IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received October 28, 2021, accepted November 15, 2021, date of publication November 23, 2021,
date of current version December 24, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3130086

"Why Should I Read the Privacy Policy, I Just Need the Service": A Study on Attitudes and Perceptions Toward Privacy Policies

DUHA IBDAH, (Member, IEEE), NADA LACHTAR, (Member, IEEE), SATYA MEENAKSHI RAPARTHI, AND ANYS BACHA, (Member, IEEE)
Department of Computer and Information Science, University of Michigan, Dearborn, MI 48128, USA

Corresponding author: Anys Bacha (bacha@umich.edu)

This work involved human subjects or animals in its research. The author(s) confirm(s) that all human/animal subject research procedures and protocols are exempt from review board approval.

ABSTRACT Online service providers are aggressively evolving the digital systems around us into surveillance platforms. From voice assistants that listen to every conversation, to apps that share sensitive location information, privacy experts have raised concerns about how such data is being abused. This comes at a time when advertisement campaigns can target users through social media platforms according to political party affiliations, reproductive health, and even religious beliefs. Such behavior raises concerns about how service providers leverage privacy policies to legitimately appropriate private data. In this work, we examine the user attitudes and perceptions towards privacy policies. We analyze user perceptions based on data collected from 655 participants. We use this information to identify different motivators and blockers that can influence the user's willingness towards reading privacy policies. We also examine the impact of previous user experiences such as cyber-attacks, as well as, online data sharing practices on reading such policies. Furthermore, we evaluate the ability of users to comprehend the content presented in privacy policies and the impact technical jargon has on the readability of such documents. Our study reveals that although less than 19% of our participants reported having some difficulty in understanding privacy policies, our study shows that more than half of the participants did not understand the content. Finally, we evaluate the implication of using different interfaces for conveying privacy policy content. We use this information to extract various pain points that could be used to assist researchers in improving the usability of privacy policies.

INDEX TERMS Privacy, privacy policy, data privacy, social media, terms of service, usability.

I. INTRODUCTION

The unprecedented growth of available data has transformed the way we approach everyday computing. The mobility of today's devices, fused with advances in cloud computing, continue to drive new synergies in the way online services are delivered to consumers, resulting in vast amounts of generated data [1]. This trend is exacerbated by the advent of the Internet of Things that is collecting staggering amounts of granular data on users that companies are increasingly harnessing for commercial purposes. Such commercial use, however, has been fraught with concern, prompting privacy advocates to sound the alarm on the risks associated with such practice. Unfortunately, despite a multitude of lawsuits and multi-million dollar settlements carried out against such companies [2]–[4], online services show no signs of abating, becoming increasingly invasive in the way they collect and exploit personal data.

In today's interconnected world, service providers are aggressively evolving digital systems around us into surveillance platforms. From voice assistants that listen to every conversation [5], to apps that share sensitive location information as their users roam around town [6]–[8], privacy experts have raised concerns about how such data is being abused. This comes at a time when advertisement campaigns can target users through social media platforms according to

The associate editor coordinating the review of this manuscript and approving it for publication was Fabrizio Marozzo.

political party affiliations, reproductive health, and even religious beliefs [6], [9], [10]. Such behavior raises an important question, "What entitles service providers to handle personal data in this fashion?" One way this question is being addressed is through privacy policies.

Privacy policies represent a legal contract between users and service providers. However, who actually reads such policies before simply clicking "I Agree?" There is a general reluctance to actually reading such policies, even though they contain pertinent information related to people's privacy and what parts of their personal data can be shared. Users often don't understand the risks associated with accepting privacy policies, resulting in privacy loss. This is exacerbated by the evasive and vague language service providers purposely use while drafting their policies. In addition to privacy policies becoming more complex, they have become significantly longer. For instance, Google's privacy policy evolved from 600 words back when it was a mere search engine to a whopping 4,000 word policy in order to reflect the practices the company engages in today [11].

Prior work examined privacy concerns of the general public with regards to their online activities. For example, a study conducted by the Pew Research Center determined that 50% of their participants were concerned about the amount of data collected by websites [12]. The study also found that 59% of their participants believed that it was possible to remain anonymous on the internet. They also found that participants were more proactive in taking steps to conceal their digital footprint from advertisers compared to the government knowing about their habits. In this work, we present a study on user attitudes and perceptions towards privacy policies. We analyze the reading behavior, frequency, and the user's susceptibility to change, in addition to categorizing what motivates the user's reading behavior. Furthermore, we divide the participants of this study into categories based on characteristics that lead to a change in behavior. We also evaluate their understanding of the content presented in privacy policies and their awareness of the actions they require. To this end, our study explores the following research questions:

Research Question 1: *Who reads the privacy policy and what is the user's general behavior towards such contracts?* In this question, we seek to understand the users' point of view on reading privacy policies, identify the characteristics of such users, understand how often they read such policies, and comprehend their general behavior towards keeping up with changes made to the terms of service.

Research Question 2: *What motivates users to read privacy policies and what prevents them from doing so?* In this question, we look into the reasons that motivate, prevent, and discourage users from reading privacy policies. We further analyze these reasons by grouping them into three categories, including: service, privacy policy, and user characteristics. In addition, we identify the main factors behind each category and how they impact consumers.

Research Question 3: *Do users understand the consequences of agreeing to the terms and services present in the privacy policy? We also explore the impact of these terms on users continuing to use the service once they understand the impact and if this would lead to any change in behavior for better privacy practices?* In this question, we analyze the overall user awareness about data collection practices and the various concerns it raises for the sampled users. Furthermore, we evaluate the percentage of users who take actions after reading the privacy policy, including changing default permissions and using opt-outs. We then correlate these actions to the level of concerns users report. Finally, we assess the willingness of participants to use custom services instead, in order to improve their privacy.

Overall, our study shows that 77% of our participants reported having some experience in reading privacy policies with the vast majority of the participants (72.4%) indicating that concerns about the service provider is the main reason behind users attempting to read such policies. We also determined that only a small fraction of our participants (12%) felt that it was unnecessary to have privacy policies in the first place. Many users expressed a general distrust in the way their data was handled, citing a lack of transparency by companies in the way they fulfill their contractual obligations when it comes to preserving private data and how most tend to demonstrate evasive behavior during this process. For instance, we found that participants shared the following views in response to some of the shady practices service providers engaged in: *"There's shady business going on behind the scenes. The Data industry is now the MOST VALUABLE industry in America."* Another participant said about service providers that, *"They aren't trustworthy, and you can't sue if they misuse your info anyway, because they all make us agree to "binding arbitration"."* Others even suggested that service providers are under the impression that it is more economical for them to violate the terms and conditions of their contracts in return for continued collection and misuse of user data, *"They state they will delete data or that you can opt out of things but you really can't. It's cheaper for them to violate their own ToS and pay a fine than to give up the data they claim not to collect."* These statements strongly underscore how users feel about service providers and the dilemma of absconding by the privacy policies they draft.

Furthermore, our data shows that over 75% of our users felt negatively about the way privacy policies were designed and the content they embodied. To this end, users cited the aforementioned concerns as a serious source of apathy towards reading privacy policies. For instance, when asked about the ability to opt-out from data collection practices, our participants overwhelmingly felt that service providers tended to employ evasive dark patterns that are designed to inhibit users from opting out of their services. For example, multiple participants indicated that there was really no way to opt-out of a service, *"We live in an age where privacy is gone. We can pretend we have control with opt-outs but we really don't."* Similarly, another participant stated the following about opt-out options, *"Anywhere... or nowhere. They are just for show, to make people feel like they have*

control over their data." The participants also felt that these services provided their users with little control over their data, irrespective of the claims made within the presented privacy policies. *"I believe that privacy is an illusion. You can blame my Political Science (BA) and Public Administration (MPA) background."* However, despite these views, in many cases, participants identified that loss of privacy was not enough of a deterrent for giving up the services they were accustomed to, *"Doesn't matter, I am not prepared to give up whatever services are involved so I just ignore the possible negatives like loss of privacy, etc."*

In addition to the aforementioned findings, our study shows that comprehension presented a major handicap in reading privacy policies. We found that although a mere 18.4% of our participants reported having some difficulty in understanding the privacy policy of popular websites, our study shows that 55% did not understand the actual content. For instance, while we found users to have an understanding of the impact of collecting information that directly links consumers to their identities, such as name, password, and IP address information, we found that users had little insight into the consequences of collecting geographical information such as location and signals and how this information could be abused. Finally, we find that although many users are not willing to give up the services they use in their entirety, 80% of them expressed willingness to consider non-customized services that don't rely on private data and present users with limited features in return for having some privacy.

Overall, this paper makes the following contributions:

- We conduct a large scale survey consisting of 655 participants to evaluate user attitudes and perceptions towards contemporary privacy policies and provide researchers with insights into how past experiences can influence the behavior of users towards such policies.
- We evaluate various factors that serve as motivators and blockers for reading privacy policies and cluster the reasons into different categories based on these factors.
- We present participants with various privacy policies from popular websites and capture their reactions towards the sensitive data they collect. We also assess the participants' comprehension levels of privacy policies and the impact technical jargon has on the readability of such policies.
- We characterize the implication of using different interfaces for conveying privacy policy content and out-opt information. We use this information to extract various pain points that could be used to assist researchers in improving the usability of privacy policies.

II. RELATED WORK

A large body of work has explored different concerns related to privacy and data sharing practices when using online services. In this section, we discuss prior work that is closely related to our study, such as challenges associated with the readability of privacy policies and user perceptions on sharing data.

A. COMPREHENSION OF PRIVACY POLICIES

Prior work [12]–[19] has shown that online consumers often face considerable challenges in understanding the terms and conditions they agree to when signing up for a service. Different studies reported that the main inhibitor to the user's comprehension, after analyzing several policies in the wild, stems from the type of language employed in privacy policies. Studies found privacy policies to often be riddled with legal and technical jargon that makes them inaccessible to the average user. For instance, Luger *et al.* [19], conducted a study that focused on the readability of the terms of conditions of websites. More specifically, they examined the readability of the terms and conditions documents associated with webpages that belong to different energy companies within the U.K. They determined while using a readability formula known as SMOG [20], that a number of policies required comprehension levels that were well beyond the abilities of the average adult in the U.K. These findings raise concerns about the fact that a significant portion of the society tend to unknowingly consent to terms and conditions of websites they don't understand. To address these concerns, Luger *et al.* proposed the use of a browser plugin designed to assist with obfuscated language embedded in the terms and conditions documents once they are displayed to the user.

