest. A total of 412 participants completed the survey.

2.3 Data Analysis

We calculated descriptive statistics (percentages rounded to nearest whole numbers) to report response frequencies. We also conducted inferential statistics using non-parametric tests since the data were not normally distributed. To look for differences between device categories for ordinal (Likert scale) responses, we used the Kruskal-Wallis H test at the significance level $\alpha < 0.05$. For categorical responses, we used Chi-square tests of association as an initial test, with post-hoc Chi-square pairwise comparisons, applying the Bonferroni correction to counteract potential issues with multiple comparisons, with adjusted significance level $\alpha < 0.01$ (0.05 / 5 device categories). We report significant results by providing the Chi-square statistic (χ^2) and degrees of freedom (df).

In addition to understanding participants' views of potential loss of manufacturer support, since smart home updates are discontinued after manufacturers

cease support, we wanted to know if those who placed more importance on updates were more concerned about the loss of manufacturer support. We also examined whether the level of security or privacy concern was related to concerns about loss of support, since unsupported products may become targets of cyber attacks if new vulnerabilities are discovered. Lastly, we looked for potential correlations between these various concerns and consumers' self-reported IT job experience since marked differences have been observed in the sophistication and accuracy of security and privacy mental models and risk understanding between experts and non-experts [19]. We calculated Kendall rank correlations to determine these relationships, with significant correlations ($\alpha < 0.05$) reported with the Kendall's Tau (τ) correlation coefficient.

2.4 Limitations

Like all self-report data, our survey is limited in that responses only capture participant intentions and perceptions, which may not reflect actual behaviors. However, perceptions can and do influence behaviors [26]. Moreover, our results only represent the attitudes of a U.S. population, but individuals in other countries may have different perceptions. Finally, since we only included five device categories in the survey and the overarching study was primarily focused on updates (not manufacturer support), we did not include smart entertainment devices or smart appliances as categories of interest. However, we acknowledge that these categories represent a sizable share of the market and may be impacted by loss of support due to their higher costs and longer lifespans.

3 Participants and Devices

Participant were from 47 U.S. states and one U.S. territory and represented a wide range of age, race, education, and income groups. Only 16% (n = 65) reported having prior or current job experience in the IT, security, or privacy fields. Other participant demographics can be found in Table 1.

Among the categories of interest, voice assistants were owned by the most participants (83%, n = 341). Security devices were owned by 65% (n = 268), sensors 52% (n = 215), lighting 50% (n = 204), and thermostats 43% (n = 177). Including devices not in those categories (e.g., entertainment devices, appliances, and smart plugs), participants owned an average of 9 devices, with 34% having 2-5 devices, 31% with 6-9 devices, and 35% with 10 or more devices.

4 Results

Because questions could be skipped and the number of participants with each device category varied, we include the number of total responses (n) in our results.

Table 1. Participant Demographics (N = 412)

Demographic	Sub-category	n	%
Age Range (years)	18 - 24	35	9%
	25 - 34	55	13%
	35 - 44	107	26%
	45 - 54	37	9%
	55 - 64	71	17%
	65+	107	26%
Gender	Male	169	41%
	Female	241	58%
	Prefer to self-describe	2	<1%
Race*	White	301	73%
	Black	78	19%
	Asian	31	8%
	Pacific Islander	2	<1%
	No answer	3	<1%
Ethnicity	Hispanic or Latino	71	17%
	Not Hispanic or Latino	335	81%
	No answer	6	<2%
Education Level	Less than high school	11	3%
	High school	62	15%
	Some college	83	20%
	Associate's degree	47	11%
	Bachelor's degree	148	36%
	Graduate degree	60	15%
IT, Security, or Privacy Job Experience	No	347	84%
	Yes	65	16%
Household Income	Less than $50,000	145	35%
	$50,000 - $99,000	161	39%
	$100,000 - $149,999	68	17%
	$150,000+	34	8%
	No answer	4	1%
U.S. Region	Northeast	86	21%
	Midwest	71	17%
	South	167	41%
	West	84	20%
	U.S. Territory	1	<1%
	No answer	3	<1%
Urbanicity	Rural	68	16%
	Suburban	213	52%
	Urban	131	32%
Smart Home Experience	Less than 1 year	15	4%
	1 - 2 years	122	30%
	3 - 5 years	198	48%
	6+ years	76	18%
	No answer	1	<1%

* Participants could select more than one option.

