Understanding People's Attitude and Concerns towards Adopting IoT Devices

Evan Lafontaine
North Carolina State University
Raleigh, North Carolina, USA

Aafaq Sabir
North Carolina State University
Raleigh, North Carolina, USA

Anupam Das
North Carolina State University
Raleigh, North Carolina, USA

ABSTRACT

The proliferation of the Internet of Things (IoT) has started transforming our lifestyle through automation of home appliances. However, there are users who are hesitant to adopt IoT devices due to various privacy and security concerns. In this paper, we elicit peoples' attitude and concerns towards adopting IoT devices. We conduct an online survey and collect responses from 232 participants from three different geographic regions (United States, Europe, and India); the participants consist of both adopters and non-adopters of IoT devices. Through data analysis, we determine that there are both similarities and differences in perceptions and concerns between adopters and non-adopters. For example, even though IoT and non-IoT users share similar security and privacy concerns, IoT users are more comfortable using IoT devices in *private settings* compared to non-IoT users. Furthermore, when comparing users' attitude and concerns across different geographic regions, we found similarities between participants from the US and Europe, yet participants from India showcased *contrasting* behavior. For instance, we found that participants from India were more trusting in their government to properly protect consumer data and were more comfortable using IoT devices in a variety of public settings, compared to participants from the US and Europe. Based on our findings, we provide recommendations to reduce users' concerns in adopting IoT devices, and thereby enhance user trust towards adopting IoT devices.

CCS CONCEPTS

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

KEYWORDS

Internet of Things (IoT), user attitude, cross-societal concerns

ACM Reference Format:
Evan Lafontaine, Aafaq Sabir, and Anupam Das. 2021. Understanding People's Attitude and Concerns towards Adopting IoT Devices. In *CHI Conference on Human Factors in Computing Systems Extended Abstracts (CHI '21 Extended Abstracts), May 8–13, 2021, Yokohama, Japan.* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3411763.3451633

CHI '21 Extended Abstracts, May 8–13,2021, Yokohama, Japan

ACM ISBN 978-1-4503-8095-9/21/05…$15.00
https://doi.org/10.1145/3411763.3451633

1 INTRODUCTION

In recent years, we have seen a proliferation of the Internet of Things (IoT). Most households nowadays are equipped with numerous IoT products, leading to the emergence of consumer privacy concerns. For instance, many consumers are concerned that voice assistants constantly record and sell their data to third parties, or that the device can be easily mis-triggered and cause unwanted actions [10, 14]. Many of these concerns are rarely addressed by manufacturers, except for barely acknowledging and updating their convoluted privacy policies — something which users rarely read, let alone understand [6, 17]. Many consumers also distrust their government and IoT manufacturers due to the lack of control and transparency over their personal data [31].

The focus of this paper is to understand how users' perceptions and concerns vary across different geographic regions among IoT and non-IoT users, and to determine what steps can be taken to address these concerns. We, therefore, conducted a user study to answer the following research questions: **RQ1:** ***What perceptions and concerns do IoT and non-IoT users have? To what extent do such perceptions and concerns differ between IoT and non-IoT users?*** This research question delves into comparing IoT and non-IoT users in order to determine barriers to IoT adoption. We analyze factors, such as concerns and levels of trust in the government between IoT and non-IoT users; this helps depict the perceptions of each group and helps determine settings under which each group is comfortable in interacting with IoT devices. **RQ2:** ***Are there differences in perceptions and concerns regarding adoption of IoT products among people from different cultures and geographic regions?*** We study whether perceptions and concerns vary by region, especially since different regions have different privacy regulations. For instance, the EU established the General Data Protection Regulation (GDPR) [23], India is finalizing the Personal Data Protection Bill (PDPB) [22], and the US recently passed the California Consumer Privacy Act (CCPA) [13].

In this paper, we conduct a user survey to understand users' concerns in adopting IoT devices. We use statistical analysis techniques to contrast perceptions and concerns among IoT and non-IoT users from different regions of the world. Our analysis reveals similarities and differences between adopters and non-adopters of IoT devices; for example, both IoT and non-IoT users have similar levels of trust in their respective governments, but IoT users are more comfortable using IoT devices in private settings. We also find that participants from different regions indicate similar concerns but emphasize different factors; for instance, participants from India are more concerned about their Internet connection and network interference when it comes to adopting IoT devices.

2 RELATED WORK

Privacy Concerns in using IoT Devices. Smart home technologies are becoming increasingly prevalent due to the convenience they offer. However, they also create new security and privacy risks. Barbosa et al. [4] found that a large number of consumers are worried about privacy, and they expect privacy protections to be embedded into the devices they purchase. Many qualitative studies have found that consumers have limited perceptions of the security and privacy risks imposed by IoT devices in smart home settings, and have suggested that policy makers and manufacturers develop an additional set of best practices specifically catered for smart home users [27, 32, 34]. Researchers have also solicited privacy preferences under various hypothetical IoT settings [7, 12, 21] and found that not only do people's preferences change under different settings, but that preferences can also be predicted using machine learning models.

Others have studied the privacy perceptions of bystanders and guests in smart home settings [16, 30] and have found that the level of concern varies depending on the trust towards the device owner. A series of studies have looked at understanding the privacy concerns and attitudes of smart speaker users [1, 11, 15, 28]. All of these studies state that consumers want to see more user-friendly privacy controls for smart speakers.