Other work by Jensen *et al.* [21] focused on examining the readability of several privacy policies using a different metric that is known as the Flesch Reading Ease Score (FRES) [22]. The authors of this study determined that over half of the privacy policies they selected in their study were inaccessible to more than 56% of the internet population due to the complexity of such policies. Similar findings were reported in another study that focused on policies related to the financial sector [16]. Other work by Graber *et al.* [17] focused on privacy policies related to health websites. They concluded that policies of the aforementioned websites required an average of two years of college in order for them to be understood, suggesting that the privacy policies used by health organizations are considered difficult to comprehend by most users. Other work by Proctor *et al.* [23] conducted a similar study on the readability of a diverse set of existing privacy policies and determined that a mean grade level of at least 13 years was required to understand the average online policy. Work by Pollach *et al.* [18] determined that many companies use modal verbs in order to make their policies vague. The study also suggests that privacy policies are written with litigation in mind instead of fair handling of user data. Other work [24] focused on analyzing various privacy policies related to social network websites. The authors also concluded that service providers often use difficult legal jargon that effectively renders the presented policies inaccessible to the average user. They also suggest that the readability of such policies is aggravated by the lack of consistency in terms that are employed across different websites. While their study entailed reviewing privacy policies of different social

networking websites and the type of data they collect, they did not survey any users on their perspective. Although many of these studies made an attempt to gain insight into how well privacy policies were understood by consumers, such studies did not consider the perspective of real users, but instead relied on various formulae such as SMOG as a way of assessing readability. Since readability is a much broader issue, our study relies on real participants reading various privacy policies and reporting on their perspectives.

B. USER PERCEPTIONS ON DATA SHARING

Multiple bodies of work [24]–[32] examined user perceptions on data sharing practices. For example, Fiesler *et al.* [26] examined public reactions in the wild in response to data sharing controversies and how news outlets shaped the attitude of users on privacy violations. Other work by Felt *et al.* [27] examined the behavior of mobile consumers and how permission requests influence users in forgoing the installation of such apps. On the other hand, work by Shklovski [28] investigated the attitudes of users towards apps accessing personal data, such as photos on their smartphones and how this affected their decision toward installing mobile apps. The study concluded that in general, users aren't necessarily careless about privacy, but rather they feel a sense of helplessness and would rather just benefit from using the service irrespective of what data is collected.

Work by Carrascal *et al.* [32] concluded that privacy concerns would be quiesced if service providers were open and direct about their data collection and usage instead of using evasive language. They determined that being more direct with users about how their data would be monetized, as suggested by Xu *et al.* [33] would reduce the perception of privacy violations. Other work by Ermakova *et al.* [34] investigated the impact of privacy policies on consumer trust. They found that a strong correlation exists between privacy policy, comprehension, and how users entrusted their information to be shared with online service providers. They concluded that the better the user understood the presented policies, the stronger the trust they had in the website handling their data. Finally, work by Leon *et al.* [31], focused on "online behavioral advertising" on websites. More specifically, they explored the willingness of users sharing data as a function of the data retention period and the ability of users to control the collected data and be able to delete it after expiration of the retention period. Unfortunately, they found that most services take an all-or-nothing approach on data collection which made users reluctant about sharing their information. Our study builds on many of these findings with more focus on how negative experiences, such as malware infections and identity theft impact users in sharing their personal information, as well as, how this affects their pro-activeness in considering other services.

Privacy policies are used to inform the user about how their data will be collected and consumed after using a given service. A study by Habib *et al.* [35] showed that more than 90% of the tested websites offered opt-out options from email communication and targeted advertisement. Furthermore, 75% of the examined websites offered data deletion options. Unfortunately, the study also found that 80% of these websites omitted important details about how to opt-out of their services. A common theme amongst many privacy policies is ambiguity. The same study in [35] found that policies employed different formats and wordings for expressing similar information as a way of confusing consumers. For instance, Fabian *et al.* [36] conducted a large scale study of examining the readability of 50,000 website privacy policies. The authors found the average privacy policy length to have 1,700 words and required some college education to comprehend the studied policies. A general remedy to this problem lies in using privacy policy agreements to enforce consumer protection and control service provider misuse. For instance, the EU's General Data Protection Regulation (GDPR) set some standards for privacy policies in Europe and enforced privacy regulations and transparency in order to protect consumer data. Linden *et al.* [37] found that GDPR generally motivated enhancement in the privacy policy's appearance and presentation of EU based websites. However, a downside to this approach is that it caused a considerable increase in length without structural improvement.

C. PRIVACY POLICY INTERFACES

Many researchers explored the enhancement of privacy policy interfaces in order to enhance comprehension and clearly communicate to consumers the available privacy controls [23], [25], [34], [38]–[40]. Tabassum *et al.* [25] explored the use of comic-based interfaces and their impact on users in terms of attention and comprehension of the terms of service agreement presented in privacy policies. The authors determined that comic-based policies held user attention longer compared to text-based alternatives, and the consumers' comprehension level of the content improved. In addition, several other interfaces have been investigated for presenting privacy policies. For example, Lipford *et al.* [41] conducted a study that compared the tradeoffs between using the Audience View and Expandable Grids policy representations and how such interfaces translated to users changing their social network settings after going through the policies. In addition, this study suggested that combining these two interfaces presented users with better readability prompting many users to change the privacy and security settings of their accounts. Other work by Schaub *et al.* [42] explored the impact of a multi-dimensional design space including timing, channel, modularity and control, and the effects they have on easing the design of privacy notices and their integration into a system with minimal disruption to the system's interaction flow. Our study builds up on these interfaces, including other designs. We collect their feedback and discuss recommendations on how to improve privacy policy interfaces across mobile devices and standard webpages tailored for the typical computer system.

D. THE PARADOX: PERCEPTION VS. BEHAVIOR

A variety of research work explored the privacy concerns of online users and the possibility of misusing it. An early study [43] discussed the concept of the *"Privacy Paradox,"* which points to the reckless privacy behavior in spite of the existence of privacy awareness. This behavior may be a result of various theories such as social interactions, psychological impact, and economics [44]. Many studies explored the evaluation of online user data sharing behavior on social media in addition to their concerns towards privacy. For example, a study [45] on college students showed that many leverage their account profile settings to protect themselves against possible privacy violations. However, many online users, such as users with active Facebook accounts, tended to share more sensitive data without any awareness of how their information was viewable by unintended audiences and how existing tools could be leveraged to limit access to such data [46], [47]. Other studies discussed how users manage their privacy concerns by limiting access to their data [48], or by stopping the use of such platforms [49], [50]. For instance, [51], [52] examined the understanding of the risks associated with data sharing practices and found that participants do indeed understand the risks associated with making their data public. However, the study also concluded that users often felt a lack of control over their shared data due to the ambiguity of what was being collected and by whom.

Other work focused on consumers reading privacy policies in response to notices sent by service providers. A study by Milne *et al.* [53] investigated why online consumers read privacy notices across a variety of situations. The authors found that the reading of such notices is typically related to concern for privacy, positive perceptions about notice comprehension, and higher levels of trust in the notice. In addition, the authors determined that consumers generally felt that reading privacy notices represented the only element in an overall strategy consumers use to manage the risks of disclosing personal information to online service providers. Other work by Groom [54] assessed the reading behavior of online consumers. The study determined that none of the participants clicked on the policy link during engagement with a fictitious search engine. Similarly, Obar *et al.* [55] conducted a study on people ignoring privacy policies and terms of agreement. The authors determined that 35% of their participants acknowledged not reading the privacy policies for any of the services during the sign up process.

III. METHODOLOGY

In this section, we outline our approach for creating the survey and collecting the data. Furthermore, we describe the analysis approach we use in this study.

A. PILOT STUDY

We created a preliminary survey to explore user perceptions of our research questions and to ensure quality survey questions. We recruited 36 local participants from our university to complete the initial survey prior to launching the full study. The age group of the participants ranged between 18 and 44. The gender breakdown of this group was 44.4% male and the remaining 55.6% were female. We analyzed the data obtained from this initial group of participants and used this information to refine our survey questions in preparation for the final study. None of the data collected during the pilot phase was incorporated in the analysis of the final study.

B. DATA COLLECTION

The survey was approved by our Institutional Review Board (IRB) before it was published on the Amazon Mechanical Turk platform for recruiting participants. All the participants resided in the United States and were 18 years old or older. Participants were also required to have a HIT approval rate of over 95% and more than 1000 completed assignments in order to participate in the survey. Mechanical Turk was selected for the ease of recruiting demographically diverse workers [56], [57], where the bias of these samples are well studied by [58]–[61]. Respondents had the option to withdraw at any point from the survey without providing any reason. The survey took approximately 25 minutes to complete. Each participant was awarded $4 for completing the survey with payments carried out directly through the Amazon Mechanical Turk system. To ensure high quality responses, we included two attention check questions and only discussed the results of the participants who passed the attention checks.

We developed a systematic approach for answering our research questions. We gathered information about the education level of the different participants, security knowledge, amount of data shared using online platforms, and time spent online. We then examined the data for possible relationships across the aforementioned four factors to determine if any correlation existed between knowledge in security, online habits, and users reading privacy policies. Most importantly, we utilized this information to answer the fundamental question of *"What motivates users to read or disregard privacy policies?"* Below is a high level overview of the questions we used for collecting our data.

C. THE SURVEY

Our survey addresses five main areas: (1) demographics and information about general online practices (2) security and privacy concerns (3) behavior towards privacy policy (4) reaction towards provided policy specifications. (5) and reflection about the survey. Below is a high-level overview of the questions we used for collecting our data.

Time Spent and Information Shared Online: We asked participants questions about their online habits including the average time they spend online, and the type and quantity of data they voluntarily share with online platforms. We allocated points to the different options under each question in order to compute a score that was used to rank the respondents and classify them into categories according to their responses. We divided participants into three categories using this point

system: users who spend 0 – 4 hours online and share a small amount of information, users who spend 5 – 8 hours online and share a medium amount of information, and users who spend more than 8 hours online and share a large amount of information. This allowed us to examine if the amount of data shared had any bearing on users reading privacy policies. The point system we used can be found in Appendix C.

Understanding of Security: We asked participants a series of questions that allowed us to assess their security acumen. This entailed asking them a range of questions including their experience with encryption and the kinds of passwords that they prefer to use. We also asked respondents about their concerns about privacy. For example, we asked them questions about their privacy settings for their social media accounts and if they have ever changed any of the default settings. Similarly, we used a point system for ranking the participants based on their responses for security related questions. The point system we used can be found in Appendix C. We also took into consideration the demographic information of each participant, such as the level of education and primary occupation. We divided respondents into three categories using this point system: limited security knowledge, medium security knowledge, and good security knowledge. This served the purpose of evaluating the impact of security acumen on users reading privacy policies.