4.1 Update Importance

We asked participants to rate their agreement that smart home device updates are important on a 5-point scale from strongly disagree to strongly agree for each of the device categories they owned (Fig. 2). Updates for security devices were rated as most important (strongly agree or agree) by 90% of participants, followed closely by sensors at 89%, voice assistants at 86%, and thermostats at 85%. Lighting devices were the lowest rated, although still viewed as important by 77%.

We found a significant but weak correlation between ratings of update importance and IT experience for the voice assistants category only ($\tau = 0.16$). Those with IT experience rated voice assistant update importance higher.

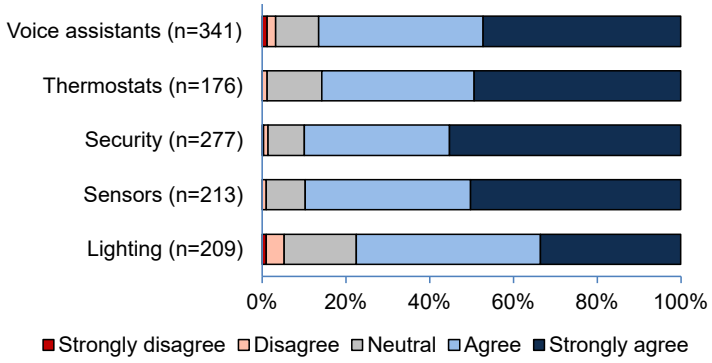

Fig. 2. Agreement with statement: "It is important for smart home devices to be updated"

4.2 Security and Privacy Concern

Participants rated their level of security and privacy concern on a 5-point scale from "not at all concerned" to "extremely concerned" (Fig. 3). They also could select an "I don't know/I'm not sure" option.

Smart security devices had the highest levels of security concern, with 43% of participants moderately or extremely concerned, followed by voice assistants (38%), sensors (35%), thermostats (33%), and lighting (28%). Depending on category, 37-55% were not at all or only slightly concerned about device security, with lighting devices eliciting the least concern. The level of security concern was higher for those with IT job experience for thermostats ($\tau = 0.21$), sensors ($\tau = 0.14$), and lighting ($\tau = 0.17$).

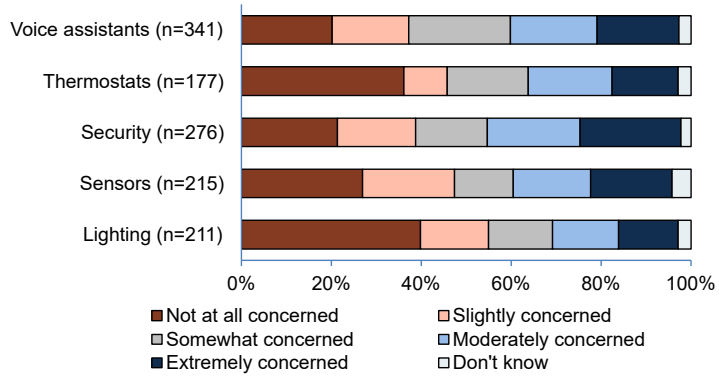

Fig. 3. Level of security concern with smart home devices

When rating their level of privacy concern (Fig. 4), 44% of participants were moderately or extremely concerned about voice assistants, 43% for security devices, 34% for thermostats, 32% for sensors, and 27% for lighting. Over half of participants were not at all or only slightly concerned about the privacy of data collected by their thermostats, sensors, and lighting devices. The level of privacy concern was higher for those with IT job experience for the thermostats ($\tau = 0.14$) and lighting ($\tau = 0.16$) categories only.