Attitude towards Buying IoT Devices. Most recently, we have seen studies that try to understand whether consumers consider security and privacy prior to purchasing IoT products [9]. A recent interview study by Emami-Naeini et al. revealed that most device owners do not consider privacy or security prior to purchasing, but become concerned once the devices are installed in their homes [9]. Reasons for such concerns surface due to the lack of access to, or information about, privacy and security of the devices. Interestingly, the study also finds 'privacy' as the third-most influencing factor on participants' decisions to buy an IoT product, appearing only after 'features' and 'price'. This line of research motivated a series of work that has examined the use of security and privacy labels to help consumers make better decisions [8, 20]. Barbosa et al. draw similar conclusions, where they found 'convenience,' 'ease of use,' 'price,' 'cost-saving,' and 'need' as the top motivators for buying IoT devices [5]. They also state that concerns arise after consumers try and test the device, while considering their experience with the device and their satisfaction with the manufacturer. Zheng et al. interviewed consumers to determine whether certain data practices, such as "who owns the data," "what data is transmitted," and "is the data encrypted," are considered prior to purchasing the device [33]. They found convenience and usability as the main reasons behind buying IoT devices and that many consumers assume that big manufacturers (i.e., well-known brands) adopt good data practices.

Distinctions from Prior Work. Most studies either focus solely on IoT users or analyze concerns from a specific geographic region. Our study contrasts concerns and potential mediation for both IoT and non-IoT users by capturing responses from different geographic locations through a user survey. To the best of our knowledge, this paper is the first to attempt to understand user concerns across different geographical regions, providing a comprehensive analysis of reservations that consumers have regarding IoT adoption. Concerns about IoT devices vary across parts of the world, as differences in markets, usage, and laws affect buying and usage patterns. All of these factors have helped shape this user study.

3 METHODOLOGY

Data Source. The goal of this paper is to elicit user concerns in adopting IoT devices and to showcase how such concerns vary across geographic regions. Given that past research has shown that privacy expectations and requirements vary between different countries [18, 19, 29], we wanted to analyze if such differences are easily discernible when it comes to adopting IoT devices. Such analysis can help understand to what extent expectations are being fulfilled and what needs to be addressed to ease user concerns. To elicit cross-societal concerns in adopting IoT devices, we resorted to a survey based study (IRB approved) where participants from different parts of the world engaged in our survey. The survey was hosted on Qualtrics [24] and posted on Amazon Mechanical Turk (MTurk) [2], a well-known crowd-sourcing platform often used by the academic community. We also selected MTurk because recent research has shown that MTurk responses are representative of the general population [25]. Through MTurk, we paid the participant $2.50 in compensation (the survey took around 10 minutes to complete), and added the following requirements to ensure quality responses: the participant must be a *Master* worker, have a 95% approval rate (HIT approval rate), and must have completed more than 100 tasks (HITs). We launched our survey in April 2020.

The survey was composed of three main sections: demographic information, questions tailored to either IoT or non-IoT users, and questions asked to both IoT and non-IoT users. We first collected demographic information to obtain background information on the participants. After asking whether participants had experience with IoT devices, specific questions were geared to each group. For instance, we asked non-IoT users why they did not use IoT devices while we asked IoT users why they used IoT devices. These tailored questions also discussed concerns surrounding IoT device use and whether actions could be taken to reduce these concerns. The third section contained questions asked to both IoT and non-IoT users. For instance, we asked about participants' levels of trust in their government as well as their comfort levels using IoT devices under different settings. Some of these survey questions were inspired by related work [21], which has analyzed people's privacy preferences in different hypothetical scenarios. Many of these questions provided a direct contrast in perceptions between IoT and non-IoT users. Furthermore, many survey questions also contained a text field to allow for additional responses. This option encouraged participants to discuss concerns that were not covered by the pre-populated answers. Some users chose to utilize this feature and provided their personal thoughts and concerns. A copy of the survey is provided in Appendix A.

Data Analysis Methods. We resorted to various statistical analysis techniques to perform a quantitative analysis of the survey data. We used Pearson's Chi-Square test to analyze relationships between ordinal and qualitative variables. Fisher's exact test was used when conditions for minimum expectancy counts were not met to compute the statistical difference [26]. Furthermore, the null hypothesis H_0 represents that there is no statistical relationship between the tested factors. The alternate hypothesis H_a indicates that there is a statistical relationship between the factors. We use $\alpha = 0.05$ for all Chi-Square tests and provide the χ^2 value, df, and $p - value$. We also use $\alpha = 0.05$ for Fisher's exact test and report the $p - value$. Additionally, we used multiple comparison tests to determine which pairs of factors are significantly different. Bonferroni's correction was used for all post-hoc analysis to adjust for the risk of a Type I error. Lastly, Theil's U (the "Uncertainty Coefficient") was also utilized to provide a measure of nominal association; this is provided instead of Cramer's V due to the asymmetrical shape of the data [3].

Data Collection Setup. We iteratively collected data from participants. We originally received 154 responses, composed of 132 IoT users and 22 non-IoT users. In order to perform comparative analysis between IoT and non-IoT users, we performed a second round of data collection. Only non-IoT users were allowed to proceed in the second round of the survey. MTurk user IDs were tracked to restrict participants from reattempting the survey (e.g., participants could not exit the survey and switch their responses to proceed with the survey). After the second iteration, we received a total of 255 responses. However, 23 responses were filtered out, as participants either completed the survey too quickly, in less than 2 minutes where the average survey duration was approximately 7 minutes, or failed to correctly answer the *attention check* question (an image of 'Google Home Mini' was shown and respondents were asked to recognize the device). After removing these responses, we had 232 total responses consisting of 120 IoT users and 112 non-IoT users. Furthermore, our survey covered three different geographic regions: US (89), EU (84) and India (54). Table 1 summarizes the demographics of our participants.

Table 1: Demographics of participants.

