An Investigation on Public Awareness Towards IoT

Data Collection

Jennifer Bidema
University of Guelph
jbidema@uoguelph.ca

Samuel Tracz
University of Guelph
traczs@uoguelph.ca

Abstract—**Smart devices and appliances have seamlessly integrated into our daily lives as we use them multiple times a day to provide convenience and efficiency. These devices achieve such things by collecting and utilizing user data, however many of those users may remain unaware of the extent and nature of the data being collected.**

This study investigates the public's level of knowledge regarding the collection of data by smart devices to determine if users are aware of the volume and type of data that is being collected. Utilizing a survey, we collected responses from diverse demographics encompassing various age groups, education levels, occupations, and geographic regions. The analysis identifies areas where user knowledge is lacking and examines those problems. Based on the findings, we create recommendations for IoT device manufacturers to take actions to increase user privacy knowledge and decrease user privacy concern.

Keywords—*Internet of Things (IoT), Smart Devices, Data Privacy, Data Collection*

I. INTRODUCTION

Smart devices are becoming more prevalent, embedding themselves into many of our daily activities. From voice activated assistants to fitness trackers, these devices offer the promise of convenience and efficiency. While smart devices may not be perceived as a necessity largely due to their cost [1], there is a significant potential for broader adoption of smart devices as they become more affordable.

Some users that adopt smart devices only use the device for a short period of time or when they do use it, they use it for the non-smart functions [2], but even during that time the devices continuously collect and process vast amounts of data to optimize performance and personalize user experience. A considerable portion of this data is processed through companion applications, which may unintentionally expose sensitive information to malicious actors [3]. These data handling practices often leave users unaware of what data is being collected and who will have access to that data. Consequently, instances where large companies like TikTok and Meta receive the data collected by smart devices like security cameras [4] become a normal practice.

Despite the importance of data privacy, many users that are conscious about their privacy often find it difficult to manage their privacy settings [5]. This leads to a scenario where users implicitly consent to their data being collected without the knowledge of it happening, or they have full knowledge of the practice but the necessary actions to protect the data are not taken. Both scenarios seem to show that users do not perceive immediate negative consequences with the use of their smart devices.

This study seeks to bridge the gap between user and manufacturer by evaluating the public's awareness and concern regarding data collection practices of smart devices and appliances. Through a structured survey distributed to a diverse demographic, we aim to determine the breadth and depth of user knowledge about data collection, their attitude towards privacy, and their concern in these practices. Ultimately, the goal is to empower consumers to make informed decisions about the use of their smart technologies by giving recommended actions towards manufacturers.

In a time where smart devices evolve rapidly, this study highlights the existing gaps in user knowledge and concerns and shows the necessity for manufacturers to educate users and have more transparent practices.

II. RELATED WORK

The privacy impact of smart devices is a significant area of research. This is an important area because there is an expectation of privacy from certain entities, yet we tend to use smart devices increasingly more as they advance in technology. Our study contributes to this area of research by getting a unique snapshot of user demographics and their knowledge regarding data collection practices.

Some users avoid smart devices due to privacy concerns. Lau et al. [6] found that people did not use smart speakers due to the distrust of the manufacturers and their privacy practices. Similarly, there are adopters of smart devices that show some concerns. Tabassum et al. [7] conducted a semi-structured survey with smart home users which revealed that many users understand that their data is being collected but feel a lack of ownership over their data and are uncertain about the data practices involved. This leads users to perceive an increased security and privacy risk.

Although some tend to be concerned about their privacy, they experience a net benefit from the use of a smart device and accept the tradeoff [8]. Zheng et al. [9] found that users prioritize convenience over privacy, causing limited actions to be taken against data collection. The users also put trust in the manufacturers to protect their privacy, but do not verify those actions. Research by Haney, Furman, and Acar [10] show us that users perceive that the responsibility for their privacy within a smart home is assigned in combination with users, manufacturers, and the government. This suggests that the data collection practice needs to be approached as a collaborative effort from the user, manufacturer, and government.

User perception of smart home surveillance has been explored as well. Zeng et al. [11] reviewed the mental models and determined that users do not perceive complete threat models when using their smart devices. Percy-Campbell et al [12] reviewed multiple studies to conclude that smart devices added perceived benefit, in this case safety for the smart home. However, it also highlighted that there is limited understanding of data collection practices or concerns.

III. MOTIVATION

The increased use of smart devices, and an increased pool of what is considered a smart device is being embedded into many aspects of daily life. They tend to offer convenience, but in turn collect data in the guise of personalization towards the user. However, this process often happens without the users' full knowledge of the extent and nature of the data these devices collect. Studies indicate that users like the benefits of smart technologies but frequently lack understanding of data collection policies.