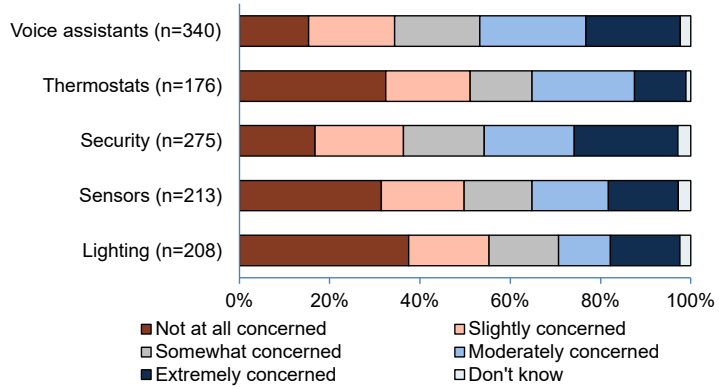

Fig. 4. Level of privacy concern for smart home devices

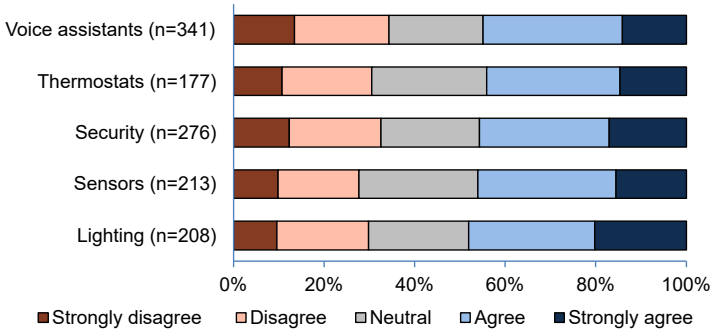

Fig. 5. Agreement with statement: "I am concerned that the manufacturer will eventually stop supporting my smart home devices."

4.3 Loss of Manufacturer Support

Level of Concern Participants rated their level of agreement (5-point scale ranging from "strongly disagree" to "strongly agree") with the following statement: "I am concerned that the manufacturer will eventually stop supporting my smart home devices." For each of the device categories, less than half agreed or strongly agreed that they were concerned about loss of support (Fig. 5): 48% lighting, 46% security devices and sensors, 45% voice assistants, and 44% thermostats.

No significant response differences were found between device categories, and responses were not correlated with perceptions of update importance nor IT job experience. However, there were significant but weak correlations for the level of security concern for all device categories: voice assistants ($\tau = 0.28$); thermostats ($\tau = 0.3$); security devices ($\tau = 0.3$); sensors ($\tau = 0.29$); and lighting ($\tau = 0.31$). Similarly, there were significant correlations to level of privacy concern for all categories: voice assistants ($\tau = 0.21$); thermostats ($\tau = 0.22$); security ($\tau = 0.22$); sensors ($\tau = 0.22$); lighting ($\tau = 0.24$).

Specific Concerns We asked participants what specific concerns, if any, they might have if their devices were no longer supported. Fig. 6 shows the percentages of responses by device category. For all device categories, the most common concern was that devices would stop working (ranging from 39-48%), followed by security updates/fixes no longer being released (31-42%).

We looked for differences among categories for each of the 7 response options. For the option "Updates containing non-security bug fixes no longer being released," there was a significant difference between security devices and lighting ($\chi^2 = 15.85$, df = 1). For "New features no longer being added," there were differences between lighting and all other categories: voice assistants ($\chi^2 = 9.6$, df = 1); thermostats ($\chi^2 = 7.03$, df = 1); security devices ($\chi^2 = 14.89$, df =

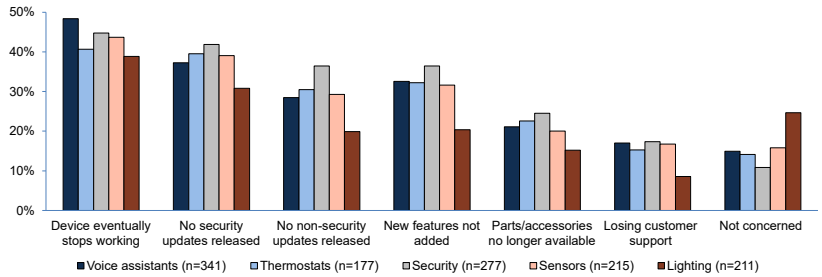

Fig. 6. Specific concerns if manufacturer support is lost

1); and sensors ($\chi^2 = 6.99$, df = 1). Finally, for those selecting "I would not be concerned," there were significant differences between lighting and the following categories: voice assistants ($\chi^2 = 8.06$, df = 1); thermostats ($\chi^2 = 0.7$, df = 1); and security devices ($\chi^2 = 16.35$, df = 1).