Attribute	Values	IoT users	Non-IoT users
Age	18-24	16	12
	25-34	69	52
	35-44	25	29
	45-54	7	12
	55-64	3	4
	65 or older	0	3
Gender	Male	86	78
	Female	33	33
	Other	1	1
Country	US	45	44
	EU *	45	39
	India	30	29

* United Kingdom (24), Italy (19), Germany (16), Spain (14), France (6), Ireland (2), Netherlands (2), Finland (1)

4 DATA ANALYSIS

We performed data analysis along three main directions. We contrasted perceptions and concerns in adopting IoT products of IoT users against non-IoT users. IoT users and non-IoT users represent the group of participants who claim to use IoT devices and those who do not, respectively. We chose this distinction to determine the potential barriers in mass adoption of IoT devices. Furthermore, analyzing IoT users against non-IoT users highlights significant concerns held by both groups and enables us to identify similar and different comfort levels, indicating where IoT devices may be commonly integrated in the future. Next, we test the impact of the participant's geographic location (i.e., cultural background) on their attitudes towards adopting IoT devices. We collected data from three main regions (the United States, Europe, and India), and each region contains statistically sufficient samples to extract distinct perceptions. We chose to analyze user concerns by geographic location due to the varying privacy regulations implemented by different governments. For instance, the European Union enforces the General Data Protection Regulation (GDPR) [23], the United States enforces the California Consumer Privacy Act (CCPA) [13], and India is finalizing the Personal Data Protection Bill (PDPB) [22]. While these regulations may have similarities, certain differences exist which allow for varying privacy sentiments; we strive to portray these differences.

Lastly, we elicit necessary actions that may reduce user concerns. By analyzing the types of actions that users would like to see be taken, we determine whether the issue stems from government regulations (or lack thereof), the manufacturer, or the product itself. This form of analysis can potentially help policymakers enforce standards to better promote transparency and control for consumers.

4.1 Difference in Perception among IoT and Non-IoT Users

It is important to differentiate between concerns of IoT and non-IoT users. Both viewpoints provide valuable information to manufacturers and governments, as they contribute insights on perceptions about device safety and whether certain actions can be taken to improve adoption. Our participants discussed numerous privacy and security concerns as well as a lack of trust for governments/manufacturers. Participants also inform us of their comfort levels in using IoT devices under specific settings. We collected a total of 232 MTurk responses, composed of approximately 52% (120/232) IoT users and 48% (112/232) non-IoT users.

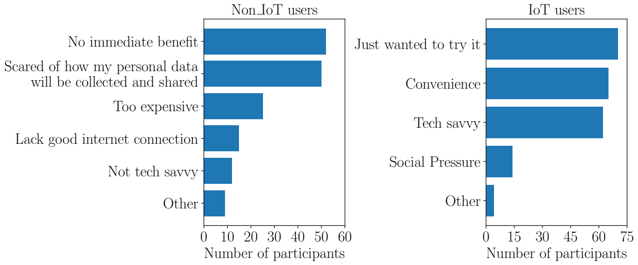

Figure 1: Reasons for not using and using IoT devices by non-adopters and adopters, respectively.

Table 1 displays the demographic information for IoT and non-IoT users. We first sought to determine perceptions that may limit the adoption of IoT products. Figure 1 explains why non-IoT users are reluctant to use IoT devices and why IoT users chose to use such devices. The majority of non-IoT users described how they saw

Table 2: Percentage of participants selecting various concerns (this was a multi-choice question).

Concerns	Non-IoT users	IoT users
Security loopholes	53.6%	63.3%
Transmit data w/o consent	54.5%	55%
Data interception	37.5%	44.2%
Network interference	25.9%	28.3%
IoT deemed not useful	25.9%	12.5%
Others	5.4%	0.8%

"no immediate benefit" from using IoT devices while being "scared about how [their] personal data will be collected and shared." On the other hand, the majority of IoT users "just wanted to try it" because they were "tech savvy," or due to the "convenience" perceived from the devices. Most IoT users who mentioned 'other' reasons specified that the device was obtained through a gift, bundle, or rental.

Finding 1: *IoT users are tech savvy and use IoT devices out of curiosity or for convenience. Non-IoT users are scared of personal data collection and see no benefit in using the device.*

Participants were also asked to discuss *concerns* surrounding either their use of IoT devices or *concerns* behind not using IoT devices. Table 2 contrasts the concerns across both groups. Many IoT and non-IoT users shared the same concerns, such as how the device may transmit additional data without user consent. However, other concerns, such as devices' perceived usefulness, was prevalent for non-IoT users but insignificant for IoT users. Non-IoT users also listed additional concerns; for instance, a non-IoT user blatantly described that they "*don't trust the companies.*" We found marginal statistical significance for the distribution of concerns across the IoT and non-IoT user groups ($\chi^2(5) = 11.105$ and $p = 0.049$). However, post-hoc testing (with Bonferroni correction) revealed that no concern was more prevalent than another, which was further confirmed through a low Uncertainty Coefficient, $U_{(IoT\_Use\,|\,Concerns)} = 0.018$. Nonetheless, Table 2 demonstrates that IoT and non-IoT users share common concerns surrounding IoT device use, and these concerns need to be addressed to promote higher device adoption.

Finding 2: *While both IoT and non-IoT users share similar concerns, no specific concern is predominant.*

Furthermore, we analyzed whether trust in government or regulations impacts adoption of IoT devices. As depicted in Table 3, IoT and non-IoT users have similar distribution of levels of trust in government. The majority of non-IoT users have some trust in their government, while the remainder of the non-IoT users varied between no trust and complete trust. This trend was similar for IoT users; thus we conclude that IoT usage/adoption does not relate to different levels of government trust ($\chi^2(3) = 1.938$ and $p = 0.585$). The independence between IoT use and government trust is further confirmed through a low Uncertainty Coefficient, $U_{(IoT\_Use\,|\,Level\_of\_Trust)} = 0.006$. Table 3 also demonstrates that only 10% of participants believe that sufficient laws are in place, which highlights the necessity of new and improved privacy and security regulations.

Finding 3: *IoT and non-IoT users have similar levels of trust in their government. The majority of participants only somewhat trust their government.*

Table 3: Percentage of participants who trust their government to properly enforce consumer-friendly data practices.