Behavior Towards Privacy Policies: We asked a series of questions to understand the general behavior of users towards privacy policies, as well as, what motivates end users to either read or ignore such policies. After we learned about the participants' general security and privacy perceptions, we explicitly asked them about their attitude towards privacy policies. Furthermore, we divided participants into two categories according to their answers to the following question: *Have you ever read or tried to read any website's or application's privacy policy?* Most mobile applications do not have their own built-in interface for viewing the privacy policy interface and therefore, rely on links that forward users to external websites that contain the relevant information. As such, we collected additional information to understand the type of device users prefer for reading privacy policies.

Opt-Out Services: We asked participants about their attitudes towards opt-out services. We began by defining opt-out services and how they are used. An opt-out service is a service that gives consumers the ability to opt-out of sharing certain private information with a given website or application provider. We then assessed the attitudes of our participants towards such services and their understanding of their rights to opt out of sharing their data. In addition, we asked about their experiences with such opt-out services, if they had any, and the ease of locating the necessary information and being able to successfully request opt outs. We also asked participants for their perceptions on the necessity of having opt-outs for services that collect user data and the need to include such information within privacy policies. Finally, we asked the respondents if the presence of an opt-out service made them feel more in control of their shared data.

Perspective on Privacy Policy Content: We asked participants different questions to assess their ability to comprehend privacy policies. We presented the participants with passages from privacy policies of popular services, including Facebook, Google, Amazon, and Uber. We then tested their understanding of the information presented in each privacy policy and asked them whether readability was a motivating factor for users to read privacy policies. In addition, we collected the respondents' perspectives on the kind of information services collect based on their privacy policies and whether that was necessary. For example, we asked them questions about commonly known data usage practices by service providers, such as *"If you are using any applications by Google, do you know that Google stores all your information provided, like operating system, mobile network information, including carrier name and phone number, IP address, crash reports, system activities, date, time, etc?"* We also asked them questions that disclose largely unknown information by the common end user about their data usage, such as *"Do you know that Facebook, Instagram, and WhatsApp track your device signals to collect information about other devices surrounding you?"* We also asked the participants if they were willing to turn down the service if they felt the privacy policy was invasive.

Behavior Change Questions In addition to finding out if users knew about the information included in privacy policies, we looked for passages that made users become concerned with the content included in them. We also asked respondents to compare their behavior towards privacy policies over the past five years and if taking the survey changed their attitude and why. We took into consideration the rapid increase in processing and sharing of private data online. Furthermore, since reading the policy is hard to track and enforce, unlike other security and privacy-related behaviors, we tested other triggers. We considered the effect of cyber-attacks on reading the policy in comparison to other behaviors. Finally, we gauged the willingness of our respondents to read privacy policies after educating them about how to locate such policies, the content included in them, and the advantages and disadvantages of not reading them. We also questioned them about their willingness to give up a service if they ever felt uncomfortable with the stated privacy policy.

Privacy Policy Interface Questions We asked participants about their perceptions on the interface and the link placement of the privacy policy. To understand the impact of the interface on users reading the policy, we presented participants with five privacy policy designs that ranged from simple plain text interfaces to summary videos. We then asked them questions about the user friendliness of each interface and which one they would consider using. We also asked the participants open-ended questions about their expectations and preferences for privacy policy interfaces. Similarly, we asked them questions to understand if the placement of the privacy policy link on websites and mobile applications had any impact on the consumers reading it. We presented participants with a range of options including adding a privacy policy link to the bottom of a webpage as a footer, checkout pages, mobile

app stores before download, and popups. We also asked the participants open-ended questions about their preferences for privacy policy link placement.

D. QUALITATIVE ANALYSIS

We used participant answers to extract user characteristics. We managed to extract the following characteristics: 1) Background security knowledge, 2) Pro-activeness towards security and privacy, and 3) Online presence. To achieve this, we first tested the relationship between these characteristics and demographics. Then we found how each one relates to the interaction and perception of the privacy policy. We used Chi-square association tests for achieving this. Furthermore, we divided the participants of our survey into personas. Each persona represented a type of user with certain experiences, behaviors, and expectations. We used statistical correlation to link the most related demographic and behavioral answers. We then used these answers as input into a K-means algorithm to produce different categories of users. We then divided the answers into an experience map that allowed us to extract different pain points.

E. LIMITATIONS

Even though studies have shown that Mechanical Turk workers are demographically diverse [56], [57], such workers have been reported to be technically savvy compared to the broader population [60]. In addition, other work has discussed Mechanical Turk workers being more privacy aware compared to the overall population [62]. Therefore, data from such respondents may not be generalizeable to the broader population of users. Our study is limited to US participants. As such, it does not reflect the behavior of residents from other countries that are subject to different privacy laws. For example, European populations that live in countries that enforce the General Data Protection Regulation (GDPR) may have different perceptions on privacy policies relative to US-based participants. Similar to other surveys, our data relies on self-reports and remembrance. For instance, some questions required users to recall past experiences such as cyber-attacks and past behavior on reading privacy policies. Therefore, it is possible that users may not remember such past experiences correctly. Finally, our data depends on the willingness of participants to share their perspectives and behaviors towards privacy policies. Although these limitations may affect our data, we believe that our study represents a step forward in understanding the general behaviors and attitudes of people towards reading privacy policies.

IV. PARTICIPANTS

In total, we received responses from 655 participants who completed the survey. After filtering out participants who did not pass the attention-check questions ($n = 94$), only 561 valid responses were used for the analysis. Within this sample, 56.0% identified themselves as male, 42.8% as female, 0.7% as non-binary/third gender, and the remaining not specified. 73.8% of the participants were between the ages of 25 to 44. In addition, 52.6% of the participants had a level of education equivalent to a bachelor's degree or higher. In terms of occupation, our participants had diverse professions. For instance, 100 of our participants were in the computing industry, another 108 participants were in the business/financial industry. We also had 5 participants with backgrounds in legal. Table 1 summarizes the demographic details of our participants, including their education level, occupation, and security expertise.

TABLE 1. Demographic information of the survey participants ($n = 561$).

Gender		
Male	314	56.0%
Female	240	42.8%
No answer	3	1.2%
Age		
18 – 24	35	6.2%
25 – 34	240	42.8%
35 – 44	174	31.0%
45 – 54	71	12.7%
55 – 64	21	3.7%
65 and over	20	3.6%
Education		
Some High School	2	0.4%
High School Graduate	80	14.3%
Some college, no degree	170	19.1%
Associate's or technical degree	77	13.7%
Bachelor's degree	242	43.1%
Graduate degree	53	9.5%
Occupation		
Administrative Support	63	11.2%
Art, Writing, or Journalism	43	7.7%
Business, Management, or Financial	108	19.3%
Education or Science	29	5.2%
Legal	5	0.9%
Medical	24	4.3%
Computer Engineering or IT	100	17.8%
Engineer in other field	13	2.3%
Service	86	15.3%
Skilled Labor	30	5.4%
Unemployed	35	6.2%
Retired	18	3.2%
College Student	4	0.7%
Graduate student	3	0.5%
Security Expertise		
Experienced	113	20.1%
No Experience	448	79.9%

A. PARTICIPANT CHARACTERISTICS

In this section, we discuss the different characteristics of our participants, including their general understanding and behavior towards security and privacy.

Background and Security Knowledge. The first criteria we used for describing our participants relates to their security background. To this end, we presented participants with several questions designed to assess our participants' experience in working with information security, as well as, questions that test their knowledge about general security concepts. We determined that 42% of our participants could not identify what we considered to be strong passwords. Such information allowed us to further classify our participants into three groups: i) Security professionals, with 22% of the survey participants having experience working in the field of information security. ii) Intermediate, this corresponds to the set of participants that have an adequate security knowledge base, but have no direct experience working in the field. This category represents 19% of our participants. iii) The normal user, most users fall into this category. Such participants have some to no background in basic information security concepts like identifying a strong password and correlate to the majority of participants at 61%.

Pro-Activeness Towards Security and Privacy. For this category, we identified proactive users, who actively try to protect their security and strive to maintain their privacy by utilizing various security features, such as two-factor authentication, password managers, and sharing less private data through opt-outs and private browsing. We found that most users could be broadly categorized into the following types; i) The proactive user. This category encompasses the set of users who actively try to protect their privacy by taking action whenever necessary. Such users are inclined to take action even if it costs them giving up the service. ii) The normal user. This category represents the average user who is characterized by accepting some compromises in privacy in return for enjoying online services. Also, these users may care about their privacy, but sometimes don't always know how to protect it. iii) The careless user. This correlates to the user who does not care about what a given service may collect. Such users generally do not let privacy violations by service providers stop them from using a given service.

Online Presence. We studied the online presence and habits of our participants by collecting information about the time they spend online, the types of services they use, and the types of data they share with other users. We also asked them about the privacy settings of their social media accounts if they were private, public, or mixed. We found that users could be classified into i) The ghost. This type of user is characterized by having minimal online presence. In addition, such users are generally not interested in sharing their data or identity while online. ii) The normal user. Unlike the ghost user, normal users have qualities that correspond to the average online consumer. They enjoy common online services. They also indulge into social media in order to communicate with others. iii) The heavy user. This user is marked by having a heavy online presence. They typically encroach onto any service they come across and actively share personal information online on a regular basis.

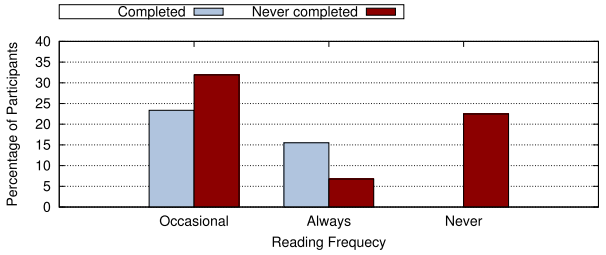


FIGURE 1. The completion degree of reading privacy policies as a function of how frequently users read policies when signing up for new services ($n = 561$).

Overall, we found that 60% of our participants spend 4 to 10 hours online every day. On the other hand, 31% of our participants tended to spend beyond 10 hours being active only. We also found that this group tended to engage in services that span social networking, entertainment, retail, banking, and back up and sync as being the most commonly used. In addition to the time our users spend online and the types of services they used, we asked our participants about their data sharing habits. We found that social media posts, photo sharing, and video sharing of themselves were the most common types of data shared. Disclosing geographical locations, on the other hand, was the least common form of data shared.