Table 2. Significant correlations (τ) between support concerns and update importance, level of security concern, and level of privacy concern. - indicates a lack of significant correlation.

Concern Option	**Update Importance**	**Security Concern**	**Privacy Concern**
Device eventually stops working	Therm (0.1884) Sec (0.1211)	-	Sen (-0.1259)
No security updates released	Therm (0.1938) Sec (0.1318) Sen (0.1345)	Light (0.1744)	-
No non-security updates released	-	Light (0.1974)	-
New features no longer added	Sec (0.1298)	-	-
Not concerned	-	Voice (-0.1383) Therm (-0.1478) Sec (-0.1707) Sen (-0.1863) Light (-0.3255)	Therm (-0.1974) Sec (-0.1395) Sen (-0.1558) Light (-0.217)

Voice = voice assistants; Therm = thermostats; Sec = security devices; Sen = sensors; Light = lighting

In exploring potential relationships between each response option and update importance, level of security concern, and level of privacy concern, we found several significant correlations (see Table 2), most notably a negative correlation

between not being concerned and: level of security concern (all categories) and level of privacy concern (4/5 categories). In other words, those who selected the option that they did not have support concerns had lower levels of security and privacy concern.

Actions Participants indicated what action they would take if their devices were no longer supported. Fig. 7 shows responses by device category. The most popular action for voice assistants, thermostats, and lighting was replacing the device eventually but not right away (37%, 36%, and 32% respectively), while participants with security devices and sensors most frequently selected replacing as soon as possible (39% and 40%). Fewer participants (5-10%) selected throwing out the device without replacement. Between 11% and 20% said they would do nothing (highest for lighting), and 6-9% said they were not sure what they would do. Significant differences were found only between lighting-security devices (χ^2 = 15.1, 4 df) and lighting-sensors (χ^2 = 13.2, df = 4), with participants more likely to do nothing or throw out their lighting devices without replacement and less likely to immediately replace them.

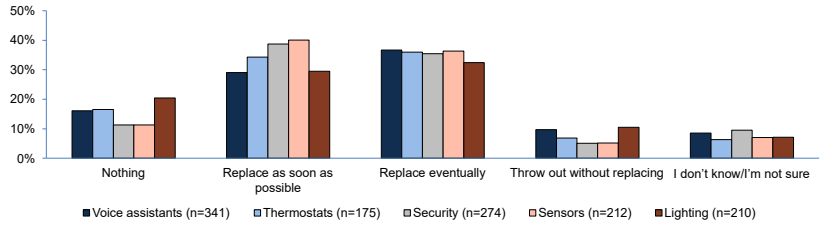

Fig. 7. Actions if manufacturer support is lost

Notification Preferences We asked participants how they would prefer to be notified that their devices would no longer be supported. Of the 400 participants who answered this question, the most popular method was email (45%), followed by receiving a message in the smart home device companion app (31%) and a letter or postcard in the mail (19%). Only 6% said that they would prefer not to be notified.

5 Discussion and Related Work

While the majority of participants believed that it is important for smart home devices to be updated, their levels of concern for support loss were much lower.

This contradiction implies that some consumers do not fully understand the implications of unsupported devices. Therefore, we offer suggestions on how manufacturers and third parties might better inform and empower consumers. We also situate our findings within related research literature. While prior studies have explored planned obsolescence and consumer responses (e.g., [16] [20], none have specifically addressed smart home obsolescence.

5.1 Proactive Communications

Proactive communication by the manufacturer can be a first step towards consumer empowerment. In line with recommendations from U.S. Government agencies and researchers, manufacturers should provide consumers with information about their end-of-life support policy, expected lifespan, when security patches will no longer be provided, and how to sign up for notifications about changes to support [13] [15] [20] [11] [22].