Our study aims to build upon this existing research by targeting a differing demographic which allows us to assess whether advancements in smart device technology in combination with the passage of time have resulted in an increased user awareness of data collection. This approach will provide insight into how effective the education of user data collection and privacy awareness has been, and how manufacturers can further improve.

Enhancing user awareness is very important to allow them to make educated decisions about their data. This must start with determining what areas of awareness are currently lacking, and figuring out how manufacturers can be more transparent towards the user with regards to their data collection practices.

IV. SURVEY DESIGN AND DISTRIBUTION

The survey included questions covering demographics, smart device usage, awareness of data collection, privacy attitudes, and determining the user consent practices. The survey layout and questions were designed to be clear and well-presented. This included multiple-choice questions, Likert scale items, and open-ended responses to capture both quantitative and qualitative data. This questionnaire was created to minimize bias and increase clarity of the collected data [13]. This survey has been administered using Google Forms [14] and distributed through online messaging platforms and word of mouth.

A. Ethical Considerations

In accordance with ethical guidelines for research including human participants [15,16], informed consent was obtained from all respondents. Participants were provided with detailed information about the study's purpose and ensuring that the participation is voluntary. This aligns with the outlines in the Tri-City Council Policy Statement: Ethical Conduct for Research Involving Humans [15].

B. Pilot Testing

An initial survey has been conducted on a sample of members of the target population. This process allowed us to determine the clarity, neutrality and the potential for leading responses. The participants provided feedback on the wording of the questions. This pilot revealed that several questions contained leading language that could affect the reply. For example, questions would lead with "Are you aware that…", potentially influencing the respondents to agree.

Based on the pilot findings, the survey has been revised to contain more open-ended questions that adopt the Likert scale rather than emotionally charged yes-no questions. These revisions lower the risk of bias by allowing the respondents to express their feelings rather than being influenced in a certain direction.

C. Participants

The study engaged a diverse sample across a few countries, age groups, education levels, and employment statuses. There were responses from 3 different age groups, with 25-34 being the most common. The participants ranged in 4 differing answers with gender, with male being the most common. There were responses from participants with 6 different levels of education, with a majority having a post-secondary or professional degree. Most responses came from Canada, but there were responses from 3 separate continents. Most respondents were also employed.
Due to data anonymization protocols to protect participant confidentiality, specific demographic details cannot be disclosed to prevent potential re-identification of any individuals.

D. Data Analysis

Upon completion of data collection, responses were exported to ARX Data Anonymization Tool to ensure that the data in this paper would be anonymized and that no identifying data will be included [17]. Additionally, Google Forms has a built-in analysis tool that provides results in percentages, which provides an overview of the participants' awareness levels. There was not enough qualitative data to have an anonymized summary of answers, so they will remain and be referred to as "other" but will not be displayed in the bar graphs for anonymization purposes.

V. RESULTS

A. Smart Device Usage

This survey revealed that 34.4% of participants reported using 1-2 smart devices, while another 36.4% reported using

3-5 devices (Fig. 1). Just under 94% of respondents used smart devices multiple times a day (Fig. 2).
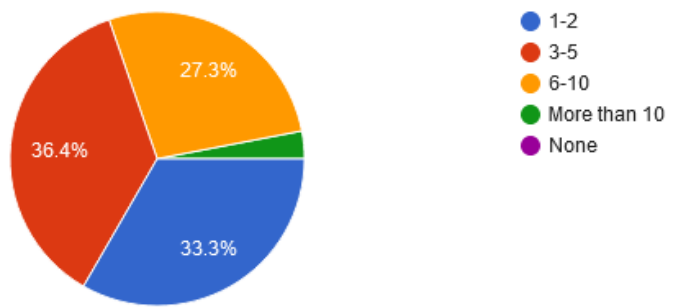

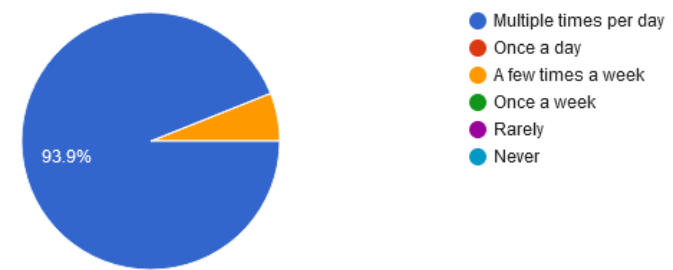Fig. 1. Number of smart devices owned or used in household

