Effective Privacy Policies for IoT Devices

Rutvik Kolhe
rkolhe@ncsu.edu
North Carolina State University
Raleigh, USA

Mohit Gupta
mgupta6@ncsu.edu
North Carolina State University
Raleigh, USA

Saurabh Joshi
sjoshi23@ncsu.edu
North Carolina State University
Raleigh, USA

1 INTRODUCTION

The Internet of Things, or IoT, is the next big thing on the market. Intel projected internet-enabled device penetration to grow from 24 billion in 2006 to 20 billion by 2020[1], which equates to nearly 4 smart devices for each human on Earth. The IoT devices include but are not limited to cameras, microphones, sensors. These devices extend from home, public spaces to the entertainment and professional environment. These devices are constantly in contact with us and thus it has become increasingly important for us to completely understand exactly how they work and what data enables to work them in that way. The scope of the project would include how to design and present the policies so that the trust is not hindered. The range of the project would also include formulating and designing the policies in such a way that gives some power back to the user. Also many times, users do not read the agreement due to its long length[2]. The project aims to design policies[4] in such a way that the user quickly understands the policies and still not losing the information. The possible way of doing so is by including a summary of critical points and also including pictures to represent otherwise verbose information

2 PROBLEM MOTIVATION

We have often seen the users tend to skip over the privacy policies and the terms of service of applications. Our this belief was also confirmed through the survey we took the results of which will also be included further. It is not difficult to see why the users skip over these policies as they are often too long[2] and the language used can also be very formal making it difficult for common users to understand. Users are often surprised when they read in news about what data is being collected and how it is used, but in reality user agrees to "most" of these things when they sign up for the services of application. Our motivation behind building these policies comes from these problems[3], we have tried to create a compact version of these long policies, understandably it is not possible to cover 100% of these long policies but we have tried to cover everything which in our opinion the user should be aware of before signing up.

3 RELATED WORK

[1]: Schaub, F., Balebako, R., Durity, A.L. and Cranor, L.F., 2015. A design space for effective privacy notices. In Eleventh Symposium On Usable Privacy and Security (SOUPS 2015) (pp. 1-17).
The authors found that the current IoT policies are not useful and also unhelpful, consequently, neglected by the users. The focus of the paper is to help designers to design policies effectively that addresses the requirements of audiences and also informs them about the system's limitations.

[2] : Sicari, S., Rizzardi, A., Grieco, L.A. and Coen-Porisini, A., 2015. Security, privacy and trust in Internet of Things: The road ahead. Computer networks, 76, pp.146-164.
The paper focuses on how data confidentiality and authentication can lead to a sense of privacy and trust among users and things, achieving this by enforcement of refined security and privacy policies for IoT devices and infrastructure. The paper also addresses the research challenges and existing solutions in the field of IoT security and privacy.

[3] : Abomhara, M. and Køien, G.M., 2014, May. Security and privacy in the Internet of Things: Current status and open issues. In 2014 international conference on privacy and security in mobile systems (PRISMS) (pp. 1-8). IEEE.
The paper discusses the current state of research on IoT security and privacy requirements, and also discusses

the possible future research directions for IoT privacy and security.

4 EXPERIMENTAL DESIGN

4.1 Privacy Policy Methodology

Currently, privacy policies are designed to fulfill business regulations[2][4]. However, policies should be integrated with the product design in order to design effective policies for the users. One of the main aspects of designing an effective privacy policy is to understand the audience that would be using the device / software[2][4]. In terms of IoT devices, we have focused our research on three general categories of IoT device users that cover Audio, Video, and Fitness/Health devices. The concerns pertaining to each device category vary based on the features provided by each device / vendor. For example - Policies pertaining to audio devices such as Amazon Alexa focus on protecting user's audio data while fitness devices such as Fitbit watches focus on preserving user's biometric information such as heart rate, BMI. The next area of focus was to summarize the long policies and explain sensitive information to the user that could be a potential privacy threat. We have referred certain products associated with each category and analyzed their privacy policies to come up with critical points that would be included in our condensed policy.