Product labels are one way to provide pre-purchase support disclosure. Based on prior research [7], Carnegie Mellon proposed an IoT security and privacy label that includes how long security updates will be available and whether devices will automatically receive updates [3]. Other researchers found that security update labels, especially those focused on how long the manufacturer guarantees to provide updates, may have a significant impact on consumer product selection [21]. To that end, several governments have proposed IoT security labels that include an expiry date that specifies when security updates will no longer be available [4] [6]. However, future work should be done to examine potential issues of including an expiry date on a label. For example, a study commissioned by the UK Government found that consumers were often confused about what the expiry date meant [18]. An Australian Government survey of 6,000 citizens revealed that a third of respondents mistakenly believed that a device with an expiry label came with an extended warranty up to the date on the label, and 20% thought the device would stop working on the date on the label [2]. In addition, it might be difficult for manufacturers to predict how long they will be able to maintain security updates given the speed at which technology and security threats change [14].

We found that many participants did care about security and privacy (particularly those with prior IT job experience) and indicated that loss of security updates was a major concern. However, participants with lower levels of security and privacy concern had less concern about loss of support. Therefore, we see a need to proactively raise awareness of smart home security, including the link between manufacturer support and security. This awareness is especially essential for device categories viewed as less important from a security/privacy and update perspective (e.g., thermostats, sensors, lighting devices) but which still have the potential to introduce vulnerabilities into the home network and affect higher-valued systems and information.

5.2 Aiding Consumers When Support Ends

To help consumers when device support ends, manufacturers should inform consumers of changes to device support in a timely manner, for example, via the notification methods most preferred by our participants (email or message in the device app). A dynamic, online product label that provides current security status may also help consumers keep abreast of support changes [22]. However, it should be noted that an appreciable number (19%) of consumers desired mail notification. This may be due to people being overwhelmed by electronic notifications and emails [32] and desiring more noticeable communication of support changes.

Support-related notifications are essentially a type of risk communication. Therefore, communicators (e.g., manufacturers) should follow security risk communication guidelines, including: using clear and concise language; being realistic about consequences (not downplaying the risk of negative impacts); providing clear and precise directions for action; and visually highlighting key information [36,24]. Translating those guidelines into the smart home context, consumers should be made aware of both the security and non-security (e.g., safety and functionality) implications of loss of support so they can make informed decisions about whether to continue using their devices and what additional protections should be enacted. Additionally, consumers should be told what options, if any, they have to safely continue using their unsupported devices. For example, if unsupported devices can still function without support outside the home network (e.g., cloud services), consumers could have the option of turning off connected capability or limiting operation of the device to the home network.

Options that allow consumers to safely continue using unsupported devices are especially desirable from a sustainability perspective to reduce waste of products that are discarded due to obsolescence [1]. Similar to prior research findings about how consumers respond to planned obsolescence [20], in our survey, a low percentage of participants said they would throw out the device without replacing it, but many said they would replace the device, leaving uncertainty about what will happen to the old devices. We acknowledge that this decision may be influenced by the state of the deprecated device, i.e., if device functionality is outwardly impacted after discontinuation of support. Global organizations are currently working on the problem of IoT sustainable development [33], with future user-centered research needed to determine how older products might continue to be easily updated and used by consumers (e.g., via modularization [14]).

Third parties (e.g., standards organizations, consumer advocacy groups, government agencies, and policymakers) may also play an important role in helping consumers navigate loss of support. These entities can encourage and set standards for manufacturers to document and communicate support issues (e.g., as in [8] [10] [5]), require organizations to purchase supported devices only and have a plan for loss for support, and engage retailers to pull unsupported devices from their stock.

Disclaimer

Certain commercial companies or products are identified in this paper to foster understanding. Such identification does not imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the companies or products identified are necessarily the best available for the purpose.

Acknowledgements

We would like to thank our colleagues Yee-Yin Choong and Barbara Cuthill for their comments that helped improve the paper.