Fig. 2. Number of smart devices owned or used in household

B. Awareness of Privacy Practices

The levels of awareness of privacy practices from our participants had varying degrees. A majority (63.6%) believed that smart devices collect data to a great extent, while 33.3% believe that data collection occurred to some extent (Fig.3).
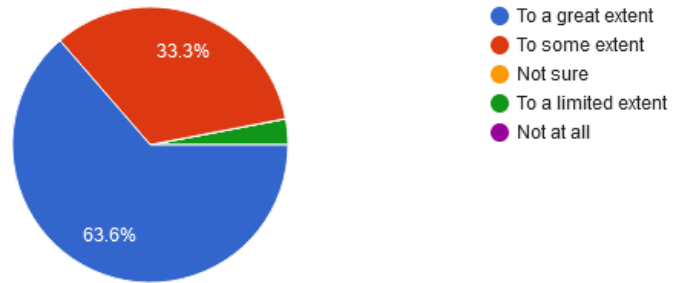

Fig. 3. Extent of data perceived to be collected by smart devices Example of a figure caption. (*figure caption*)

When asked about the types of data that smart devices collect, participants most frequently responded with personal identifiable information (87.9%) and location data (87.9%). Usage patterns and health data were both commonly believed to be collected as well at 75.8% each. Financial (57.6%) and "other" (6%) were the lowest perceived data collections (Fig 4.).
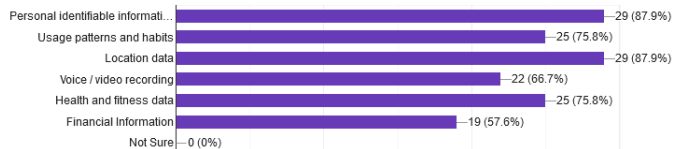

Fig. 4. Types of data believed to be collected by smart devices

This awareness of data being collected, however, did not translate into user engagement with privacy policies. 30.3% of participants stated that they occasionally read privacy policies, 33.3% responded that they only glance over them, and 15.2% admitted they never read them (Fig. 5). 75.8% of users also reported social media as the source of education for data collection practices.
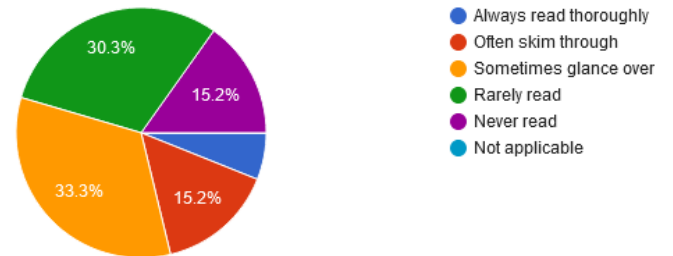

Fig. 5. Frequency of reading privacy policies

The knowledge about how data is shared and used seemed uniform. 81.8% believe that the data collected is used to improve service, 78.8% think that the data is shared with third parties, and 72.7% indicated that the data gets used internally. 6% were not sure how data is shared or used and 6% provided other ways that the data can be used (Fig 6.).

Fig. 6. User understanding of data sharing and usage practices

Finally, the awareness of data accessibility and data retention seem to have polarizing answers. 46.5% perceived that smart devices collect data no matter the state of the device, with an additional 18.2% thinking that only active use causes data collection. However, when asked about data retention, 36.4% admitted not knowing about the data retention period their smart devices use. A majority reported being slightly knowledgeable (24.2%) and somewhat knowledgeable (33.3%).

C. Attitute Towards Data Collection

Participants expressed different levels of concern regarding smart device data collection. Almost half (49.4%) expressed moderate to high concern, whereas 12% seem to have no concern (Fig 7).
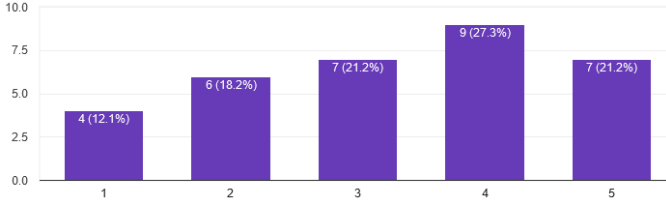
Fig. 7. Levels of concern regarding smart device data collection

Discomfort towards these practices was also prevalent, with 24.2% feeling very uncomfortable and 36.4% somewhat uncomfortable. 33.3% remained neutral.