The privacy notice information can be shared in four different ways- Time, Channel, Modality, Control[2]. Based on our analysis, we concluded that every IoT product is associated with a mobile application that needs to be installed in order to sync user's data to a personal cloud account (Third-party included). We have designed our policies to be displayed just before the user signs up to create an account or an existing third-party account (Google, Facebook, Apple).

4.2 Data Collection

As mentioned above we divided our IoT devices categories into 3 types : Audio, Video and Fitness based. We reviewed the following device policy to observe what were the problems that can be encountered. Audio : Google Home Mini, Video : BleepBleeps baby monitor, Fitness based : Fitbit fitness band.

The following were the problems which we noticed :

(1) Google Home mini :
There are no separate privacy policies for Google Home, all the privacy policies[5] present as of today cover Google as an entire entity.

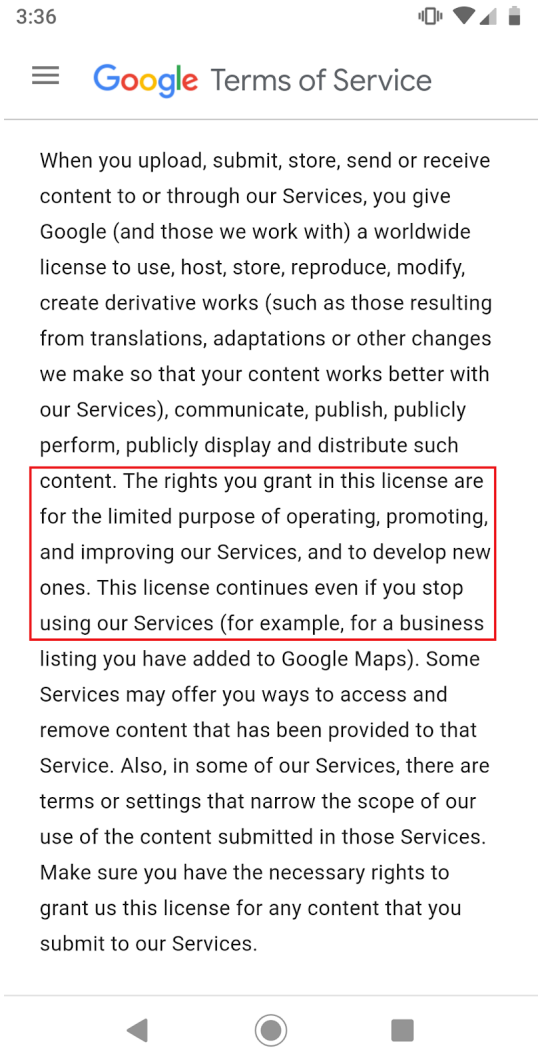

Figure 1

The Google Home app does not ask for any permission while you install it, as it uses the same permission you have given to Google on your phone. Moreover, While installing the Google Home app, you get the message shown in the right image and that's it! There is no mention of the type of data that will be collected or the type of sensors[12] that would be used. We plan on editing this by providing icons instead of the above message which will

then expand into short text summarizing policies. The text in the red box in the Figure 1 is something that the user deserves to know.

(2) BleepBleeps Baby Video Monitor:
One of the most significant drawbacks we found, is that the company has the same policy agreement[6] for all of its devices. Different devices collect different information, but the privacy policy is the same for all. While installing their application, Bleepbleeps assumes that the user is in compliance with their privacy policy. No power is given to the user to agree or disagree with their privacy policy.