V. BEHAVIORS AND PERCEPTIONS

A. READING THE PRIVACY POLICY

Figure 1 summarizes the privacy policy reading habits of our surveyed participants in terms of frequency (occasional, always, and never). We show the set of users who occasionally read privacy policies, those who always read policies, and the participants who never read privacy policies. In addition to the aforementioned frequency information, we provide a breakdown the users based on the degree of completion. In other words, we further divide users based on whether they have completed reading the privacy policies of their services or not. We observe that a total of 435 participants (77%) had a positive attitude towards privacy policies by either reading or having attempted to read a privacy policy at least once. We found that the majority of users tended to occasionally read privacy policies. On the other hand, 23.4% of our participants have fully read the policy at least once, whereas, 31.9% of the participants claimed to have partially read a privacy policy at least once. We observe a slightly different trend for participants who read every privacy policy when signing up for a service (always read privacy policies). We found that 15.5% of the participants completely read privacy policies and a mere 6.7% of the participants exhibited partial reading behavior (read every privacy policy during sign up, but never complete it). Finally, we find that 22.5% of our participants never attempted to read a privacy policy. This corresponds to 126 of the participants who have never tried reading a policy.

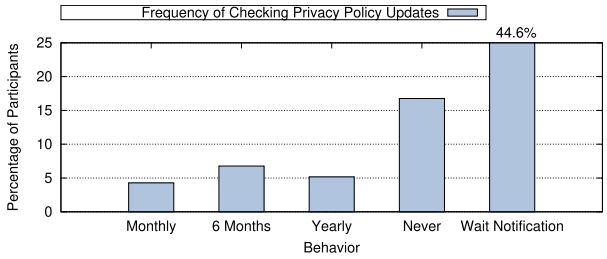


FIGURE 2. The frequency of participants checking for privacy policies updates over time ($n = 435$).

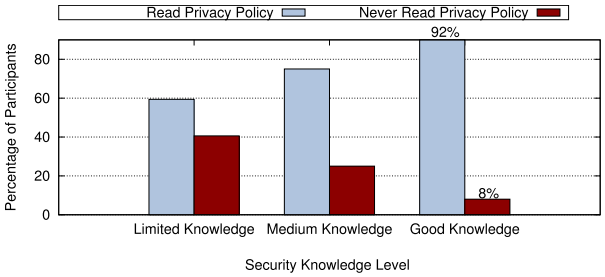


FIGURE 3. Distribution of participants according to security knowledge and the impact of security knowledge on reading privacy policies.

1) READING BEHAVIOR OVER TIME

To better understand the reading habits of our users towards reading privacy policies, we examined the reading behavior of our participants over time by asking them how often do they check for updates made to the privacy policy. In order to gain this insight, we focused on participants who have either read or tried to read any privacy policy ($n = 435$). This information is summarized in Figure 2. On average, we observe an increasing trend over time in terms of how often users check for updates to privacy policies. Overall, we observe that the fraction of participants who voluntarily check for updates is well below 10% even when considering different time periods that range from monthly to yearly. We find that only 5.5% of the participants check for privacy policy updates on a monthly basis. A slightly higher fraction of our participants check for updates made to the privacy policies associated with their services. We find that 8.7% of our users check for updates twice a year. On the other hand, we find that only 6.7% of the participants bother to review any updates on a yearly basis. Our data shows that the vast majority of our participants (44.6%) wait for notifications to be issued by the service providers. The remainder of the surveyed participants simply never check for updates, suggesting that most users who intend to read a given policy never follow through. In addition, our results show that notifying users of privacy policy updates is more effective when providers use multiple methods including email followed by pop-ups while using the service. Issuing multiple reminders to users using different mechanisms is the best way for making sure consumers are informed about updates to the services they use.

2) IMPACT OF SECURITY KNOWLEDGE

We explored the impact of security knowledge on reading behavior amongst our participants. In order to gain this insight, we developed a point system that allowed us to classify users into one of the following categories: limited security knowledge (32 participants), medium security knowledge (416 participants), and good security knowledge (113 participants). This was presented to our participants as a series of questions designed to gauge their familiarity with concepts such as two factor authentication, the competence to distinguish between weak and strong passwords, and the ability to encrypt computer files. The full list of questions that we asked our participants can be found in Table 8 in Appendix C.

Figure 3 summarizes the results of our security knowledge experiment and its impact on the privacy policy behavior. Overall, we observe an upward trend in terms of reading the privacy policy as a function of security knowledge. In other words, the more knowledgeable participants were about security, the more likely they were to read a given privacy policy during service sign up. For instance, amongst the group of participants who had limited security knowledge, 59.4% of them have read a privacy policy either partially or completely. However, amongst the group of participants who had medium knowledge, the fraction of users who read a privacy policy increased to 75%. This percentage increased to 92% for the group that consisted of participants who had good security knowledge. Finally, this data underscores the importance of educating online users on security.

3) INFORMATION SHARING AND READING BEHAVIOR

We analyzed the relationship between our participants sharing their information online and how that compared to the privacy policy reading behavior. Similar to the security knowledge experiment, we created a point system designed to infer the amount of data users share while using online services. This allowed us to classify users into the following categories: limited sharing (190 participants), medium sharing (331 participants), and excessive sharing (40 participants). This was presented to our participants as a series of questions about the types of services our participants use and the type of data they share. The full list of questions that we asked our participants can be found in Table 7 in Appendix C.

Figure 4 summarizes the results of our information sharing experiment and its impact on the privacy policy behavior. Contrary to our expectations, we did not observe an increasing trend where participants who shared more data were more likely to read the privacy policy. Overall, unlike what we observed for security knowledge, our results show that there is little difference across all three categories in terms of reading behavior irrespective of the amount of data shared. For instance, we found that 72.6% of the participants in the limited sharing category read the privacy policy. This trend increased to 80.4% for the medium group. Finally, we observed a slight decrease for the excessive data

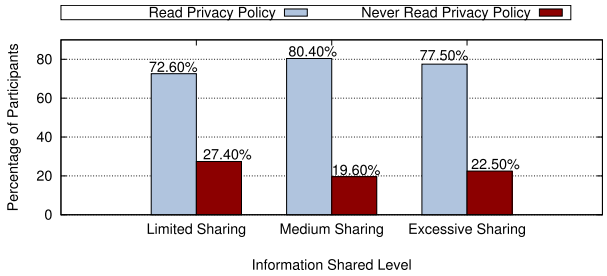


FIGURE 4. Distribution of participants according to online data sharing practices and the impact of such practices on reading privacy policies.

sharing category relative the aforementioned medium group. We found that 77.5% of the participants read the privacy policy. We also note that most of our participants share limited to medium amounts of information online.

4) PRIVACY POLICY CONTENT

Furthermore, we investigated the behavior of our participants with respect to the content they examine within privacy policies. We find that for the group of participants who had experience in reading privacy policies ($n = 435$), highlighted sections and titles were considered to be important. They also mentioned that segments that discussed information usage by third parties, how data is shared, and details related to opt-out were of interest to participants. Our data shows that a relatively small portion of our participants (22.5%) consider information included in the entire privacy policy to be important. About 51% of the surveyed participants focused on segments of the policy that described how data was used by third party vendors. Similarly, users showed interest in reading information related to opt-outs with 43.4% of surveyed participants falling into this category. Users who typically focus on highlighted parts of the privacy policy and the type of information collected represented 48.5% and 49.7% of our users, respectively. For example, one of our participants shared the following in response to our survey: *"I skim it very fast looking for specific keywords."* A breakdown of the content users typically examine when reading privacy policies is summarized in Table 2.

B. USER PERCEPTIONS ON PRIVACY POLICIES

In this study, we examine the perception of our participants with respect to the necessity of online providers furnishing privacy policies for their associated services. We also consider the perception of users on the necessity of reading the provided policies and how helpful they find such content with respect to preserving their privacy. A summary of these findings is shown in Figure 5.

1) NECESSITY OF PRIVACY POLICIES

Overall, we find that the vast majority of our participants feel that service providers must supply privacy policies for their consumers. This correlates to more than 96% of the surveyed participants agreeing to the necessity of providing policies.

TABLE 2. Breakdown of the content users examine when reading a privacy policy.

Information read in privacy policies		
The full privacy policy – everything	93	21.4%
Highlighted sections and titles	211	48.5%
Information the service collects	216	49.7%
Information participants think is important	239	54.9%
New updates and update notices	110	25.3%
Tracking policy	138	31.7%
How information is used by third parties	223	51.3%
Data shared with third party websites	215	49.4%
How to opt-out from data collection	189	43.4%
Random information	36	8.3%
Other	6	1.4%

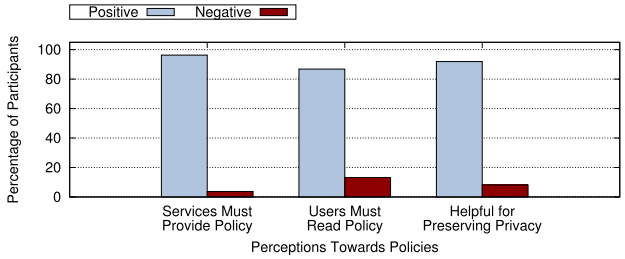


FIGURE 5. The perception of users towards the need for service providers to supply privacy policies and the perceptions on the need for users to read the furnished policies ($n = 561$).

Similarly, we find that 87% of our participants feel that it is necessary for consumers to read privacy policies prior to signing up for a given service. However, a small fraction of our consumers (13%) thought that it was unnecessary to go through such information. As such, they disagreed with the necessity of reading privacy policies. This is likely due to the fact that such users are of the opinion that service providers will utilize their data irrespective of what the policy states. Furthermore, this group of participants is mostly skewed towards users who are not willing to give up the services they use in return for better privacy.

2) USEFULNESS OF PRIVACY POLICIES

We investigated whether participants believed that policies were helpful for them. To answer this question, we posed this question to the fraction of participants who had prior experience in reading privacy policies. Therefore, the findings of this portion of the study are based on a sample of 435 participants ($n = 435$). In general, we find that over 8% of the total number of participants thought that privacy policies were not helpful in preserving some privacy. Further analysis of this data revealed that this figure stems from various negative experiences that our participants encountered while reading privacy policies. For instance, 52% of the participants in this group claimed to have interacted with complex and user unfriendly interfaces that made them lose trust in how the respective service providers would handle their data.