Adding to the concerns and discomfort, a majority of participants (69.7%) believe that their privacy has been invaded due to data collection. However, when asked if the data collection practices made them hesitant to use smart devices, 36.4% responded "no". 33.3% were hesitant and 30.3% were sometimes hesitant (Fig 8.)
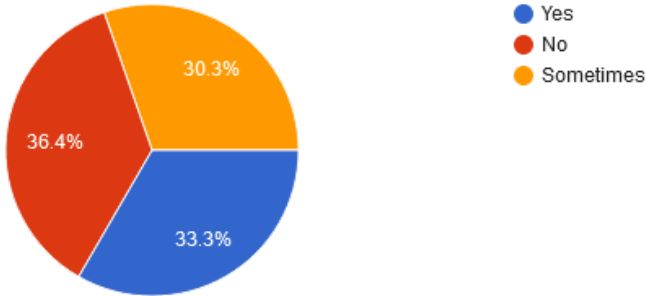
Fig. 8. Are users hesitant towards using smart devices

D. Engagement with Consent Practices

The survey showed us that there is limited understanding and engagement when it comes to consent practices. Only 9.1% of participants perceived to have a very thorough understanding of the consent process, whereas the majority said to have a limited (51.5%) to no understanding (3%) (Fig 9)
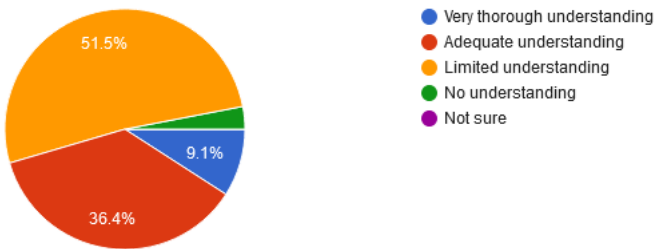

Fig. 9. Understanding of the consent process for data collection by smart devices

A majority (42.4%) of respondents admitted to skimming through user agreements or terms of service before accepting them, while 39.4% reported rarely reading them. When it comes to adjusting privacy settings on smart devices, 15.2% adjust them regularly. However, 42.4% rarely adjust privacy settings and 3% never do (Fig 10).
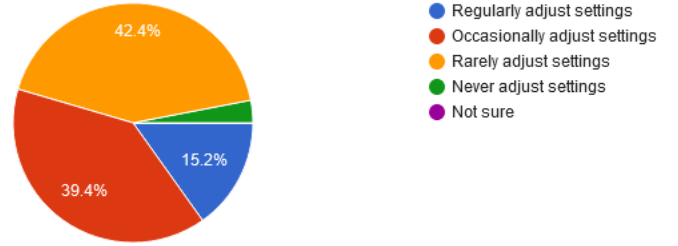

Fig. 10. How often users adjust privacy settings on smart device

VI. DISCUSSION

This study explored user awareness of data collection practices. The findings highlight that there are gaps in understanding and there are opportunities to educate the public on them. We additionally explored the user attitudes towards data collection practices to determine if the public would be willing to learn more, or if they are indifferent towards it.

We found that the overwhelming majority have at least one smart device which they use multiple times per day, which leaves a great opportunity for their data to be collected. The findings show that users believed a wide array of types of data were being collected. This is likely due to the differing data collection practices that a wide variety of smart devices use. Nevertheless, users seem to know that data is being collected to a varying degree.

A very informative result from this study is where users are educating themselves on smart device data collection practices. There is not as much first-hand education from manufacturers as there is from social media and the news. This is likely due to many factors; many people spend hours on social media [18] and there is anecdotal evidence that people are starting to prefer short form text over long form [19]. This can explain why short social media posts and news media take precedence over the manufacturers' own privacy policies and manuals. This suggests that manufacturers may be overwhelming the users with the amount of information, causing the user to refuse an attempt at educating themselves.

This gap in education is seen clearer in the responses regarding user consent over data collection. When a majority of users admit that they rarely read or skim through user agreements, that means that manufacturers give the users the opportunity to skim through the agreements. If those same agreements were in a digestible format, it would surely increase the number of users that would read the entire agreement. Due to the admissions of not reading through all the user agreements, it is understandable that the responses show us that users believe they have a limited understanding of the consent process for their data collection.

This study aligns with previous studies [5,7] showing that as much as it is a concern for the users to have their data collected, they do not feel like they are in control of their data. A strong correlation from this survey shows us that a small quantity of users regularly adjust privacy settings on their smart devices. This may mean that users do not see the value in adjusting those settings and may believe that it is not enough to stop the data collection.