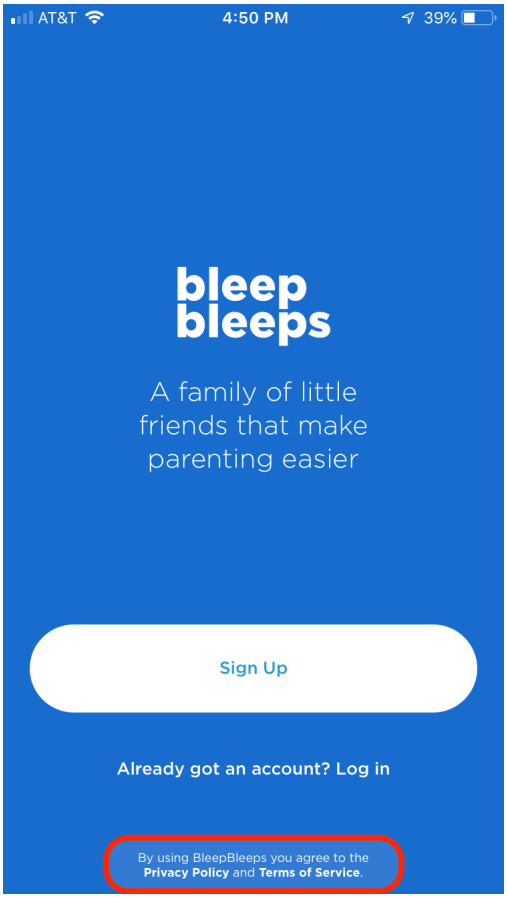

Figure 2

As shown in Figure 2, the privacy policy link's text size is small, at the bottom of the screen and could be inadvertently ignored by the users. The privacy policy has no mention about the methods of collecting information from the user. They have no mention about the types of trackers or sensors[12] used for providing certain features. For example- Baby Monitors would use a camera, microphone, and movement detector but nothing such as mentioned in the privacy policy. The policies also do not discuss the permissions that the IoT application is using. The user is given no option to turn off any of the sensors (speaker or microphone). The policy fails to address the type of data being collected. For example- There is no information whether the device is recording the videos or just providing real-time streaming to the users. Let's assume that they are recording the baby's movements. This could potentially have access to baby's sleeping patterns and medical conditions which is major privacy threat.
An additional drawback that we observed was that the user would not be notified after any changes in BleepBleep's policy. The company would simply update their policy on the website and leave it up to the user to check their website regularly.

(3) Fitbit Fitness Band:
The most critical privacy term that the product fails to address is the sharing of personal and non-personal information. The user is given an option to read the privacy policy before registration. The location and size of the privacy policy link is similar to that of the BleepBleep's application. The UI is switched from the mobile application to their privacy policy website. The text is almost 10-12 page long and does not highlight any privacy related sensitive points.

These were some of the distinct problems that we observed while reading detailed policies of IoT devices form all three domains. We conducted an initial survey[3][8] in order to confirm the general notion of people towards existing privacy policy matched ours. We asked the participants whether they found any scope for improvement in the existing policies. Furthermore, we asked them to choose some potential improvements listed by us. Finally, we asked them for their suggestions that they would like us to incorporate in our improved privacy model [10]. The number of user responses for this survey was limited to 10 people.
Based on our prior research and survey responses, the

following were existing problems that we had to address in our improved policy:

- Unstructured policy
- Verbose and lengthy
- Non interactive
- Excessive legal jargon
- No mention of application permissions
- Difficulty in locating important information

4.3 Improvised Privacy Policy Design

We noticed that there are two essential parts that the user must be aware of. Firstly, the permissions for the sensors[12] of the device and secondly, the policies & terms of usage.
A crucial point missing in the existing polices was that none of the apps asks for sensor or data specific permissions. For example- The mobile application for Bleepbleeps IoT devices does not ask for any sensor specific permissions. The privacy policies also do not have any mention about the sensors used. In order to improve this aspect of the policy, we have included a separate tab for "Permissions" in our design. This tab includes all the device related permissions required for the application to function. Each permission term is associated with a pseudo graphical icon to provide a visual hint of the permission/ sensor being used. Additionally, it includes a short text explaining the reason behind the requirement of that permission. For example- Fitbit devices requires permission to sensors which is required to calculate heart-rate and record sleep cycles. The permission would only be granted after the user clicks on the icon. We have divided the permissions of our policy into two parts- Essential and Optional. The essential permissions are the ones that need to be accepted to use the application whereas optional permission acceptance would be decided by the user. If the user opts-out of a certain permission, he/she is notified of the potential loss of features associated with the same. Users that are unconcerned about their privacy have an option to skip reading and setting the permissions manually. All the "essential" permissions would be set by default.
With reference to the policy tab, the user is provided with a quick summary of important points from the long policy. It will be mandatory for all the users to visit and read policy tab pages. Each page covers a point wise summary with a short description of the point. Our goal was to inform every user about all the permissions and policy points. We have ensured to include crucial points that directly affect the privacy of the user but were hidden deep into the privacy policy text.