Trust in govt. to enforce policies	Non-IoT users	IoT users
Do not trust government	24.1%	26.7%
Somewhat trust government	50%	45.8%
Fully trust government	19.6%	24.2%
Sufficient laws in place	6.3%	3.3%

Lastly, we asked participants of their comfort levels in interacting with IoT devices under different settings. Participants could rate their comfort levels from "very uncomfortable" to "very comfortable." Figure 2 highlights the distribution of comfort levels across various settings. We found statistically significant differences in comfort levels among IoT and non-IoT users for the following settings: at home ($\chi^2(4) = 59.538$, $p < 0.001$, and $U_{(IoT\_Use\,|\,Home)} = 0.066$), with family or friends ($\chi^2(4) = 39.525$, $p < 0.001$, and $U_{(IoT\_Use\,|\,Family/Friends)} = 0.054$), with a colleague ($\chi^2(4) = 18.618$, $p < 0.001$, and $U_{(IoT\_Use\,|\,Colleague)} = 0.048$), and after work ($\chi^2(4) = 33.797$, $p < 0.001$, and $U_{(IoT\_Use\,|\,After\_Work)} = 0.052$). Post-hoc analysis (with Bonferroni correction) depicts that the most prominent locations with differences are 'at home' ($p < 0.001$ in all cases) and 'with family or friends' ($p < 0.001$ in all cases). These differences are also visible in Figure 2, where it can be seen that IoT users are much more comfortable using their devices at home and with friends compared to non-IoT users. Additionally, Figure 2 demonstrates that both IoT and non-IoT users are less comfortable in interacting with IoT devices in more public locations.

Finding 4: *IoT users are more comfortable using their devices in a variety of locations/settings, especially in private settings. However, both non-IoT and IoT users hesitate in interacting with IoT device in public areas.*

4.2 Difference in Perception across People from Different Cultures

In recent years, many data privacy regulations (such as GDPR, CCPA, or PDPB) have become increasingly prevalent throughout the world. There are differences in the proposed regulations due to the cultural differences that exist between many regions. We collected data from 232 participants throughout three main regions — 89 participants from the United States, 84 participants from Europe, and 59 participants from India. In this section we aim to understand how perceptions in adopting IoT devices vary across different geographic regions.

We found that non-IoT users' reasons for not using IoT devices differed by region ($p < 0.001$ and $U_{(Region\,|\,Reasons)} = 0.144$). The distribution of reasons varied significantly for Indian participants when compared to participants from the US ($p < 0.001$) and Europe ($p < 0.001$). Figure 3 demonstrates that the vast majority of Indian non-IoT users did not buy IoT devices due to a poor internet connection or because the devices are too expensive. Compared to American and European participants, Indian non-IoT users were

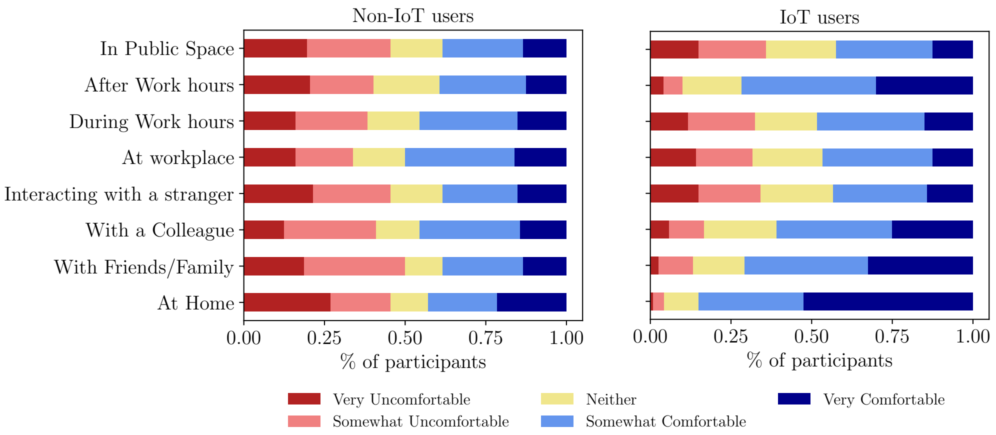

Figure 2: Level of comfort in interacting with IoT devices under different contexts.

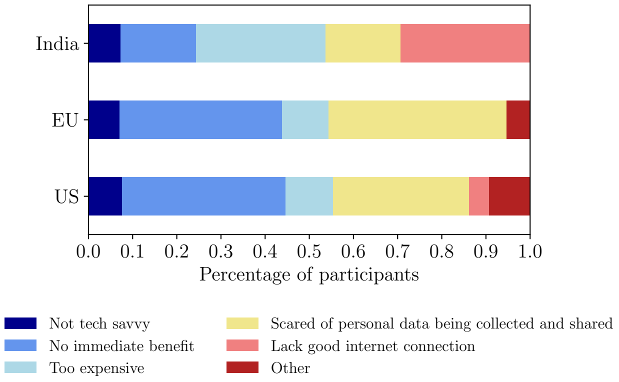

Figure 3: Distribution of reasons for *not* adopting IoT devices across participants from different regions.

not very concerned about the collection of personal data and viewed IoT devices as beneficial.

Finding 5: *Many Indian participants do not use IoT devices because they lack a fast Internet connection or simply cannot afford the devices, whereas many American and European participants are more worried about personal data being collected or simply fail to see any immediate benefits from IoT devices.*

Similarly, we found that reasons for adopting IoT devices also greatly differed by region ($p = 0.002$ and $U_{(Region\,|\,Reasons)} = 0.067$). The distribution of reasons for adopting IoT devices among Indian participants differed significantly when compared to American ($p < 0.001$) and European ($p = 0.025$) participants. Figure 4 displays that Indian IoT users faced more social pressure in buying IoT devices, while many of the participants from the US and Europe just wanted to try different devices.