VII. Conclusion

It is difficult to have a large understanding of smart device data collection practices in a world with rapidly evolving technology. Large neutral groups in the responses show us that users seem to have awareness of the practice but can be further educated on the practice.

The survey results from this study should be used as an indicator of whether user understanding of smart device data collection practices is heading in a positive or negative direction.

To effectively educate users while providing actionable recommendations to smart device manufacturers, it is important to present information in concise and easily digestible formats. Manufacturers should use social media platforms to convey this information since these platforms can reach a broad audience and align with the preference of short-form content.

References

[1] Coskun, A., Kaner, G., & Bostan, I. (2018). Is smart home a necessity or a fantasy for the mainstream user? A study on users' expectations of smart household appliances. International Journal of Design, 12(1), 7-20.

[2] A. Lazar, C. Koehler, J. Tanenbaum, and D. H. Nguyen, "Why we use and abandon smart devices," Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing - UbiComp '15, 2015, doi: https://doi.org/10.1145/2750858.2804288.

[3] Y. Nan et al., "Are You Spying on Me? Large-Scale Analysis on IoT Data Exposure through Companion Apps," www.usenix.org, 2023. https://www.usenix.org/conference/usenixsecurity23/presentation/nan

[4] P. Team, "Spies in your home: Which? warns of security camera that sends data to TikTok and washing machines that demand to know your age - Which? Policy and insight," Which?, Sep. 07, 2023. https://www.which.co.uk/policy-and-insight/article/spies-in-Your-home-which-warns-of-security-camera-that-sends-data-to-Tiktok-and-washing-machines-that-demand-to-know-your-age-aF55W5S5eNqB

[5] S. Park, M. Zimmer, A. Lenhart, and J. Vitak, "'Nobody's Happy': Design Insights from Privacy-Conscious Smart Home Power Users on Enhancing Data Transparency, Visibility, and Control." Accessed: Dec. 07, 2024. [Online]. Available: https://pearl.umd.edu/wp-content/uploads/2023/06/Park_etal-2023-SOUPS-smart-homes.pdf

[6] J. Lau, B. Zimmerman, and F. Schaub, "Alexa, Are You Listening? Privacy Perceptions, Concerns and Privacy-seeking Behaviors with Smart Speakers," Proceedings of the ACM on Human-Computer Interaction, vol. 2, no. CSCW, pp. 1–31, Nov. 2018, doi: https://doi.org/10.1145/3274371.

[7] M. Tabassum, T. Kosiński, and H. Lipford, "'I don't own the data': End User Perceptions of Smart Home Device Data Practices and Risks This paper is included in the Proceedings of the Fifteenth Symposium on Usable Privacy and Security. 'I don't own the data': End User Perceptions of Smart Home Device Data Practices and Risks," 2019. Available: https://www.usenix.org/system/files/soups2019-tabassum.pdf

[8] J. M. Haney, S. M. Furman, and Y. Acar, "Research Report: User Perceptions of Smart Home Privacy and Security," Nov. 2020, doi: https://doi.org/10.6028/nist.ir.8330.

[9] S. Zheng, N. Apthorpe, M. Chetty, and N. Feamster, "User Perceptions of Smart Home IoT Privacy," Proceedings of the ACM on Human-Computer Interaction, vol. 2, no. CSCW, pp. 1–20, Nov. 2018, doi: https://doi.org/10.1145/3274469.

[10] J. Haney, S. Furman, and Y. Acar, "'It's the Company, the Government, You and I': User Perceptions of Responsibility for Smart Home Privacy and Security 'It's the Company, the Government, You and I': User Perceptions of Responsibility for Smart Home Privacy and Security," 2021. Available: https://www.usenix.org/system/files/sec21-haney.pdf

[11] E. Zeng, S. Mare, F. Roesner, and P. Allen, "End User Security and Privacy Concerns with Smart Homes End User Security & Privacy Concerns with Smart Homes," 2017. Available: https://www.usenix.org/system/files/conference/soups2017/soups2017-zeng.pdf

[12] J. Percy-Campbell, J. Buchan, C. Chu, A. Bianchi, J. Hoey, and S. S. Khan, "User Perception of Smart Home Surveillance: An Integrative Review," Surveillance & Society, vol. 22, no. 3, pp. 304–324, Sep. 2024, doi: https://doi.org/10.24908/ss.v22i3.16084.

[13] K. KELLEY, B. CLARK, V. BROWN, and J. SITZIA, "Good practice in the conduct and reporting of survey research," International Journal for Quality in Health Care, vol. 15, no. 3, pp. 261–266, 2003, doi: https://doi.org/10.2307/45125879.