We used wireframe software[7],[9] to design the improvised privacy policies[10]. Wireframe is software that is designed to mock up a wireframe layout as quickly and efficiently as possible. Furthermore, Wireframe software was chosen since it gave us the option to make privacy policies interactive. Users liked the mimicked wireframe design, especially the interactive feature. Below are the snapshots of one of the three wireframes, these provide a structure for audio devices.

Click on the following links to the wireframe designs created for three domains[7][9]:
Audio: Audio Wireframe
Video: Video Wireframe
Fitness: Fitness Wireframe

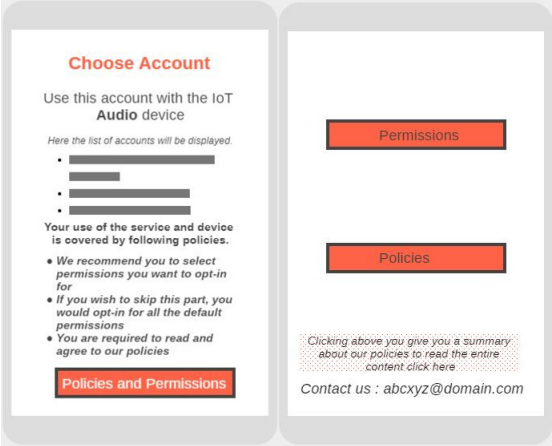

Figure 3

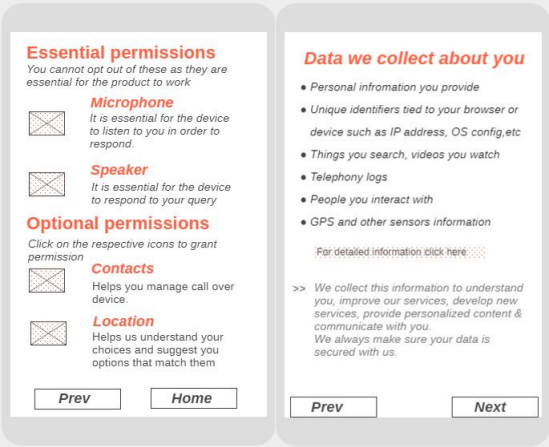

Figure 4

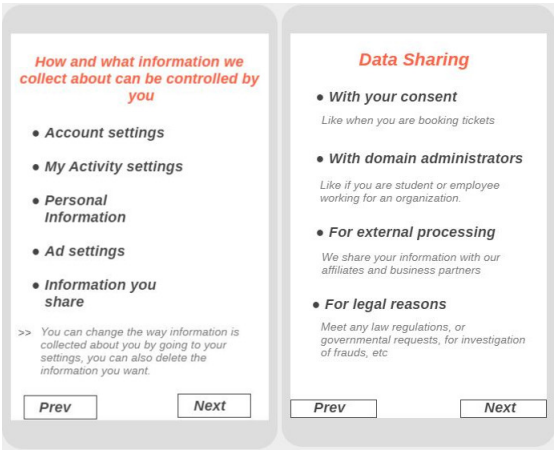

Figure 5

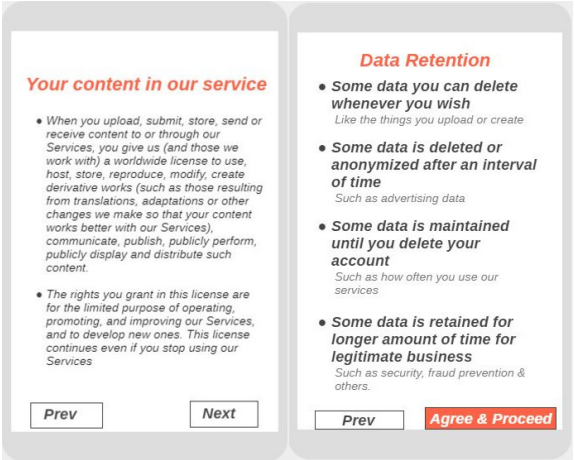

Figure 6

4.4 Experiment Setup

For the purpose of evaluating improvised policies, we conducted three surveys[3][8]. Each survey was designed to evaluate the improvised policy for each domain i.e. Audio, Video and Fitness. Further, each given survey had three sections. First section in each survey had questions to check the user's knowledge about IoT devices and its policy. It also contained questions to get insights into how often the user reads the privacy policy of their IoT devices. In each survey, we provided links for both standard policies and our improvised policies. Then users were asked "check questions" to determine the validity of the responses and also to assess the understanding of the users. Furthermore, we removed bias, if any, by randomly alternating the order of the standard and improvised policies that we gave users to read. So, a section of the people who were invited for the survey would be given the standardized policy first, and the other section of participants would be given the improvised policy first.

To recruit the people, we rolled out a survey on various WhatsApp and facebook groups. Furthermore, we requested people in-person to fill out the survey. To have the necessary diversity in the responses, we tried to get the responses from the computer science students, IT professionals, non-IT students, and non-IT professionals.

5 EVALUATION & RESULT

Let's us now see what were the results of our survey, section by section and also what did we infer from those sections.

Survey - Section 1

The questions in this section were to test the basic knowledge and usage of the IoT devices of the users. From the overall responses of the three surveys we could conclude that our audience had a fair idea about what are IoT devices. This does not come as a surprise since most of the audience we distributed the surveys to were in the age group of 20-30. Furthermore we asked questions about the kind of IoT device they had used and more than 90% of the users had used devices like Google Home mini, Alexa, Fitness bands, etc. We were fortunate in this regard since our questions were built