Finding 6: *Many Indian participants bought IoT devices due to social pressure, whereas many American and European participants bought devices out of curiosity.*

We also analyzed whether participants' concerns in using or not using IoT devices varied across different geographic regions. Figure 5 displays the types of concerns across different regions;

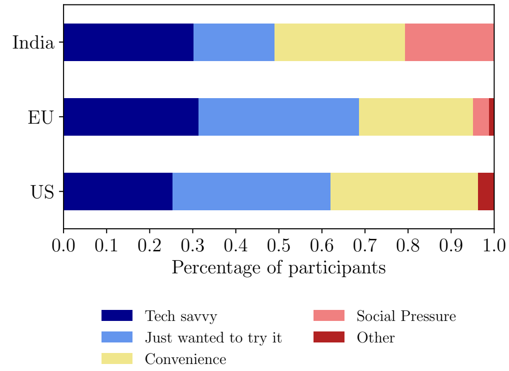

Figure 4: Distribution of reasons for using IoT devices across participants from different regions.

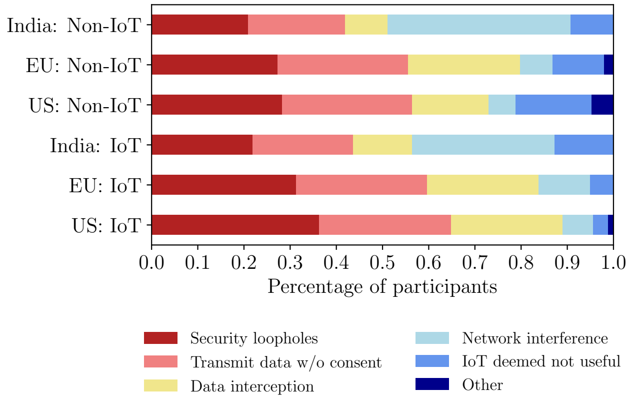

Figure 5: Distribution of concerns in using or not using IoT devices across participants from different regions.

it is evident that Indian participants were much more concerned about network interference than American or European participants. Pairwise statistical testing confirmed that Indian participants discussed significantly different concerns compared to American

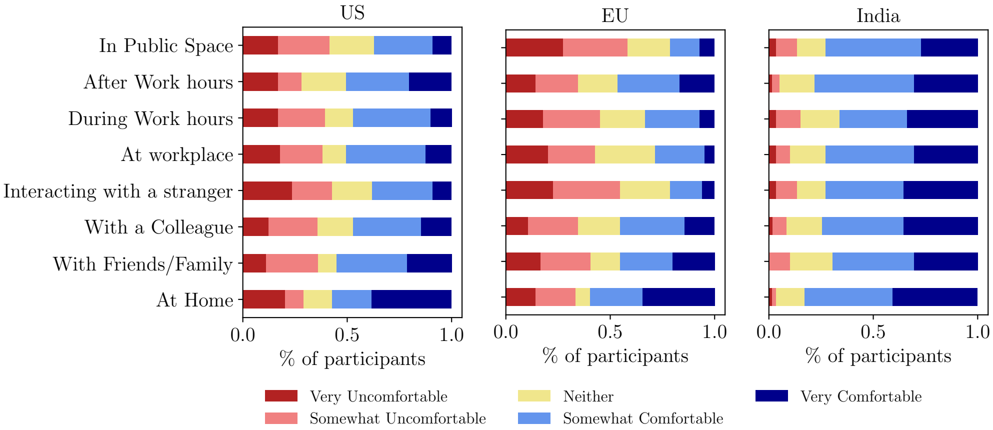

Figure 6: Levels of comfort in interacting with IoT devices under different context for people from different parts of the world. This plot combines IoT and non-IoT users per region.

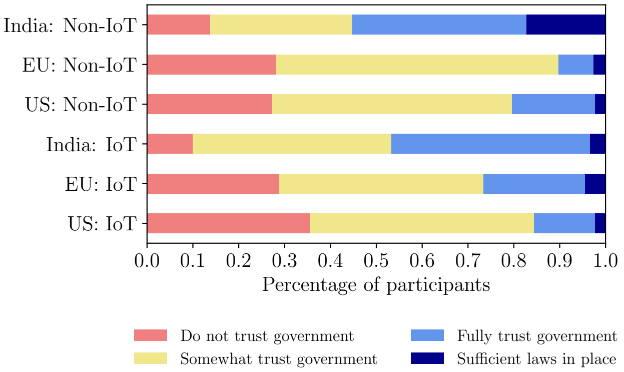

Figure 7: Distribution of levels of trust on government across participants from different regions.

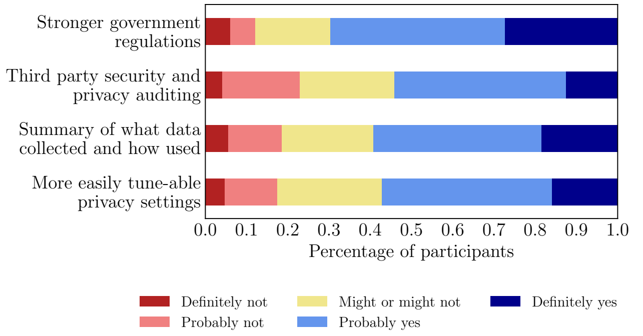

Figure 8: Likelihood of using an IoT device in the future based on different transparency-inducing actions (for non-iot users).