This trend is exacerbated by the amount of time users are willing to dedicate towards reading privacy policy content. We believe that having well organized policies with important information clearly outlined would go a long way in service providers gaining the trust of their consumers and providing them with an easy way to find the information that they need. We believe this would also encourage more consumers to read the privacy policy. For instance, some participants expressed that even having larger text with well-organized links that provide more detail would improve the overall user experience. Examples from our participants include *"Bigger text, better organization, videos, links to different sections of the privacy policy."* and *"I would increase the font size since the font is small a lot of the time. I would make sure topics are bolded and that people can quickly click on links to get to relevant information."*

3) IMPORTANCE OF MEDIUM

In terms of the preferred medium for users reading privacy policies, we found that our participants favored reading web-based policies on standard computer systems over hand-held devices such as smartphones and tablets. For instance, 38.4% of our participants read policies using desktop and laptop systems, whereas only 4.6% of our users opted for hand held devices. Although our participants showed more interest in reviewing policies on standard computer systems, we found that most users (57%) were open to using both kinds of systems (desktops, laptops, smartphones, and tablets). This data also correlates to our participants' perceptions on which policy types are more important for maintaining privacy. We found that the majority of our participants (78.2%) felt that reviewing privacy policies that were geared for both types of systems were important in order to maintain good privacy. On the other hand, 15.4% of our users thought that web-based policies tailored for standard systems (desktops and laptops) were more important, while the remaining 6.4% of our users felt that reviewing the policies of mobile apps that are geared for smartphones and tablets were more important. Given the aforementioned findings, we believe it is important to consider design improvements for privacy policies across both kinds of devices. For example, integrating privacy policies into mobile apps that don't require using an external link that requires a browser would improve the overall user experience and facilitate better navigation for mobile users.

4) OPT-OUT SERVICES

A general knob that users have available for reclaiming some of their privacy lies in the use of opt-out services. In order to infer the perception of users towards opt-out services, we presented our participants with a general definition of what such services mean. Once our surveyed participants read the following definition, *"An opt-out service lets users know that they have the right to opt out of sharing certain private information on a website or application, and also have a clear and easy to follow method for actually opting out."*, we proceeded to analyzing their behavior towards this service. Table 3 includes a breakdown of the various perceptions users had about opt-out services.

TABLE 3. The perception of users towards opt-out services ($n = 561$).

Perception about opt-outs		
Use of any opt-out options	357	63.6%
Necessity of opt-outs in privacy policies	484	86.3%
Knowledge about opt-out information present in privacy policies	363	64.7%
Presence of opt-out options vs. control over privacy	503	89.7%

Overall, we found that 64.7% of our participants had knowledge about the inclusion of opt-outs within privacy policies. On the other hand, the remaining 35.3% of participants had no knowledge about this. In general, we found that 63.6% of our participants used opt-out services. This underscores the fact that a good number of our users care about their privacy. In addition, many users (86.3%) felt that having the ability to opt-out of a given service was a necessary feature that must be available with every service. We also observe that the presence of opt-out services generally had a positive impact on participants using a given service. For instance, 89.7% of our participants felt more in control of their privacy when using services that had opt-out services available. While these findings do show that opt-out services are being leveraged by most users, many users (35.3%) are still unfamiliar with such services. This underscores the necessity of having campaigns that can educate more consumers about the availability of such services.

C. COMPREHENSION OF PRIVACY POLICIES

In this section, we explore the accessibility of privacy policies to our participants in terms of comprehension. For this purpose, we assess the ability of our participants to understand passages from real privacy policies and the different challenges they faced. We found that 89% of the participants who reported having experience with reading privacy policies encountered some difficulty in understanding the content of such policies. For example, although only 18.4% of our participants considered the presented privacy policy to be difficult to understand, 55% of the surveyed users answered incorrectly when asked to interpret what the passage actually meant. The passage from the privacy policy included terms such as IP address, Cookies, Flash Cookies, Operating System, Mouse overs, and JavaScript. Figure 6 summarizes the participants' unfamiliarity with the aforementioned terms. With regards to the degree of difficulty experienced by our users, we observed that 21.9% of the participants mentioned that the policy was easy to read, 59.7% reported the passage being somewhat difficult to read, while the remaining 18.4% declared the passage as being difficult to read. Surprisingly, we observed that participants who had a legal background were least likely to answer correctly in contrast to participants

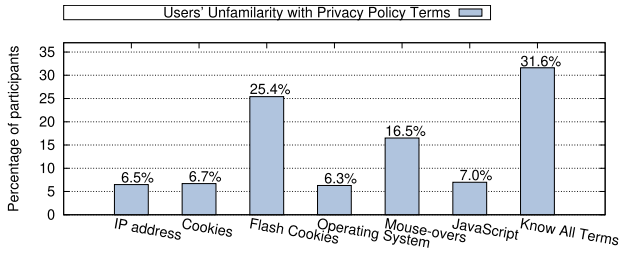


FIGURE 6. Summary of privacy policy terms that participants were unfamiliar with ($n = 561$).

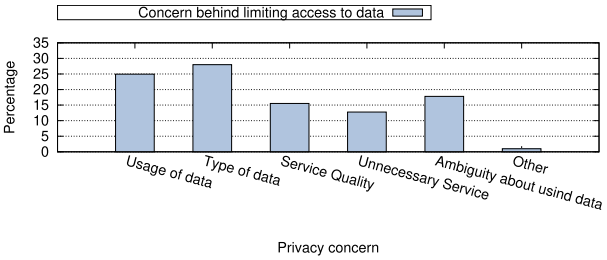


FIGURE 7. Summary of the concerns behind users limiting service provider's access to their data.

with a computer or business background, followed by participants who either administrators and journalists.

In addition, we asked the participants about the terms they were unfamiliar with. We determined that more than 68% of the participants were not familiar with at-least one term. Only 31.6% of the users were familiar with all the terms mentioned. In addition to the aforementioned, we collected various reactions of users to the presented passages. For example, one of the participants felt that privacy policies are designed to be intentionally vague, *"The main issue is the language used in privacy policies. It's often a lot of legal jargon that is intentionally vague."*. Similarly, another participant mentioned *"Sometimes the wording is so broad it is hard to tell what they are actually doing."* Other participants commented on the need for easier to understand policies by sharing comments, such as *"The terms used in the privacy policies text should be more easy to understand and also very brief and concise so people just don't lose interest when seeing those wall of texts."* and *"I would make the information bulleted. I would make the font larger so you are not trying to read such small print. I would use words that are easily understood by the general population"*.

Furthermore, our data consists of five users who are in the legal field. Surprisingly, from this group, only one participant has completely read the privacy policy. Two participants attempted to read, but didn't finish. The other two participants have never read any privacy policy. This shows that even people who work in the legal field are not reading the privacy policy. This underscores that importance of educating users on the need to read the privacy policy. It also highlights the importance of service providers ensuring that their privacy policies are easy to understand in order to not discourage users from reading them.

D. DATA COLLECTION AND USAGE

We evaluated our participants' perspective on the data collection and usage practices associated with service providers. We also asked our participants about the various actions they take as a result of such practices as a way of preserving some of their privacy. Overall, we found that more than 86% of our participants expressed concern about such data collection and usage practices which in turn prompted them to take various steps in order to restrict service providers from accessing their data. A summary of the different concerns that were raised by our participants is shown in Figure 7. For instance, most users (28%) were concerned about the type of data that was being collected by service providers. On the other hand, 24.9% of the participants were concerned with the way the collected data was being used instead. Another concern that users reported which prompted action is related to the ambiguity of how the collected data is consumed by service providers. Approximately 17.8% reported the aforementioned as a concern. Other concerns that prompted action on the participants' behalf, include the quality of the service (15.5%). This is because users felt that limiting the data shared with service providers would not impact the overall service. Other participants (12.8%) felt that the data collected by providers was unnecessary for the kind of service they offered.

In addition to concerns about data collection and usage practice, we captured their reaction to data commonly collected by major service providers such as Google, Amazon, and Facebook. To achieve this, we presented our participants with passages of different privacy policies that we labeled as Google, Amazon, Facebook – Device Signals, and Facebook – Information. The different samples that were used for the aforementioned labels are listed below:

- **Google**: The following passage shows how Google stores information about the user including, the operating system type, mobile network information including carrier name and phone number, IP address, crash reports, system activities, date, time etc. More specifically, users were presented with the following passage: *"The information we collect includes unique identifiers, browser type and settings, device type and settings, operating system, mobile network information including carrier name and phone number, and application version number. We also collect information about the interaction of your apps, browsers, and devices with our services, including IP address, crash reports, system activity, and the date, time, and referrer URL of your request"* [63].
- **Amazon**: The following passage shows how Amazon stores personal information that includes email, passwords, credit card information, social security numbers, driver's license etc. More specifically, users were presented with the following passage: *"**Examples of Information Collected, Information You Give Us:** You provide most such information when you search, buy,*

post, participate in a contest or questionnaire, or communicate with customer service. For example, you provide information when you search for a product: place an order through Amazon.com or one of our third-party sellers; provide information in Your Account (and you might have more than one if you have used more than one e-mail address when shopping with us) or you profile; communicate with us by phone, e-mail, or otherwise; complete a questionnaire or a contest entry form; use our service such as Amazon Instant Video; compile Wish List or other gist registries; participate in discussion Boards or other community features; provide and rate Reviews; and employ Product Availability Alerts, such as Available to Order Notifications. As a result of those actions, you might supply us with such information as your name. address and phone number; credit card information; people to whom purchases have been shipped, including addresses and phone number; people (with addresses and phone numbers) listed in 1-Click settings; e-mail addresses of your friends and other people; content of reviews and e-mails to us; personal description and photograph in Your Profile; and financial information, including ***Social Security*** *and driver's license number"* [64].

- **Facebook – Signals**: The following passage illustrates how Facebook examines the signals surrounding the device to infer additional information about their users and the various systems they possess. This policy spans multiple services that Facebook offers including Instagram and WhatsApp. Our participants were presented with the following passage: *"**Device signals**: Bluetooth signals, information about nearby Wi-Fi access points, beacons and mobile phone masts"* [65].
- **Facebook – Information**: Similar to Facebook's policy on signals, the following reflects Facebook's approach to collecting user information spanning services that include Facebook, Instagram, and WhatsApp. Their policy states that even in cases when your account, information about the user will still be retained. For example, if you delete your account, Facebook will claim that it will retain your conversation history because such conversations involve other users who did not delete their accounts. The following is a sample of what Facebook shares with its users: [65] *"**Things others do and information they provide about you**. We also receive and analyse content, communications and information that other people provide when they use our Products. This can include information about you, such as when others share or comment on a photo of you, send a message to you or upload, sync or import your contact information"* [65].