References

1. ATT. End of life, unsupported IoT devices. https://securityinnovation.att.com/stories/end-of-life-unsupported-devices/, August 2020.
2. Behavioral Economics Team of the Australian Government. Stay smart: Helping consumers choose cyber secure smart devices. https://behaviouraleconomics.pmc.gov.au/sites/default/files/projects/beta-report-cyber-security-labels.pdf, 2021.
3. Carnegie Mellow University. IoT security and privacy label. https://iotsecurityprivacy.org/, 2020.
4. Department for Digital, Culture, Media & Sport, United Kingdom. Consultation on the government's regulatory proposals regarding consumer Internet of Things (IoT) security. https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security/consultation-on-the-governments-regulatory-proposals-regarding-consumer-internet-of-things-iot-security#the-top-three-guidelines, February 2020.
5. 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.
6. Department of Home Affairs, Commonwealth of Australia. Code of practice: Securing the Internet of Things for consumers. https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf, 2020.
7. Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. Exploring how privacy and security factor into IoT device purchase behavior. In *CHI Conference on Human Factors in Computing Systems*. ACM, 2019.
8. ETSI. ETSI EN 303 645 V2.1.1 CYBER; cyber security for consumer Internet of Things: Baseline requirements. https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf, 2020.
9. Michael Fagan, Mohammad Maifi Hasan Khan, and Ross Buck. A study of users' experiences and beliefs about software update messages. *Computers in Human Behavior*, 51:504–519, 2015.
10. Michael Fagan, Katerina Megas, Paul Watrobski, Jeffrey Marron, and Barbara Cuthill. NISTIR 8425 profile of the IoT core baseline for consumer IoT products. Technical report, National Institute of Standards and Technology, September 2022.

11. Michael Fagan, Katerina N. Megas, Karen Scarfone, and Matthew Smith. NISTIR 8259 Foundational cybersecurity activities for IoT device manufacturers. https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf, 2020.
12. 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.
13. Federal Trade Commission. Careful connections: Keeping the internet of things secure. https://www.ftc.gov/tips-advice/business-center/guidance/careful-connections-keeping-internet-things-secure, 2020.
14. Susanne Furman and Julie Haney. Human factors in smart homes technologies workshop. https://csrc.nist.gov/CSRC/media/Projects/usable-cybersecurity/images-media/Human%20Factors%20Smart%20Home%20Workshop%20Summary%20Report.pdf, 2019.
15. Jack M. Germain. Unsupported IoT devices are cyber-trouble waiting to happen. *Ecommerce Times*, August 2021.
16. Joseph Guiltinan. Creative destruction and destructive creations: Environmental ethics and planned obsolescence. *Journal of Business Ethics*, 89(1):19—28, 2009.
17. Julie M. Haney and Susanne M. Furman. Work in progress: Towards usable updates for smart home devices. In *Proceedings of the 10th International Workshop on Socio-Technical Aspects in Security*, pages 107–117, 2020.
18. Harris Interactive. Consumer internet of things security labelling survey research findings. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/798543/Harris_Interactive_Consumer_IoT_Security_-Labelling_Survey_Report.pdf, 2019.
19. Iulia Ion, Rob Reeder, and Sunny Consolvo. "... no one can hack my mind": Comparing expert and non-expert security practices. In *Proceedings of the 11th Symposium on Usable Privacy and Security*, pages 327–346, 2015.
20. Volker G. Kuppelwieser, Phil Klaus, Aikaterini Manthiou, and Othman Boujena. Consumer responses to planned obsolescence. *Journal of Retailing and Consumer Services*, 47:157–165, 2019.
21. Phillip Morgner, Christoph Mai, Nicole Koschate-Fischer, Felix Freiling, and Zinaida Benenson. Security update labels: establishing economic incentives for security patching of IoT consumer products. In *Proceedings of the 2020 IEEE Symposium on Security and Privacy (SP)*, pages 29–446. IEEE, 2020.
22. National Institute of Standards and Technology. Recommended criteria for cybersecurity labeling for consumer internet of things (iot) products. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042022-2.pdf, 2022.
23. NPD Group. Half of U.S. consumers own at least one smart home device. https://www.npd.com/news/press-releases/2021/half-of-u-s-consumers-own-at-least-one-smart-home-device-reports-npd/, 2021.
24. Jason R. Nurse, Sadie Creese, Michael Goldsmith, and Koen Lamberts. Trustworthy and effective communication of cybersecurity risks: A review. In *Workshop on Socio-Technical Aspects in Security and Trust (STAST)*, pages 60–68, 2011.
25. Postscape. Closed IoT companies and devices: A directory of failed IoT startups. https://www.postscapes.com/closed-iot-companies/, 2019.
26. William T. Powers. *Behavior: The control of perception*. Benchmark Publications, Inc., 2nd edition, 2005.