around these the domains of these devices.

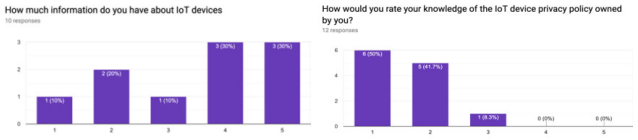

Figure 7

The next question checked whether the users read the privacy policy and how would they rate their knowledge regarding the same. It was surprising to see that irrespective of the amount of knowledge regarding IoT devices or which device they had used or not, majority of the people said that they were not interested in reading the policies. This result further motivated us to dig deeper into this topic. This was because there were people in our survey with knowledge about risks of privacy from such devices and still were reluctant to read the privacy policies before using IoT applications.

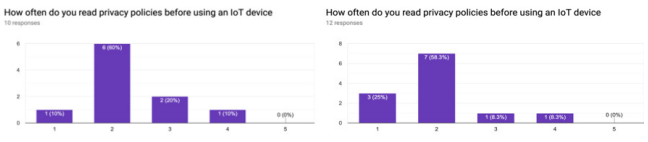

Figure 8

Survey - Section 2 and Section 3
Section 2 included detailed privacy policy for the particular privacy vendor associated with the survey[3][8]. Section 3 included link to the improved privacy policy[10] designed via Wireframe. The questions were designed in order to test the understanding of the participant about the privacy policy for each IoT device. The type of questions for both the sections were same in order to clearly compare the user's information about existing and improved policies. The questions were asked in the following order.

Q. 1 - Data collection :
The user should be aware about the type of information - (personal / non - personal) collected by the vendors [11]. The type of information may include name, email, gender, address, payment info, biometric information [11]. We asked this question to know the user's understanding about the information that is collected about him/her by the vendor. The options included in the questions were - IP address, OS config, SIM number, Device specific information (Hardware), biometric data. A couple of options were not applicable to all the IoT domains, this was deliberately done to test the participant's knowledge about the same. The responses for Audio and Fitness devices were almost similar before and after reading the improved policies [10]. We can observe that the responses for Google's privacy was a mix of all options. Most of the user's opted for all the given options. Whereas after reading the improved, the accuracy of the responses increased with the number of incorrect responses significantly decreasing. For ex- The device information, biometric and sim card info graphs have correctly decreased.