($p < 0.001$) or European ($p < 0.001$) participants. Figure 5 depicts that the majority of participants agreed on certain concerns, such as security loopholes or transmitting data without consent. These concerns were also reflected in both IoT and non-IoT participants.
Finding 7: *Indian participants were very concerned with interference on their network compared to American or European participants. Nonetheless, most participants were greatly concerned with security loopholes and transmission of personal data without consent.*

Furthermore, we sought to determine whether specific regions have different perceptions towards their respective governments in terms of properly regulating how consumer data is collected and shared. We found that participants' trust also varied across regions ($p = 0.001$ and $U_{(Region\,|\,Government\_Trust)} = 0.048$). We determined that Indian participants trusted their government more than American ($p < 0.001$) and European ($p = 0.002$) participants. Figure 7 demonstrates how American and European participants both had little-to-no trust in their government.
Finding 8: *Indian participants were more likely to trust their government and regulations, while American and European participants were more hesitant in trusting their respective governments.*

Lastly, we revisit the comfort level of interacting with IoT devices under various settings among participants across different regions. We found statistically significant differences across different regions for all settings ($p < 0.01$ in all cases). Indian participants were significantly more comfortable interacting with IoT devices than American and European participants ($p < 0.01$ in both cases). Furthermore, American and European participants displayed a similar trend in comfort levels across the different settings, as evident in Figure 6.
Finding 9: *Indian participants were more comfortable using IoT devices in any setting, while American and European participants were more hesitant (especially in public spaces and during work hours).*

5 DISCUSSION

Our analysis thus far has shown that both IoT and non-IoT users have certain concerns in interacting with IoT devices. We, therefore, asked non-IoT users whether certain actions would convince them to use IoT devices in the future. Figure 8 depicts that the majority of non-IoT users agree on various actions. Stronger government regulations proved to be the most effective action, as over 80% of users agreed that this action may convince them to buy an IoT device (i.e., "might or might not" to "definitely yes" to buying an IoT device). Similarly, providing a summary of collected data influenced the majority of non-IoT users to reconsider using IoT devices. However, no specific action was found to be statistically more significant than another ($\chi^2(8) = 17.338$ and $p = 0.364$). In other words, different users may prefer different actions. For instance, one participant may prefer a summary of data collection while another may prefer stricter government regulations. Furthermore, some participants mentioned that they would prefer to see limited functionality; for instance, a participant described how "*IoT reaching cars ... is a really worrying idea.*" Another participant mentioned a requirement of transparency surrounding IoT devices, such as open-source systems.

Through our user study, we propose the following measures and actions for IoT manufacturers and policy-makers in order to reduce consumer concerns, and thereby enhance transparency. This will also help them better gain consumer trust.

- Policy-makers can hire third-party auditors or implement government auditors to analyze a manufacturer's data practices and ensure that no privacy violations are occurring. This would increase consumer trust, since users would know that their data is protected as the manufacturer's data practices have been verified by an auditor. At the same time, manufacturers should vet their products internally by hiring a third-party auditor before they release their product to market.
- To increase consumer trust, manufacturers should provide periodic or real-time summaries of all actions taken on a user's personal data, including collection, storage, and share of data.
- Consumers also want to gain more control over their data and want to be able to act on such controls through easily tune-able privacy settings. Thus, more research is required to develop usable privacy settings.
- Stronger government regulations need to be implemented in order to increase consumer trust. While we are seeing new regulations, such as GDPR, CCPA and PDPB come to light, more effort is required in actually enforcing such regulations. Such efforts will further improve IoT adoption.
- Consumers in certain countries, such as India, hesitate to purchase and use IoT devices due to poor/unstable network conditions. Internet service providers and governments in these countries need to improve wireless networks in order to improve IoT device adoption rates.

Limitations. There are a few limitations to our study. Firstly, we had a limited number of participants from different countries. Our participants' demographics were also more skewed towards males than females. While we still found statistically significant differences, more diverse data collection could reveal new findings. Secondly, we did not provide an explicit definition of IoT devices to the participants. Therefore, it is possible that certain users had different perceptions of IoT devices while taking the survey. However, our survey included a list of example IoT devices to provide a better context to the participants.

6 CONCLUSION

This paper reports consumer privacy and security concerns based on the rapidly expanding field of IoT. We sought to answer the research questions — (1) what perceptions and concerns do IoT and non-IoT users have, and do these differ between IoT and non-IoT users, and (2) are there any differences in perceptions and concerns for IoT adoption across different geographic regions? Through these questions, we seek to understand the factors differentiating IoT and non-IoT users as well as participants in different regions; which in turn allow us to provide recommendations to policy-makers and manufacturers. We answer these questions by eliciting user concerns through a survey from 232 participants located in different geographic regions.

Our analyses demonstrate that consumers discuss specific privacy and security concerns that need to be addressed to improve IoT device adoption. Consumers worldwide are concerned about the lack of transparency (i.e., data collection without consent), and security loopholes, each of which may lead to data privacy violations. Also, the default privacy settings need to be revisited as consumers from different parts of the world have different comfort levels in interacting IoT devices.

Future work is required in this field to determine on a larger scale the difference in perceptions and concerns between different geographic regions. Furthermore, with the development of new privacy regulations and increased enforcement of current regulations in separate countries, privacy sentiments may change over time. These new sentiments will need to be analyzed to determine whether manufacturers and policy-makers have successfully improved consumer trust and enhanced IoT device adoption.

ACKNOWLEDGEMENTS

We thank our anonymous reviewers for their feedback. This material is based upon work supported in parts by the National Science Foundation under grant number CNS-1849997 and NCSU FRPD grant. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

REFERENCES

[1] Noura Abdi, Kopo M. Ramokapane, and Jose M. Such. 2019. More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants. In *Proceedings of the 15th Symposium on Usable Privacy and Security (SOUPS)*. USENIX Association, Santa Clara, CA, 451–466.