Figure 8 summarizes the perception of our participants towards the data collection of major service providers, such as Google, Amazon, and Facebook. Overall, we found our participants to be aware of data collection practices instituted by service providers or at least have heard about such

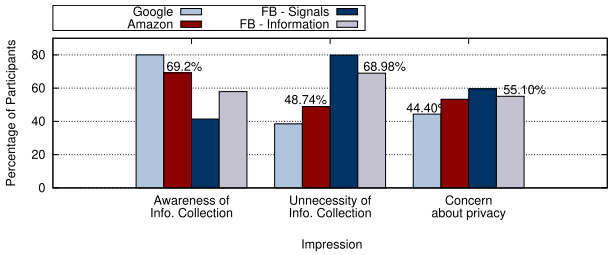


FIGURE 8. **The perception of users towards the data collection practices of major service providers.**

behavior. For instance, more than 80% of our participants were familiar with information, such as system activities, carrier names, and phone number information being collected, as practiced by Google. Similarly, the majority of our participants, although slightly less than before seemed to be familiar with information, such as names, credit card numbers, social security numbers, and driver's licence information, as collected by Amazon. For instance, 69.2% of our participants reported to be familiar with the aforementioned type of data being collected. On the other hand, participants were less familiar with the type of information Facebook collected. For instance, only 57.9% of our participants acknowledged being acquainted with information, such as conversation histories being retained even after account deletion as previously outlined in the "Facebook – Information" passage. The number of participants who claimed to be familiar with signal data being collected ("Facebook – Signals") dropped to 41.4%.

In addition, our participants shared their perspective on the necessity of providers to collect the aforementioned data. Overall, we found that participants seemed to be more understanding of why data, such as that collected by Google and Amazon. On the other hand, the participants felt differently about the type of data collected by Facebook. We observed that the majority of the users were under the impression that collecting such data was unnecessary. More specifically, only 38% of our participants felt that data collected by Google was unjustified. However, this trend worsened for the type of data collected by the other service providers with the collection of signal information being the least popular. We found that 53.3%, 69%, and 79.9% of our participants felt that data collected by Amazon, Facebook – Information, and Facebook – Signals, respectively, was unnecessary.

We also examined the concerns our participants shared regarding such practices. Overall, we found that our participants were the least concerned with the type of information collected by Google. On the other hand, our participants were the most concerned with the type of data Facebook collected from its users (Facebook – signals and Facebook – Information). More specifically, 44.4%, 53.3%, 55.1%, and 59.9% of our participants were concerned with the type of data collected by Google, Amazon, Facebook – Information, and Facebook – Signals, respectively. In general, different users had concerns over specific types of data. For instance, some

participants expressed concern over personal information, such as photos and contacts being collected as stated here: *"I think snapchat's policy does or used to say that they have the rights to any photos taken through the app, that they store them and can use them how they want. It is overly difficult to actually delete your account fully."* and *"I've heard about people using apps that have access to the user's photos, that state they can use their photos in their business however they wish. This is very concerning. It's also concerning to me how some apps seem to require access to my photos and contacts, and seemingly don't need access to them."* Other participants were more concerned over signal information as expressed by this participant, *"I think network information including mobile carriers and wifi access points, all details like that is uniquely disturbing. I feel they could map out people's lives with that kind information in a degree of detail that is disturbing."* The main concern that participants had over signal information relates to the ability of service providers to map out the geographical location of their consumers. On the other hand, a number of our participants were concerned about their data lingering in the cloud even after account deletion, as stated by these participants, *"I find it odd that my info is saved even after I delete it."* and *"I wonder if Facebook really deletes the information, or just hides it?"* Finally, the aforementioned concerns emphasize the necessity of having opt-outs which can allay some of these worries.

VI. POINTS OF INFLUENCE

In this section, we discuss different points of influence that can either motivate or discourage users from reading privacy policies. We also consider other contributing factors, such as the service type, privacy policy content, design, in addition to perceptions and attitudes, and how these can influence online users.

A. MOTIVATORS FOR READING PRIVACY POLICIES

Our results show that different users are motivated by different reasons when it comes to reading privacy policies. We determined that our participants were influenced by characteristics that correlated to the following main categories: the service, the privacy policy itself, and the type of user. Table 4 lists the different characteristics associated with each category and a breakdown of our surveyed population and how they were motivated by such factors. Overall, we observed that users were influenced mostly by characteristics that belong to the service category. For instance, our participants felt that characteristics such as the credibility of the service (51.3%), the type of data collected (45.6%), and the amount of data collected (42.1%), prompted users to read privacy policies. Although, some of these factors, as previously reported, tended to raise concerns amongst our participants, it drew them more towards reading online privacy policies. For instance, 51.3% of our participants were driven to read the privacy policy whenever a service was considered to be suspicious. On the other hand, we found that the popularity of the service had significantly less impact on users reading privacy policies. For instance, only 11.1% of our participants were motivated by the popularity of services.

TABLE 4. Summary of what motivates users to read the privacy policy ($n = 541$).

Service		
Service Credibility	101	51.3%
Service Type	96	48.8%
Type of data collected by service	90	45.6%
Amount of data collected by service	83	42.1%
Service Popularity	22	11.1%
Privacy Policy		
Readability	51	9.1%
Location on web page	29	5.2%
Interface design	19	3.4%
User		
User habits	27	4.9%
Recommendations	23	4.1%

In addition, we found that characteristics related to the privacy policy played a role in motivating users. More than 17.6% of our participants acknowledged that characteristics that are associated with the privacy policy itself had some influence on their reading behavior. We observed that the readability of the policy had the most impact with 9.1% of the participants falling into this category. Fewer participants (5.2%) shared that the ease of finding the privacy policy was a driver for reading the privacy policy. Only 3.4% of our participants, on the other hand, felt that user friendliness had an impact on them reading privacy policies. We also found that other factors such as the amount of time the user spends using a given service and recommendations made by other users had some influence on participants reading privacy policies. For example, 4.9% of our participants were motivated to read the privacy policies of services they used more often (listed as "User habits" in Table 4). Similarly, 4.1% of our participants felt motivated to read a given privacy policy if someone recommended it based on a previous experience.

We also analyzed the participants' behavior and motivation towards reading privacy policies after becoming a victim of a cyber-attack. In our study, 32.4% of our participants were victims of a previous cyber-attack. After analyzing the responses of these participants we determined that 42.3% of the affected participants started to read privacy policies more often. Furthermore, we found that these participants took additional steps beyond just reading privacy policies. We observed a 62% increase in the number of participants who changed their default account settings in response to a cyber-attack. Furthermore, more than 57% of the affected participants changed their perspective towards privacy policies after becoming a victim of a cyber-attack. A summary of the impact of cyber-attacks on our participants is shown in Table 5.

Furthermore, we analyzed our participants responses to determine if there was any change in their privacy policy reading behavior over the past five years. We found that

TABLE 5. Cyber-attacks and their impact on users being more privacy aware ($n = 182$).

Impact of cybersecurity attacks		
Change in perspective or behavior towards privacy policies after a cyber attack	104	57.1%
Explicitly changed default settings for services **before** the attack	82	45.1%
Explicitly changed default settings for services **after** the attack	133	73.1%
Increase in reading privacy policies after the attack	77	42.3%

40.3% of our participants are now reading privacy policies more frequently compared to compared to five years ago. In addition to being a victim of a cybersecurity attack, participants listed the following reasons for reading privacy policies more: increased use of technology, concern about data misuse, hearing about security breaches and information leakage, becoming more security aware through work and/or college, and advised by others.

B. BLOCKERS FOR READING PRIVACY POLICIES

We examined factors that were considered to be deterrents for reading privacy policies. In general, we found that the majority of our participants did not trust service providers having access to their data. More than 94% of our users felt that sharing personal data with service providers would negatively impact their privacy. Furthermore, we found that for participants who have attempted reading privacy policies in the past, readability was the main barrier. As previously discussed in section V-C, privacy policies often use terms that are unfamiliar to the average user, in addition to passages that are written to be vague. The aforementioned factors accounted for 30.5% of our participants. For example, one of the participants mentioned *"less text.. less legalize. less tech (I understand it, but many don't)."* Furthermore, 34.4% of our participants felt that the length of privacy policies discouraged users from reading them. Most users are not willing to dedicate time towards reading long polices that are difficult to comprehend. Finally, 17.8% percent of our participants felt that the content of such policies in addition to being long, was also boring. This underscores the need for service providers to present privacy policies that are more engaging such as using comics and videos.

In the case of participants who have never read a privacy policy, we found that their reluctance primarily stemmed from the perception of helplessness and lack of control over their data. Such users often had the perception that reading the privacy policy was unnecessary because they had no say on how their data would be consumed if they wanted to use a given service. For example, one participant stated that *"Companies will just do what they want anyways."* Other participants felt that offering their data in return for using a given service took an all or nothing approach. For example, one of the participants mentioned the following: "*If you disagree you're barred from the website.*" Similarly, another participant expressed the following: "*I either accept, or do not use the site, so it doesn't matter.*" Finally, we had some participants who had a preconceived perception that privacy policies were difficult to read. Among these participants was a participant in the legal profession. This participant shared that such documents tend to be difficult to understand which is why they don't read. Even though the participant had a background in law, they stated the following: *"I know it's difficult to read and understand the content, so I haven't read it."*

We also analyzed our participants responses to determine if there was any change in their privacy policy reading behavior over the past five years. While the majority of our participants (51.7%) reported that their reading behavior has not changed over the past five years, we found that 8% of our participants are now reading privacy policies less frequently. Most of the participants who started to read privacy policies less often started doing so as a result of the following main reasons: the need to use the service anyway, lack of control over the consumed data, and the fact that most people within their circles use the same services. A relatively small fraction of this group of participants mentioned other reasons, such as not caring about privacy and that the collection of personal information by providers is not harmful.

VII. USABILITY AND DESIGN IMPLICATIONS

In this section, we explore the usability of different privacy policy interfaces and their impact on consumers reading privacy policies. We focused on interfaces that are used by known service providers such as Zillow, Uber, Amazon, Facebook, and Google. We considered interfaces that ranged from the most basic interface to interfaces that involved the use of videos. A summary of the interfaces we used in this study along with their descriptions are shown in Table 6. Furthermore, a visual sample of the different interfaces can be found in Appendix A.

Overall, the majority of our participants (49%) found that "Interface 4" which belonged to Facebook, to be the most user friendly. Users found having a side bar that listed the different sections of the privacy policy coupled with a high level overview of the company's policy on the given section, easy to use. The overview was designed to include links to more detail through links. Therefore, users who wanted to delve into more detail could do so by clicking on the embedded links that would in turn take them to appropriate pages. We found that although only 21.4% of our participants have seen or used this interface before, more than 47% of our participants were willing to read privacy policies using this interface.