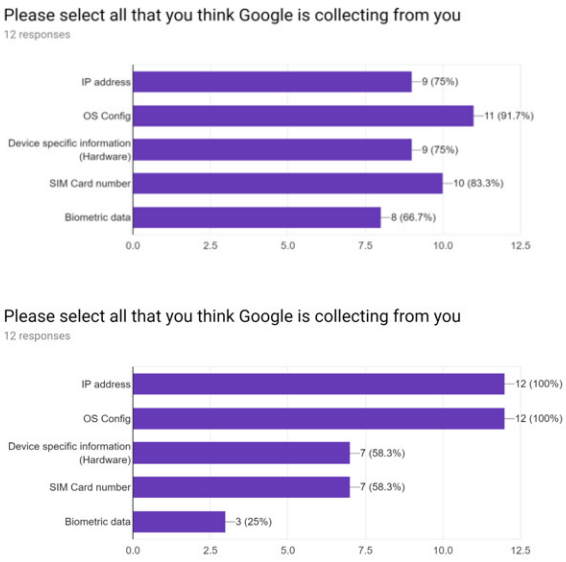

Figure 9

Q.2 - Data retention :
This question was aimed to check whether the user has knowledge about the amount of time for which his/her will be stored by the application. This question is important because the if the data is retained with the company for long amount of time it has risks, data leaks or other risks such as selling off information to third parties if the ownership of data changes. The most interesting response in this case was captured in the case of Fitbit's policy.

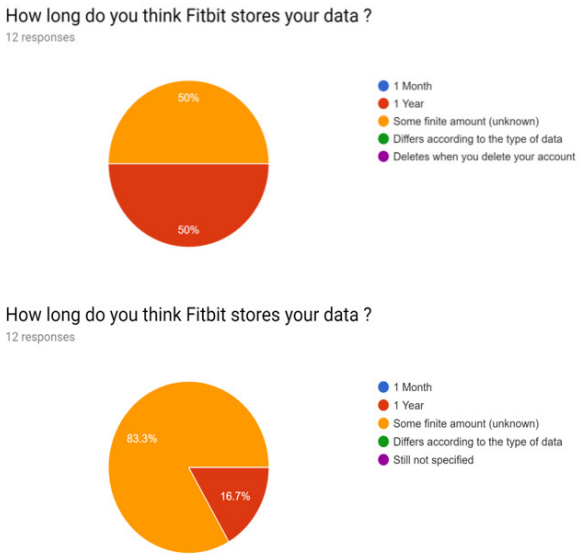

Figure 10

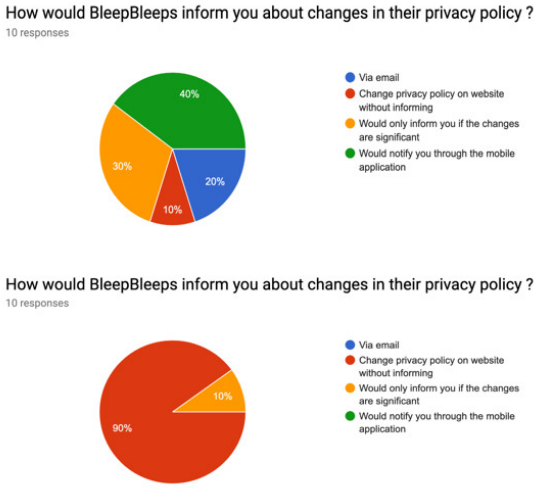

Figure 11

According to our research the Fitbit's policy was well sorted. The responses after reading the existing policy had accuracy of 50% which was good considering people had no interest in reading the policy earlier. But we were able to increase the percentage from 50% to 83% which is a significant increase. We had a page dedicated to showing this information in our wireframe[7][9] which indicated that Fitbit's stores the user information until the user has an active account. Below are the result before and after viewing the improvised version.

Q.3 - Privacy Policy Updation :

The focus of the question was to check the user's understanding of the change in the privacy policy. This question is important because many times, the company changes the privacy policy and does not informs the user. For instance, 80 percent of users responded with the wrong answer after reading the Bleepbleeps standard policy. The 90 percent of users reacted with the correct answer, i.e., "change privacy policy on a website without informing" after reading the improvised policy. We have explicitly mentioned this information in our wireframe design [7][9] and have a section associated with it since we think it's a critical piece of information.