[14] Smart Device/Appliance Survey, "Smart Device/Appliance Survey," Google Docs, 2024. https://forms.gle/aMCFeaHBnrxTPtdWA (accessed Dec. 08, 2024).

[15] I. A. P. on R. E. Government of Canada, "Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans – TCPS 2 (2018) – Chapter 3: The Consent Process," ethics.gc.ca, Apr. 01, 2019. https://ethics.gc.ca/eng/tcps2-eptc2_2018_chapter3-chapitre3.html

[16] "Do I need Informed Consent from my survey respondents? | Office of Research," www.uoguelph.ca. https://www.uoguelph.ca/research/support-document/do-i-need-informed-consent-my-survey-respondents

[17] F. Prasser and F. Kohlmayer, "Putting Statistical Disclosure Control into Practice: The ARX Data Anonymization Tool," Medical Data Privacy Handbook, pp. 111–148, 2015, doi: https://doi.org/10.1007/978-3-319-23633-9_6.

[18] T. DeAngelis, "Teens are spending nearly 5 hours daily on social media. here are the mental health outcomes," American Psychological Association, Apr. 01, 2024. https://www.apa.org/monitor/2024/04/teen-social-use-mental-health

[19] R. Horowitch, "The Atlantic," The Atlantic, Oct. 01, 2024. https://www.theatlantic.com/magazine/archive/2024/11/the-elite-college-students-who-cant-read-books/679945/

Appendix

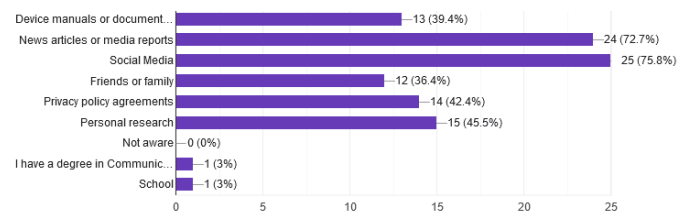### A. Additional Survey Results

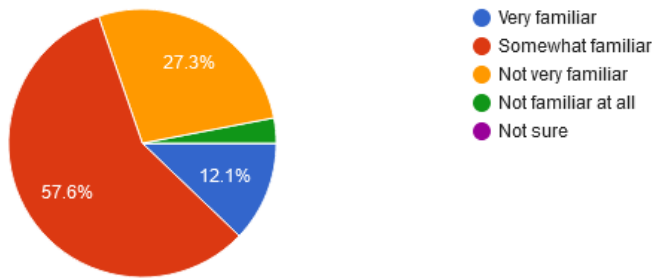Fig. 11. Source of education for data collection practices

Fig. 12. Familiarity with the data collection capabilities of smart devices when not actively in use
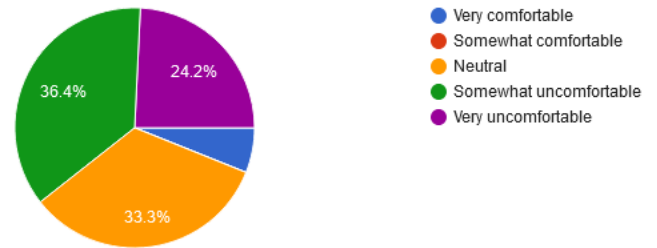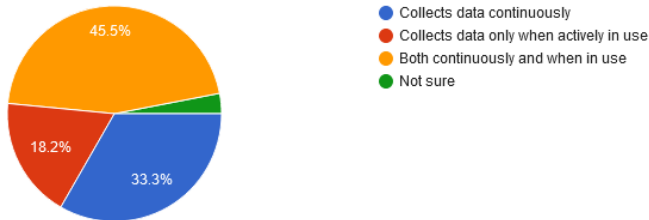

Fig. 13. Perception of data collection behaviour of smart devices

Fig. 14. Perception of how data can be accessed

Fig. 15. Understanding regarding third parties receiving data

Fig. 16. Knowledge regarding data retention periods of smart devices

Fig. 17. Feeling towards data collection

Do you believe that the data collected by your smart devices can impact your privacy?
33 responses

Fig. 18. Perceptions of privacy risks associated with data collection by smart devices
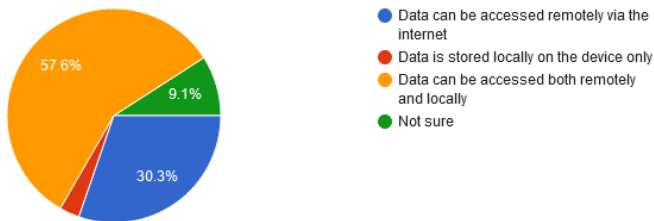
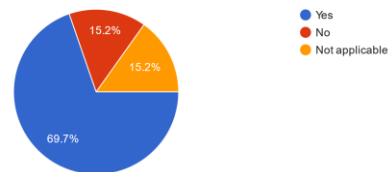Have you ever felt that your privacy was invaded due to data collection by smart devices?
33 responses