27. Research on Investment. The IoT revolution: 5 industries that will change forever. https://researchoninvestment.com/iot-revolution-5-industries-that-will-change-forever/, March 2021.
28. Bruce Schneier. The internet of things is wildly insecure – and often unpatchable. *Wired Magazine*, January 2014.
29. Statista. Smart home device household penetration in the United States in 2019 and 2021. https://www.statista.com/statistics/1247351/smart-home-device-us-household-penetration/, 2021.
30. Madiha Tabassum, Tomasz Kosinski, and Heather Richter Lipford. "I don't own the data": End user perceptions of smart home device data practices and risks. In *Proceedings of the 15th Symposium on Usable Privacy and Security*, 2019.
31. Kami Vaniea, Emilee Rader, and Rick Wash. Betrayed by updates: How negative experiences affect future security. In *Proceedings of the 2014 SIGCHI Conference on Human Factors in Computing Systems (CHI 14)*, pages 2671–2674, Toronto, Canada, April 2014. ACM.
32. Tilo Westermann, Sebastian Moller, and Ina Wechsung. Assessing the relationship between technical affinity, stress and notifications on smartphones. In *Proceedings of the 17th International Conference on Human-computer Interaction with Mobile Devices and Services*, pages 652–659, 2015.
33. World Economic Forum. IoT for sustainable development project. https://widgets.weforum.org/iot4d/index.html, 2021.
34. Eric Zeng, Shrirang Mare, and Franziska Roesner. End user security and privacy concerns with smart homes. In *Proceedings of the 13th Symposium on Usable Privacy and Security*, 2017.
35. Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. User perceptions of smart home IoT privacy. *ACM on Human-Computer Interaction*, 2(CSCW), 2018.
36. Yixin Zou, Shawn Danino, Kaiwen Sun, and Florian Schaub. You might be affected: An empirical analysis of readability and usability issues in data breach notifications. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–14, 2019.

Appendix A: Survey Questions

The following are the survey questions related to the contents of this paper. These are a subset of a broader survey addressing smart home updates.

Throughout the survey, the following terms are used:

- **Smart home device** is a network-connected device (connected via Wi-Fi, Bluetooth, or similar protocols) that is used to remotely and/or more effectively and efficiently control functions or physical aspects of the home.
- **Smart home device app** is an application on your smartphone, computer, laptop, or tablet that is used to remotely control or access your smart home device.
- **Smart home update**s are incremental changes or improvements that manufacturers make to the software or firmware of smart home devices and device apps. Updates may be automatic in which updates are installed without you having to take any action or manual in which you may have to click a button or take some other action to install the update.

- The **security** of smart home devices refers to the prevention of damage to, unauthorized use of, and exploitation of smart home devices and the information they contain, in order to strengthen the confidentiality, integrity, and availability of these devices. In this survey, "security" is equivalent to "cybersecurity." Physical security related to the home or its occupants is different and will be referred to as "home security."
- The **privacy** of smart home devices refers to the right of a party to maintain control over and be assured confidentiality of personal information that is collected, transmitted, used, and stored during the use of smart home devices.

SMART HOME DEVICES

1) Which of the following smart home devices do you own? (Select all that apply.)