Q.4 - Data sharing :

The focus of this question was to check the understanding about sharing of user data by the application company. It is important to check this factor since it is a major concern for privacy among the users as indicated by many research works in recent years.

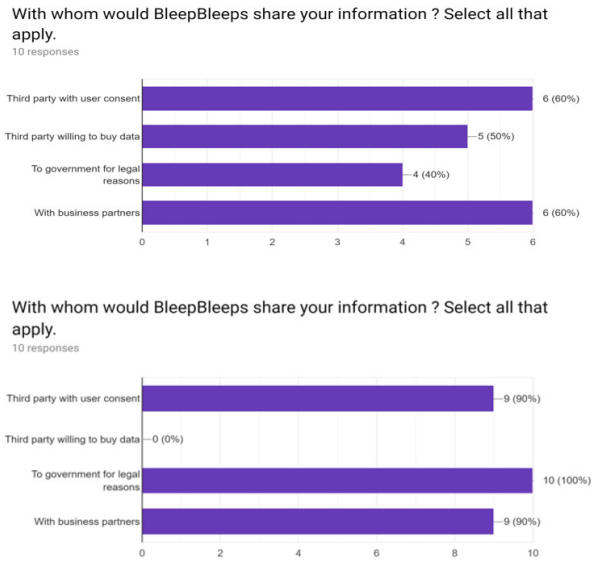

Figure 12

The policy of Bleepbleeps is obscure in this regard as this information is stored in a big chunk of text and

difficult to find. It was very surprising to see that the users answered more for selling to third party than sharing with government. Our wireframe had a specific page which covered this in detail that there is no trading of data with third parties. As a result we can see that users answered accurately keeping this in mind.

Q.5 - Sensor Information :
This question captures the user's knowledge about various types of sensors that are used by the application/device[12] for different features. We had included separate a section for device related permissions. The section included sensors included for each feature including graphical icons pertaining to the sensor used (For ex - camera, GPS, Pulse rate sensor). Due to the above reasons, the responses in Figure 13 showed a positive increase in the video device accuracy.

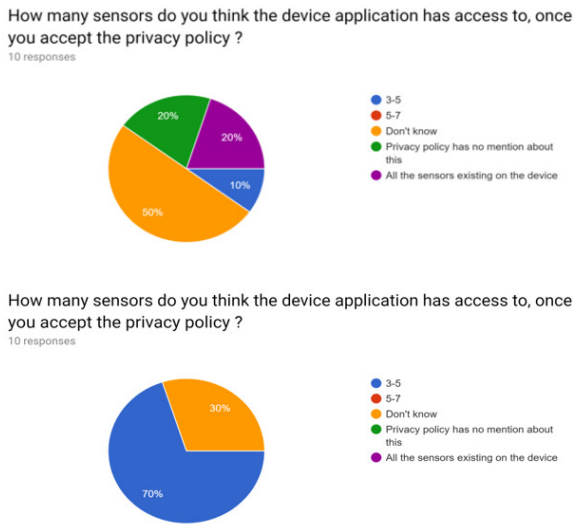

Figure 13

6 CONCLUSION

At the start of the project, we researched the possible problems in standard IoT privacy policies. We implemented certain solutions and hypothesized that the user would like the shortened and interactive version of the IoT policy. From the evaluations and the results shown in figure 14, it is clear that not only users want the improvised privacy policy but also have a better understanding when they read an improvised privacy policy design. We can conclude that the reason behind this is the structured and brief design of the improvised privacy policy.