Fig. 19. Proportion of respondents who have experienced a sense of privacy invasion due to data collection by smart devices
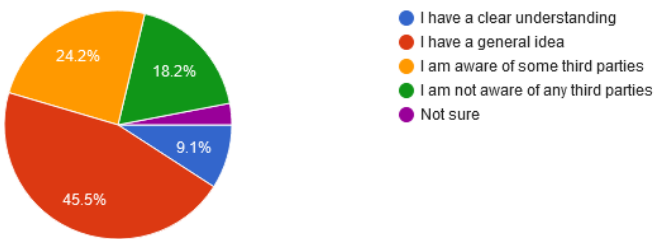
Do you think the data collected by smart devices can be used to personalize your experience (e.g., recommendations, services)?
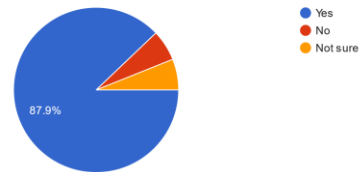33 responses

Fig. 20. Views on whether data collected by smart devices can enhance personalization
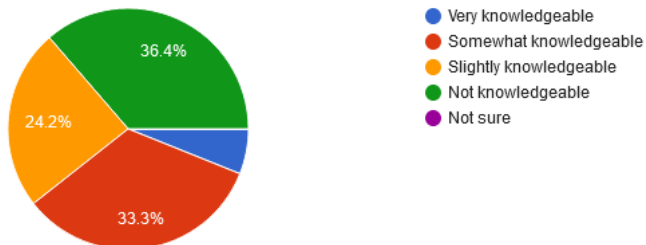
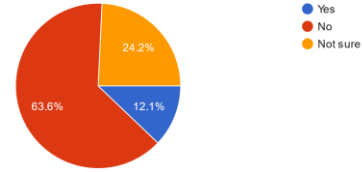Fig. 21. Thoroughness of reading policy agreements
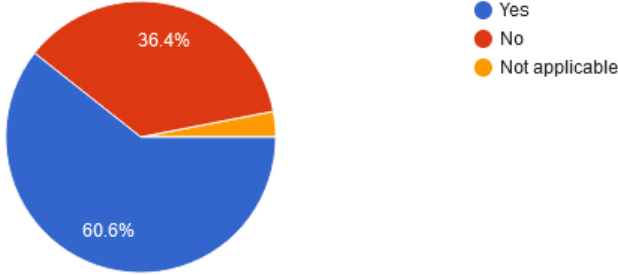

Fig. 23. Perception of control over data

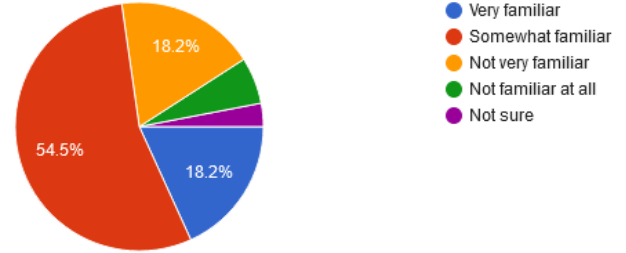Fig. 22. Awareness of data capturing policies before the purchase of smart device

Fig. 24. Familiarity of privacy settings available on smart devices to manage data collection

B. Participants

Table 1: The following table is an anonymized (3-anonymous) table of the participants that were involved in our survey. This shows the variety of smart devices considered in the survey.

What is your age?	What is your highest level of education completed?	What is your country of residence?	What is your employment status?	Which smart devices do you own or use? (select all that apply)
25-34	Higher Education	Canada	Employed Workforce	Smartphone, Smart Lock
25-34	Higher Education	Canada	Employed Workforce	Smartphone, Smart TV, Smart Doorbell (e.g., Ring Doorbell), Wearable devices (e.g., Smartwatch, fitness tracker)
25-34	Higher Education	Canada	Employed Workforce	Smartphone, Smart TV, Smart Speaker (e.g., Amazon Alexa, Google Home)
25-34	Higher Education	Canada	Employed Workforce	Smartphone, Smart Speaker (e.g., Amazon Alexa, Google Home)
25-34	Higher Education	Canada	Employed Workforce	Smartphone, Smart TV, Smart Speaker (e.g., Amazon Alexa, Google Home), Smart Lights, Smart Doorbell (e.g., Ring Doorbell), Wearable devices