[2] Amazon. 2020. Amazon Mechanical Turk. https://www.mturk.com/

[3] Hoang Anh. 2019. Correlation between discrete (categorical) variables. https://rstudio-pubs-static.s3.amazonaws.com/558925_38b86f0530c9480fad4d029a4e4aea68.html

[4] Natã M. Barbosa, Joon S. Park, Yaxing Yao, and Yang Wang. 2019. "What if?" Predicting Individual Users' Smart Home Privacy Preferences and Their Changes. *Proceedings on Privacy Enhancing Technologies* 2019, 4 (2019), 211 – 231.

[5] Natã M. Barbosa, Zhuohao Zhang, and Yang Wang. 2020. Do Privacy and Security Matter to Everyone? Quantifying and Clustering User-Centric Considerations About Smart Home Device Adoption. In *Proceedings of the 16th Symposium on Usable Privacy and Security (SOUPS)*. USENIX Association, Virtual, 417–435.

[6] F. H. Cate. 2010. The Limits of Notice and Choice. *IEEE Security & Privacy* 8, 02 (2010), 59–62.

[7] A. Das, M. Degeling, D. Smullen, and N. Sadeh. 2018. Personalized Privacy Assistants for the Internet of Things: Providing Users with Notice and Choice. *IEEE Pervasive Computing* 17, 3 (Jul 2018), 35–46.

[8] Pardis Emami-Naeini, Yuvraj Agarwal, Lorrie Faith Cranor, and Hanan Hibshi. 2020. Ask the Experts: What Should Be on an IoT Privacy and Security Label?. In *Proceedings of the 41st IEEE Symposium on Security and Privacy (S&P)*. IEEE,

Virtual, 447–464.

[9] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. 2019. Exploring How Privacy and Security Factor into IoT Device Purchase Behavior. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI)*. ACM, Glasgow, Scotland UK, 1–12.

[10] Geoffrey A. Fowler. 2018. *Hey Alexa, come clean about how much you're really recording us.* The Washington Post. https://www.washingtonpost.com/news/the-switch/wp/2018/05/24/hey-alexa-come-clean-about-how-much-youre-really-recording-us

[11] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. 2018. Alexa, Are You Listening? Privacy Perceptions, Concerns and Privacy-Seeking Behaviors with Smart Speakers. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW, Article 102 (2018), 31 pages.

[12] H. Lee and A. Kobsa. 2017. Privacy preference modeling and prediction in a simulated campuswide IoT environment. In *Proceeding of the 15th IEEE International Conference on Pervasive Computing and Communications (PerCom)*. IEEE, Hawaii, USA, 276–285.

[13] California State Legislature. 2020. California Consumer Privacy Act (CCPA). https://oag.ca.gov/privacy/ccpa

[14] Sapna Maheshwari. 2018. *Hey, Alexa, What Can You Hear? And What Will You Do With It?* The New York Times. https://www.nytimes.com/2018/03/31/business/media/amazon-google-privacy-digital-assistants.html

[15] Nathan Malkin, Joe Deatrick, Allen Tong, Primal Wijesekera, Serge Egelman, and David Wagner. 2019. Privacy attitudes of smart speaker users. *Proceedings on Privacy Enhancing Technologies* 2019, 4 (2019), 250–271.

[16] Shrirang Mare, Franziska Roesner, and Tadayoshi Kohno. 2020. Smart Devices in Airbnbs: Considering Privacy and Security for both Guests and Hosts. *Proceedings on Privacy Enhancing Technologies* 2020, 2 (2020), 436–458.

[17] Aleecia M McDonald and Lorrie Faith Cranor. 2008. The Cost of Reading Privacy Policies. *I/S: A Journal of Law and Policy for the Information Society (ISJLP)* 4 (2008), 543.

[18] Sandra J Milberg, Sandra J Burke, H Jeff Smith, and Ernest A Kallman. 1995. Values, personal information privacy, and regulatory approaches. *Commun. ACM* 38, 12 (1995), 65–74.

[19] Sandra J Milberg, H Jeff Smith, and Sandra J Burke. 2000. Information privacy: Corporate management and national regulation. *Organization science* 11, 1 (2000), 35–57.

[20] Philipp Morgner, Christoph Mai, Nicole Koschate-Fischer, Felix Freiling, and Zinaida Benenson. 2020. Security Update Labels: Establishing Economic Incentives for Security Patching of IoT Consumer Products. In *Proceedings of the 41st IEEE Symposium on Security and Privacy (S&P)*. IEEE, Virtual, 429–446.

[21] Pardis Emami Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. 2017. Privacy expectations and preferences in an IoT world. In *Proceedings of the 13th Symposium on Usable Privacy and Security (SOUPS)*. USENIX Association, Santa Clara, CA, 399–412.

[22] Parliament of India. 2019. The Personal Data Protection Bill (PDPB). https://www.prsindia.org/billtrack/personal-data-protection-bill-2019

[23] Council of the European Union. 2019. EU's General Data Protection Regulation (GDPR). https://gdpr.eu/

[24] Qualtrics. 2020. Qualtrics Survey. https://www.qualtrics.com/

[25] E. M. Redmiles, S. Kross, and M. L. Mazurek. 2019. How Well Do My Results Generalize? Comparing Security and Privacy Survey Results from MTurk, Web, and Telephone Samples. In *Proceedings of the 40th IEEE Symposium on Security and Privacy (S&P)*. IEEE, San Francisco, CA, 1326–1343.

[26] Guogen Shan and Shawn Gerstenberger. 2017. Fisher's exact approach for post hoc analysis of a chi-squared test. *PLOS One* 12, 12 (2017), 1–12.

[27] Madiha Tabassum, Tomasz Kosinski, and Heather Richter Lipford. 2019. "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 (SOUPS 2019)*. USENIX Association, Santa Clara, CA, 435–450.

[28] Madiha Tabassum, Tomasz Kosiundefinedski, Alisa Frik, Nathan Malkin, Primal Wijesekera, Serge Egelman, and Heather Richter Lipford. 2019. Investigating Users' Preferences and Expectations for Always-Listening Voice Assistants. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 3, 4 (2019), 1–23.