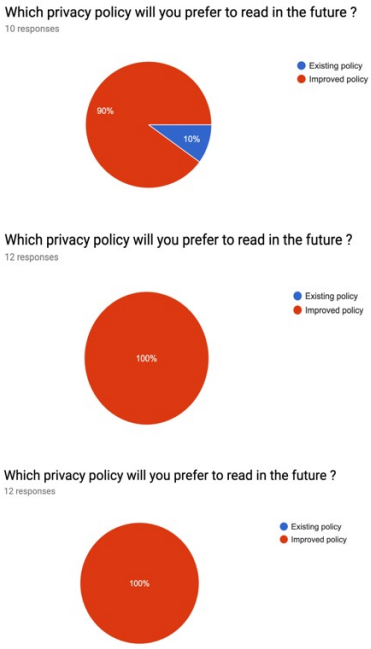

Figure 14

Figure 14 shows that 100% of the users who participated in health and audio IoT device domain-specific surveys preferred improvised IoT privacy policy, which we designed respectively. Furthermore, 90% of the users liked the improvised policy designed for video IoT devices.

7 LIMITATIONS

The improvised policy is the summarised form of a standard policy. Consequently, the improvised policy would lose some information. If the users want to have in-depth knowledge of the privacy policy, then the user has to read the standard policy. Furthermore, the company has to make changes in two separate policy documents in case of any policy update.

8 FUTURE WORK

The research could be extended to other domains of IoT devices, as well. The design policy was designed to be shown to the user explicitly only at the start of the application. The research could be grown upon,

and separate (or similar) privacy policy can be designed which would be shown while the user is using the corresponding feature [2]. Furthermore, a separate designed privacy policy could be designed that could be displayed or played (possibly audio) on the IoT device/ wearable rather than the mobile application.

9 INDIVIDUAL CONTRIBUTIONS

The project work completion and the individual contribution is as follows:

Task	Completion Date	Contributor
Understood the scope and found possible drawbacks in standard IoT policies	10/04	Rutvik, Mohit, Saurabh
Identified software to develop the UI prototype	10/07	Mohit, Rutvik
Literature survey	10/14	Rutvik
Evaluation plan, determined the IoT domains for which IoT policies would be redesigned	10/24	Mohit, Saurabh
Completed reading the standard policies and summarised critical points to be included in wireframe	11/13	Rutvik, Mohit, Saurabh
Created the wireframes	11/23	Rutvik, Mohit
Created and rolled out the survey to potential audience	11/24	Saurabh, Mohit
Final Evaluation based on survey results	by 12/04	Rutvik, Mohit, Saurabh
Limitations and Future Work	by 12/06	Saurabh
Completed the presentation	by 12/08	Mohit, Saurabh
Completed the final report	by 12/10	Rutvik, Mohit, Saurabh

10 REFERENCES

[1] "There will be 24 billion IoT devices installed on Earth by 2020" :
https://www.businessinsider.com/there-will-be-34-billion-iot-devices-installed-on-earth-by-2020-2016-5

[2] "Schaub, F., Balebako, R., Durity, A.L. and Cranor, L.F., 2015. A design space for effective privacy notices" :In Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)

[3] Janes, J., 1999. Survey construction. Library hi tech, 17(3), pp.321-325.

[4]Jensen, C. and Potts, C., 2004, April. Privacy policies as decision-making tools: an evaluation of online privacy notices. In Proceedings of the SIGCHI conference on Human Factors in Computing Systems (pp. 471-478). ACM.

[5] Google Privacy Policy
https://policies.google.com/privacy?hl=en-US.

[6] Bleepbleeps Privacy Policy
https://bleepbleeps.com/pages/privacy

[7] "wireframe software"
https://wireframe.cc/

[8] Couper, M.P., 2008. Designing effective web surveys (Vol. 75). New York: Cambridge University Press.

[9] Yang, Q., Zimmerman, J., Steinfeld, A. and Tomasic, A., 2016, June. Planning adaptive mobile experiences when wireframing. In Proceedings of the 2016 ACM Conference on Designing Interactive Systems (pp. 565-576). ACM.

[10] "2016 Model Privacy Notice "
https://www.healthit.gov/sites/default/files/2016_model_privacy_notice.pdf

[11] "type of data collected"
https://www.online-tech-tips.com/computer-tips/what-type-of-data-do-websites-collect-about-you-2/

[12] Masoud, M., Jaradat, Y., Manasrah, A. and Jannoud, I., 2019. Sensors of Smart Devices in the Internet of Everything (IoE) Era: Big Opportunities and Massive Doubts. Journal of Sensors, 2019.