- ☐ Virtual voice assistants and smart speakers (e.g., Amazon Echo/Alexa, Google Nest Home Hub, Apple HomePod)
- ☐ Thermostats (e.g., Nest, Ecobee)
- ☐ Home security devices (e.g., video doorbells, cameras, door locks, garage door openers)
- ☐ Home environment sensors (e.g., smoke and leak detectors)
- ☐ Lighting (e.g., lightbulbs, lighting systems)
- ☐ Appliances (e.g., refrigerators, washing machines/dryers, ovens, coffee makers/espresso machines)
- ☐ Entertainment (e.g., TVs, streaming devices such as AppleTV or Roku)
- ☐ Plugs or outlets (e.g., Wemo Mini, Wyze Plug)
- ☐ Domestic robots that do household chores (e.g., robot vacuums such as iRobot Roomba, smart lawn mowers)
- ☐ Smart home hubs (e.g., Samsung SmartThings, Hubitat Elevation)*
- ☐ Other (e.g., smart windows solutions, smart watering system, smart pet feeder) (please specify):

2) Please indicate the number and types (including the brand) of smart home devices you own in each of the following categories.

[answer for each device category owned]

UPDATES

3) Rate your agreement with the following statement for each category of smart home device: It is important for smart home devices to be updated.

Strongly Disagree - Disagree - Neither Agree nor Disagree - Agree - Strongly Agree

[answer for each device category owned]

MANUFACTURER SUPPORT

4) Please rate your agreement with the following statement: I am concerned that the manufacturer will eventually stop supporting my smart home devices.

Strongly Disagree - Disagree - Neither Agree nor Disagree - Agree - Strongly Agree

[answer for each device category owned]

5) Which of the following would concern you if the manufacturer stopped supporting your smart home devices? (Select all that apply.)

- ☐ My devices eventually stop working
- ☐ Updates containing security bug fixes no longer being released
- ☐ Updates containing non-security bug fixes no longer being released
- ☐ New features no longer being added
- ☐ Parts or accessories no longer being available
- ☐ Losing online/call-in customer support from the manufacturer
- ☐ I would not be concerned

[answer for each device category owned]

6) What would you do if your smart home devices were no longer supported by the manufacturer?

- ◦ Nothing - leave it as is
- ◦ Replace it with a new or different device as soon as possible
- ◦ Replace it with a new or different device eventually but not necessarily right away
- ◦ Throw the device out without replacing it

[answer for each device category owned]

7) What would be your *preferred* method of notification from the manufacturer to inform you they were no longer supporting your smart home devices?

- ◦ Email
- ◦ Message/notification sent to the device app
- ◦ Text message on my phone
- ◦ Letter/postcard in the mail
- ◦ I prefer not to be notified
- ◦ Other (please specify):

SECURITY AND PRIVACY

8) Please rate your level of concern with the security of your smart home devices for each category:

Not at all concerned - Slightly concerned - Somewhat concerned - Moderately concerned - Extremely concerned

[answer for each device category owned]

9) Please rate your level of concern with the privacy of your smart home devices for each category:

Not at all concerned - Slightly concerned - Somewhat concerned - Moderately concerned - Extremely concerned

[answer for each device category owned]

DEMOGRAPHICS

10) In which state or US territory do you live?

11) In which type of area is your home?

- Rural
- Suburban
- Urban

12) How long have you been using smart home devices?

- Less than 1 year
- 3 - 5 years
- 6 or more years

13) What is your age range?

- 18 - 24
- 25 - 34
- 35 - 44
- 45 - 54
- 55 - 64
- 65+

14) What is your gender?

- Male
- Female
- Prefer to self-describe
- Prefer not to answer

15) What is your race?

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Native Hawaiian or Other Pacific Islander
- ☐ White
- ☐ Other
- ☐ Prefer not to answer

16) What is your ethnicity?

- Hispanic, Latino/a, or Spanish Origin
- Not Hispanic, Latino/a, or Spanish Origin
- Prefer not to answer

17) What is your highest level of education?

- Less than high school degree
- High school degree or equivalent
- Some college
- Associate degree
- Bachelor's degree
- Master's degree
- Doctoral or Juris Doctoral degree
- Other:
- Prefer not to answer

18) Have you ever worked in a field/job related to information technology (IT) (for example, a system or network administrator, IT help desk, cybersecurity professional)?

- Yes
- No