[29] Blase Ur and Yang Wang. 2013. A Cross-Cultural Framework for Protecting User Privacy in Online Social Media. In *Proceedings of the 22nd International Conference on World Wide Web (WWW)*. ACM, Rio de Janeiro, Brazil, 755–762.

[30] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. 2019. Privacy Perceptions and Designs of Bystanders in Smart Homes. *Proc. ACM Hum.-Comput. Interact.* 3, CSCW, Article 59 (2019), 24 pages.

[31] Tal Zarsky. 2013. *Transparency in Data Mining: From Theory to Practice.* Springer Berlin Heidelberg, Berlin, Heidelberg, 301–324.

[32] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End User Security and Privacy Concerns with Smart Homes. In *Proceedings of the 13th Symposium on Usable Privacy and Security (SOUPS 2017)*. USENIX Association, Santa Clara, CA, 65–80.

[33] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. User Perceptions of Smart Home IoT Privacy. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW (Nov. 2018), 20 pages.

[34] Verena Zimmermann, Paul Gerber, Karola Marky, Leon Böck, and Florian Kirchbuchner. 2019. Assessing Users' Privacy and Security Concerns of Smart Home Technologies. *i-com* 18, 3 (2019), 197 – 216.

APPENDIX

A SURVEY

A.1 Demographics

Following survey questions were posted on Amazon MTurk to obtain user responses catering to their concerns with using IoT devices:

(1) In which country do you currently reside? (drop down list)

(2) How old are you?
- 18 - 24
- 25 - 34
- 35 - 44
- 45 - 54
- 55 - 64
- 65 or older

(3) What is your gender?
- Female
- Male
- Prefer not to answer
- Other

(4) Have you ever used an IoT device, such as, but not limited to, Google Home devices, Amazon Alexa devices, smart light switches, smart thermostats, or smart doorbells?
- Yes
- No

A.2 Non-IoT Users

(1) Why have you not previously used an IoT device?
- I'm not tech savvy and do not know to operate them
- I see no immediate benefit in using these devices
- Lack good internet connection
- Too expensive in my country
- I am scared of how my personal data will be collected and shared by such devices
- Others, Please specify

(2) Does any of the following concerns preventing you from using IoT devices?
- There could be someone intercepting my data at the other end
- Might transmit extra data without my consent
- Security loopholes in the device. For example, passively listening in the background when it shouldn't
- Interference between devices on the network
- IoT has not evolved enough to deem useful
- Others, please mention below

(3) How much would you trust your government to enforce/pass consumer-friendly laws governing the collection and use of data by IoT devices?
- I would not trust my government at all
- I somewhat trust my government to have some laws
- I fully trust my government is taking/has taken efforts
- My government has sufficient strict laws in place that govern what information is being used

(4) For each of the following settings, please rate how you would feel about interacting with (or being captured by) an IoT device with the ratings being : Very Uncomfortable, Somewhat Uncomfortable, Neither comfortable nor uncomfortable, Somewhat Comfortable, Very Comfortable
- At Home
- With family/friends
- When with a colleague
- When interacting with a stranger
- At workplace
- During work hours
- After work hours
- In public space(e.g. Mall)

(5) Do you recognize the device in the picture? (attention check question)

- Google Home Mini
- Amazon Echo Dot
- JBL Wireless Speaker
- Sonos One
- Apple HomePod

(6) Which of the following actions would reduce your concerns about using IoT devices?
- Stronger government regulations
- More easily tune-able privacy settings
- Summary of various data collected and how is it used by the devices
- Third party security and privacy auditing (something like a security and privacy rating)
- None of the above
- Others(specify)

(7) Would you reconsider using any IoT devices in the near future?
- Definitely yes
- Probably yes
- Might or might not
- Probably not
- Definitely not

A.3 IoT Users

(1) You answered 'Yes' to owning an IoT device, what device(s) do you own?
- Google Home
- Amazon Alexa
- Philips Hue
- Ring Doorbell
- Wyze Doorbell
- Facebook Portal
- Tile Lock
- Smartwatch
- Other (please mention)

(2) How many IoT devices do you own?
- 1
- 2
- 3
- 4
- 5+

(3) For how long have you used IoT devices?
- 1 year or less
- 1 to 2 years
- 2 to 4 years
- 4 years or more

(4) What factors lead to buying/using an IoT device?
- Convenience
- I'm tech savvy
- Social Pressure (friends/colleagues bought it)
- Just wanted to try it
- Other (please specify)

(5) For each of the following settings, please rate how you would feel about interacting with (or being captured by) an IoT device with the ratings being : Very Uncomfortable, Somewhat Uncomfortable, Neither comfortable nor uncomfortable, Somewhat Comfortable, Very Comfortable
- At Home
- With family/friends
- When with a colleague
- When interacting with a stranger
- At workplace
- During work hours
- After work hours
- In public space(e.g. Mall)

(6) Do you recognize the device in the picture? (attention check question)

- Google Home Mini
- Amazon Echo Dot

- JBL Wireless Speaker
- Sonos One
- Apple HomePod

(7) Does any of the following concerns resonate with you when you use an IoT device?
- There could be someone intercepting my data at the other end
- Might transmit extra data without my consent
- Security loopholes in the device. For example, passively listening in the background when it shouldn't
- Interference between devices on the network
- IoT has not evolved enough to deem useful
- Others (please specify)

(8) How much would you trust your government to enforce/pass consumer-friendly laws governing the collection and use of data by IoT devices?
- I would not trust my government at all
- I somewhat trust my government to have some laws
- I fully trust my government is taking/has taken efforts
- My government has sufficient strict laws in place that govern what information is being used

(9) Would you buy another IoT device?
- Definitely, yes, I find them really useful
- No, as I don't see any need for it
- No, as they are not as safe as I perceived them to be
- Others (please specify)