				(e.g., Smartwatch, fitness tracker)
25-34	Higher Education	Canada	Employed Workforce	Smartphone, Smart TV, Smart Speaker (e.g., Amazon Alexa, Google Home), Smart Lights, Wearable devices (e.g., Smartwatch, fitness tracker)
25-34	Higher Education	Canada	Employed Workforce	Smartphone, Smart TV, Smart Speaker (e.g., Amazon Alexa, Google Home), Smart Doorbell (e.g., Ring Doorbell)
25-34	Higher Education	Canada	Employed Workforce	Smartphone, Smart TV, Smart Lock, Smart Doorbell (e.g., Ring Doorbell)
25-34	Higher Education	Canada	Employed Workforce	Smartphone, Smart TV, Smart Speaker (e.g., Amazon Alexa, Google Home), Smart Appliances (e.g., refrigerator, oven, washing machine), Wearable devices (e.g., Smartwatch, fitness tracker)
25-34	Higher Education	Canada	Employed Workforce	Smartphone, Smart Speaker (e.g., Amazon Alexa, Google Home)
25-34	Higher Education	Canada	Employed Workforce	Smartphone
25-34	Secondary and Pre-Degree Education	Canada	Employed Workforce	Smartphone, Smart TV, Smart Speaker (e.g., Amazon Alexa, Google Home), Smart Thermostat
25-34	Secondary and Pre-Degree Education	Canada	Employed Workforce	Smartphone, Smart TV, Wearable devices (e.g., Smartwatch, fitness tracker)
25-34	Secondary and Pre-Degree Education	Canada	Employed Workforce	Smartphone, Smart TV
25-34	Secondary and Pre-Degree Education	Canada	Employed Workforce	Smartphone
35-44	Higher Education	Unspecified or Diverse Locations	Employed Workforce	Smartphone, Smart TV, Smart Speaker (e.g., Amazon Alexa, Google Home), Smart Appliances (e.g., refrigerator, oven, washing machine)
35-44	Higher Education	Unspecified or Diverse Locations	Employed Workforce	Smartphone, Smart Lights, Wearable devices (e.g., Smartwatch, fitness tracker)

35-44	Higher Education	Unspecified or Diverse Locations	Employed Workforce	Smartphone
35-44	Higher Education	Unspecified or Diverse Locations	Employed Workforce	Smartphone, Smart TV, Smart Speaker (e.g., Amazon Alexa, Google Home), Smart Appliances (e.g., refrigerator, oven, washing machine), Wearable devices (e.g., Smartwatch, fitness tracker)
35-44	Higher Education	Unspecified or Diverse Locations	Employed Workforce	Smartphone, Smart TV, Smart Appliances (e.g., refrigerator, oven, washing machine), Wearable devices (e.g., Smartwatch, fitness tracker)
35-44	Higher Education	Unspecified or Diverse Locations	Employed Workforce	Smartphone, Smart TV, Smart Appliances (e.g., refrigerator, oven, washing machine), Smart Doorbell (e.g., Ring Doorbell)
35-44	Higher Education	Unspecified or Diverse Locations	Employed Workforce	Smartphone, Smart TV, Smart Appliances (e.g., refrigerator, oven, washing machine)
25-34	Higher Education	Canada	Independent or Educational Engagements	Smartphone
25-34	Higher Education	Canada	Independent or Educational Engagements	Smartphone, Smart Lights
25-34	Higher Education	Canada	Independent or Educational Engagements	Smartphone, Smart TV, Smart Speaker (e.g., Amazon Alexa, Google Home), Smart Lock, Smart Doorbell (e.g., Ring Doorbell)
25-34	Secondary and Pre-Degree Education	Canada	Independent or Educational Engagements	Smartphone
25-34	Secondary and Pre-Degree Education	Canada	Independent or Educational Engagements	Smartphone, Smart Doorbell (e.g., Ring Doorbell)
25-34	Secondary and Pre-Degree Education	Canada	Independent or Educational Engagements	Smartphone
*	*	*	*	Smartphone, Smart TV
*	*	*	*	Smartphone, Smart Lights
*	*	*	*	Smartphone

*	*	*	*	Smart Appliances (e.g., refrigerator, oven, washing machine)
*	*	*	*	Smartphone, Smart TV, Smart Thermostat, Smart Appliances (e.g., refrigerator, oven, washing machine)