Another interface that had some acceptance amongst our users was "Interface 5." We found that 24.8% of our participants thought that "Interface 5" was user friendly. We also observed that even though only 15.3% participants have either seen or used this interface, more participants (21.4%) were willing to read privacy policies through this interface.

TABLE 6. A summary of the interfaces shared with the participants in order to collect their opinions on user friendliness and the likelihood of each interface in convincing the participants in reading privacy policies.

Interface	Description	User Friendliness	Willingness to read	Seen/read before
Interface 1 [66]	Basic design with headings	2.7%	3.6%	31.1%
Interface 2 [67]	Design with tabs and summaries	10.3%	13.0%	16.7%
Interface 3 [64]	Design with links to more information	13.2%	14.6%	24.8%
Interface 4 [68]	Design with headings in sidebar	49%	47.4%	21.4%
Interface 5 [63]	Sidebar design with video description	24.8%	21.4%	15.3%

Similar to ''Interface 4'', ''Interface 5'' used a side bar for listing the different sections of the privacy policy. However, one key difference is that ''Interface 5'' used a video to describe the content to the user. Despite the overall friendliness of the approach, we found that users generally preferred interfaces that rely on a textual approach that readily included all of the important information. However, some users felt that having videos that describe complicated parts of the policy would be useful. For instance, one of the participants stated, *"1. Organized in clickable Left side list menu. 2. Have some graphic videos in case of complex explanation. 3. Detail orientated and has sub-menus. 4. Easy to understand 5. No loophole Word or Sentences."* Overall, most users were content with interfaces 4 and 5 as stated by the following participant, *"I would make it more user friendly by making the UI more interactive and more "friendly" looking, just like Interfaces 4 and 5."* Moreover, we found that some participants suggested improvements that included having a webpage for Frequently Asked Questions as stated by this participant *"Interface* 4 *is user friendly. The addition of "Your privacy controls" in interface 5 is useful. I want a FAQ's page, where users can find pertinent questions and answers."*. Furthermore, some recommended having a chat section on privacy policy pages for getting questions answered. Although service providers may not be inclined to dedicate service agents for this purpose, we believe the rapid advances in the field of natural language processing within the recent years may make this a reality in the near future.

Moreover, we found ''Interface 3'' and ''Interface 2'' to be less popular amongst our participants. Only 13.2% and 10.3% of participants found ''Interface 3'' and ''Interface 2'', respectively, to be user friendly. In the case of ''Interface 3,'' although 24.8% of our participants have either seen or used this interface before, less participants (14.6%) were willing to consider it for reading privacy policies. As for ''Interface 2,'' although more users were willing to consider this interface for reading policies, this increase was less than 3%. Finally, our participants found ''Interface 1'' to be the least appealing for reading privacy policies. Although more than 31% of our participants reported either seeing or having used such interfaces, only 3.6% were willing to consider reading privacy policies using this interface. As such, it is not recommended for service providers to rely on monolithic documents for conveying important information that relates to privacy.

Finally, in addition to interfaces for reading privacy policies interfaces, we conducted an experiment where we presented our participants with two styles for consenting providers to use consumer data. On one hand, we presented our participants with an interface that uses an explicit checkbox for consenting to having read the privacy policy and accepting the terms. The other interface simply used the statement "*By clicking Sign Up, you agree to our terms, Data Policy and Cookies Policy.*" next to the ''Submit'' button. We found that the majority of our participants preferred using the first interface that required users to explicitly give their consent. Over 80% of our participants favored the approach of explicitly accepting the service provider's terms and consenting them to using their data.

A. LOCATING PRIVACY POLICIES

In addition to exploring the user friendliness of different privacy policy interfaces, we investigated our participants' preference for locating the privacy policy of service providers across standard websites and mobile apps.

Standard Websites. In terms of websites that are often viewed using standard computer systems such as laptops and desktops, our participants emphasized the importance of making the link to the provider's privacy policy visible to consumers. Overall, the majority of our participants expressed interest in having a link to the privacy policy placed depending on the type of the page being served to the user and the kind of information being collected. For instance, 74% of our participants indicated their preference for having a link to the privacy policy always available at the bottom of every page (footer of the page) as stated by this participant, *"My preference is always visible at the bottom of every page."* In addition, a large number of our participants (85.7%) indicated their preference to having a link to the privacy policy displayed on checkout pages that are associated with online shopping, especially when payment information is being exchanged. Furthermore, 67.7% of our participants leaned towards having a banner or a prominently placed link on pages that consume private data. For example, one of our participants mentioned *"I like it to be placed prominently (such as in the main navigation) on sites that handle sensitive information."*

Mobile Applications. In the case of mobile applications, we found that our participants preferred having the ability to

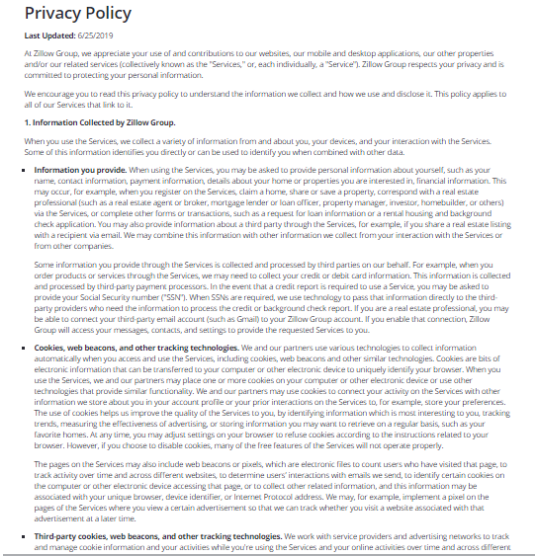
locate the privacy policy on stores where the corresponding app could be downloaded. More than 91% of our participants preferred the option of including links to the privacy policy on the App/Play store itself. For example, one of our participants confirmed the aforementioned preference by saying *"On the Google Play store page would be best."* Another participant mentioned *"I think when downloading an app there should be a privacy policy more front and center and visible."* Furthermore, we found that 84.3% of our participants preferred being able to get to the service provider's privacy policy through different mechanisms that are integrated within the app. For instance, this participant mentioned, *"I prefer to have the privacy policy in the settings where I know I can find it."* Finally, similar to the case of standard websites, more than 78% of our participants preferred having pop ups and sign in requests with pertinent information related to the privacy policy whenever private data is being consumed.

VIII. CONCLUSION

In this work, we examine the user attitudes and perceptions towards privacy policies. We achieve this by conducting a large scale survey consisting of 655 participants. We consider various factors that serve as motivators and blockers. Our study shows that 77% of our participants reported having some experience in reading privacy policies with the vast majority of the participants indicating that concerns about the service provider is the main reason behind users attempting to read such policies. We also determined that only 12% felt that it was unnecessary to have privacy policies in the first place. We also present participants with various privacy policies from popular websites and capture their reactions towards the sensitive data such service providers collect. Furthermore, we assess the participants' comprehension levels of privacy policies and the impact technical jargon has on the readability of such policies. Our study shows that comprehension presented a major handicap in reading privacy policies. We found that although a mere 18% of our participants reported having some difficulty in understanding the privacy policy of popular websites, well over 50% did not understand the actual content. Finally, we discuss the implication of using different interfaces for conveying privacy policy content and out-opt information. We found that over 75% of our users felt negatively about the way privacy policies were designed and the content they embodied with users citing the aforementioned concerns as a serious source of apathy towards reading privacy policies.

APPENDIX A
INTERFACES

See Figures 9–13.


Privacy Policy

Last Updated: 6/25/2019

At Zillow Group, we appreciate your use of and contributions to our websites, our mobile and desktop applications, our other properties and/or our related services (collectively known as the "Services," or, each individually, a "Service"). Zillow Group respects your privacy and is committed to protecting your personal information.

We encourage you to read this privacy policy to understand the information we collect and how we use and disclose it. This policy applies to all of our Services that link to it.

1. Information Collected by Zillow Group.

When you use the Services, we collect a variety of information from and about you, your devices, and your interaction with the Services. Some of this information identifies you directly or can be used to identify you when combined with other data.

- **Information you provide.** When using the Services, you may be asked to provide personal information about yourself, such as your name, contact information, payment information, details about your home or properties you are interested in, financial information. This may occur, for example, when you register on the Services, claim a home, share or save a property, correspond with a real estate professional (such as a real estate agent or broker, mortgage lender or loan officer, property manager, investor, homebuilder, or others) via the Services, or complete other forms or transactions, such as a request for loan information or a rental housing and background check application. You may also provide information about a third party through the Services, for example, if you share a real estate listing with a recipient via email. We may combine this information with other information we collect from your interaction with the Services or from other companies.

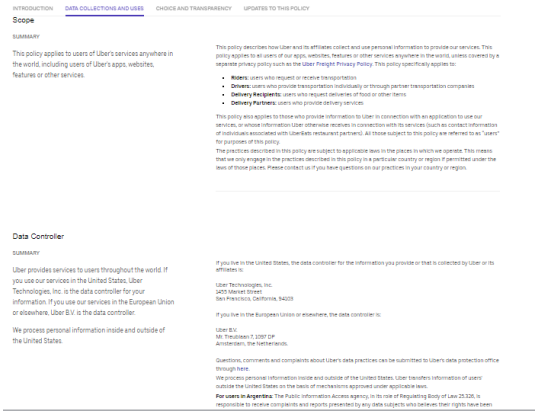
  Some information you provide through the Services is collected and processed by third parties on our behalf. For example, when you order products or services through the Services, we may need to collect your credit or debit card information. This information is collected and processed by third-party payment processors. In the event that a credit report is required to use a Service, you may be asked to provide your Social Security number ("SSN"). When SSNs are required, we use technology to pass that information directly to the third-party providers who need the information to process the credit or background check report. If you are a real estate professional, you may be able to connect your third-party email account (such as Gmail) to your Zillow Group account. If you enable that connection, Zillow Group will access your messages, contacts, and settings to provide the requested Services to you.

- **Cookies, web beacons, and other tracking technologies.** We and our partners use various technologies to collect information automatically when you access and use the Services, including cookies, web beacons and other similar technologies. Cookies are bits of electronic information that can be transferred to your computer or other electronic device to uniquely identify your browser. When you use the Services, we and our partners may place one or more cookies on your computer or other electronic device or use other technologies that provide similar functionality. We and our partners may use cookies to connect your activity on the Services with other information we store about you in your account profile or your prior interactions on the Services to, for example, store your preferences. The use of cookies helps us improve the quality of the Services to you, by identifying information which is most interesting to you, tracking trends, measuring the effectiveness of advertising, or storing information you may want to retrieve on a regular basis, such as your favorite homes. At any time, you may adjust settings on your browser to refuse cookies according to the instructions related to your browser. However, if you choose to disable cookies, many of the free features of the Services will not operate properly.

  The pages on the Services may also include web beacons or pixels, which are electronic files to count users who have visited that page, to track activity over time and across different websites, to determine users' interactions with emails we send, to identify certain cookies on the computer or other electronic device accessing that page, or to collect other related information, and this information may be associated with your unique browser, device identifier, or Internet Protocol address. We may, for example, implement a pixel on the pages of the Services where you view a certain advertisement so that we can track whether you visit a website associated with that advertisement at a later time.

- **Third-party cookies, web beacons, and other tracking technologies.** We work with service providers and advertising networks to track and manage cookie information and your activities while you're using the Services and your online activities over time and across different

FIGURE 9. **Interface 1: Basic design with headings. The privacy policy only has headings, subheadings, and matter within [66].**


INTRODUCTION | DATA COLLECTIONS AND USES | CHOICE AND TRANSPARENCY | UPDATES TO THIS POLICY

Scope

SUMMARY

This policy applies to users of Uber's services anywhere in the world, including users of Uber's apps, websites, features or other services.

This policy describes how Uber and its affiliates collect and use personal information to provide our services. This policy applies to all users of our apps, websites, features or other services anywhere in the world, unless covered by a separate privacy policy such as the Uber Freight Privacy Policy. This policy specifically applies to:

- **Riders:** users who request or receive transportation
- **Drivers:** users who provide transportation individually or through partner transportation companies
- **Delivery Recipients:** users who request deliveries of food or other items
- **Delivery Partners:** users who provide delivery services

This policy also applies to those who provide information to Uber in connection with an application to use our services, or whose information Uber otherwise receives in connection with its services (such as contact information of individuals associated with Uber Eats restaurant partners). All those subject to this policy are referred to as "users" for purposes of this policy.

The practices described in this policy are subject to applicable laws in the places in which we operate. This means that we only engage in the practices described in this policy in a particular country or region if permitted under the laws of those places. Please contact us if you have questions on our practices in your country or region.

Data Controller

SUMMARY

Uber provides services to users throughout the world. If you use our services in the United States, Uber Technologies, Inc. is the data controller for your information. If you use our services in the European Union or elsewhere, Uber B.V. is the data controller.

We process personal information inside and outside of the United States.

If you live in the United States, the data controller for the information you provide or that is collected by Uber or its affiliates is:

Uber Technologies, Inc.
1455 Market Street
San Francisco, California, 94103

If you live in the European Union or elsewhere, the data controller is:

Uber B.V.
Mr. Treublaan 7, 1097 DP
Amsterdam, the Netherlands

Questions, comments and complaints about Uber's data practices can be submitted to Uber's data protection office through here.

We process personal information inside and outside of the United States. Uber transfers information of users' outside the United States on the basis of mechanisms approved under applicable laws.

For users in Argentina: The Public Information Access agency, in its role of Regulating Body of Law 25.326, is responsible to receive complaints and reports presented by any data subjects who believes their rights have been

FIGURE 10. **Interface 2: Design with tabs and summaries. The privacy policy has different tabs for different headings. Each subheading in a given heading contains a summary [67].**

APPENDIX B
SURVEY QUESTIONS

Tell us about yourself.

1- How old are you?

2- What is your gender?

3- What is the highest level of education you have completed?

4- Which of the following best describes your primary occupation?

5- Do you have any experience working in the field of cybersecurity?

Time spent online

6- On an average, how many hours do you spend online per day?

7- What online services do you use?

Behavior and understanding of cybersecurity.

General security behavior:

8- Do you use antivirus on any of your devices?

9- Which of these passwords do you prefer to use?

10- What is meant by the lock symbol next to google.com in the figure below?

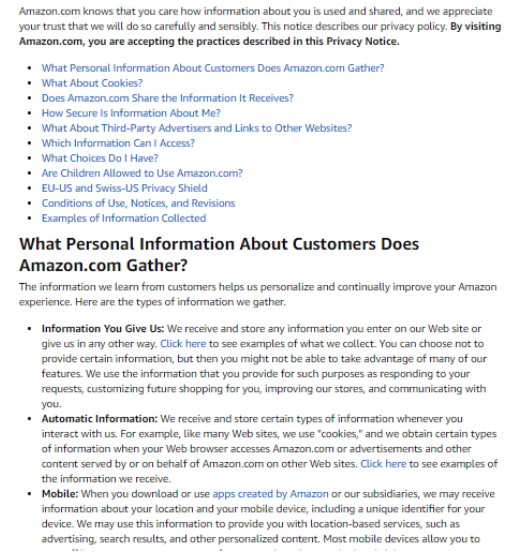


FIGURE 11. **Interface 3: Design with links to more information. Each heading is listed at the beginning of the privacy policy. Clicking on a given heading forwards the user to the relevant content. The content may also have links to other relevant pages [64].**

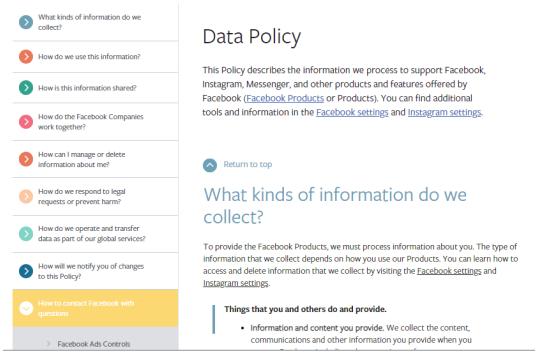


FIGURE 12. **Interface 4: Design with headings in sidebar. Each heading is listed in a side bar. Clicking on a given heading presents the user with the relevant part of the privacy policy. The content may also have links relevant pages that contain more detail [65].**

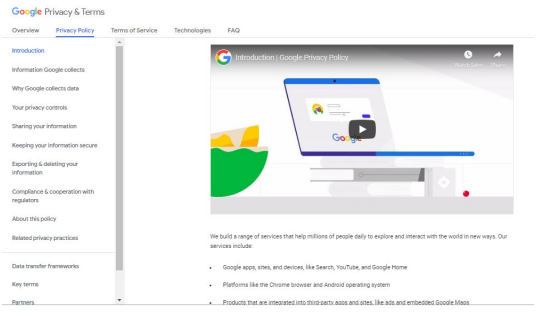


FIGURE 13. **Interface 5: Sidebar design with video description. Each heading in privacy policy is listed in the sidebar that has a video that describes the relevant content. Links are also included with the video that can forward the user to other parts of the policy [63].**

11- Do you use Two-Factor Authentication (2FA) for any online services?

12- Do you use a Password-Manager?

13- Have you ever personally encrypted any of your files to defend against malicious people?

Behavior towards social networks.

14- What is the privacy setting for most of your social media accounts?

15- Have you ever changed the default privacy settings on any of your accounts?

16- What kind of information do you share on social media with other people?

Behavior towards online privacy policies.

17- Do you think it is necessary for online services provide privacy policies?

18- Do you think reading privacy policies is necessary?

29- Would you be willing to read a privacy policy if you had the option to selectively decline parts of it that you do not agree with?

20- Have you ever read or tried to read any website's or application's privacy policy?

If I have never read or tried to read privacy policy is chosen: Go to **Block 1**

If I have read or tried to read the privacy policy is chosen: Go to **Block 2**

BLOCK 1

21- What prevents you from reading the privacy policy?

22- The only way to obtain a service is to consent to the complete privacy policy, Does that discourage you from reading it?

BLOCK 2

****NOTE HERE: Question 23 is asked if the users have tried reading the privacy policy but have not finished reading.**

23- Why haven't you finished reading a privacy policy?

24- Do you try to read the privacy policy for every website you sign up with?

25- How often do you check for updates in the privacy policy after you have signed up?

26- In general, which of the following motivates you to read the privacy policy?

27- What do you usually read in the privacy policy?

28- Do you think reading the privacy policy is helpful?

29- Do you think privacy policies are hard to understand?

30- If the only way to obtain a service is to consent to the complete privacy policy. Does that discourage you from reading it?

31- Have you ever changed the default permission settings a service provider has over your data after reading its privacy policy?

32- If Yes (You changed the default permissions a service provider is granted over your data after reading the privacy policy), then Why?

Privacy policies on websites (desktop/laptop) and phone applications (smart phone/tablet).

33- Where have you tried reading the privacy policy?

34- Which one is important in order to maintain your privacy?

****NOTE HERE: From question 33, If privacy policy through websites (Desktop/laptop) is chosen: Go to Block 3**

If privacy policy from mobile applications (Smart phone/tablet) is chosen: Go to Block 4

If privacy policies on websites (Desktop/laptop) and phone applications (Smart phone/tablet) is chosen: Go to Block 5

BLOCK 3

35- Why do you only read the privacy policy on Desktop/laptop?

36- Did you know that mobile applications have privacy policy?

37- If yes (If you know that mobile applications have privacy policy), Why haven't you read the privacy policy on mobile application?

BLOCK 4

38- Why do you only read the privacy policy on mobile applications (Smart phone/tablet)?

39- Do you know that privacy policy also exists for web-based applications (Desktop/laptop)?

40- If yes (If you know that privacy policy also exists for web-based applications (Desktop/laptop)), why haven't you tried reading the privacy policy on any web-based applications (Desktop/laptop)?

BLOCK 5

41- Which privacy policy is easier to find?

42- Which interface do you think is better?

43- Which privacy policy do you prefer to read the most?

Common question for all - An opt-out service lets users know that they have the right to opt out of sharing certain private information on a website or application, and also have a clear and easy to follow method for actually opting out.

44- Have you ever used any opt-out options?

45- Do you think opt-outs are necessary for the privacy policy?

46- Do you know that opt-out information is present in the privacy policy?

47- If yes (You know that opt-out information is present in the privacy policy), what kind of opt-outs have you used?

48- Does the presence of opt-out options make you feel more comfortable and in control of your privacy?

BEHAVIOR WITHIN PAST 5 YEARS

49- In the last 5 years how has your perception of reading privacy policy changed?

50- If you read privacy policies more frequently now than you have in the last five years, then why?

51- If you read privacy policies less frequently now than you have in the last five years, then why?

CYBERSECURITY ATTACKS

52- Were you ever a victim of a cybersecurity attack (e.g., identity theft, stolen credentials, malware)?

****NOTE: If question 52 answer is no: Go to Readability block**

Since you answered "yes" to the above question (You were a victim of a cybersecurity attack), please share us with more details.

53- What kind of cybersecurity attack was it?

54- Did this experience affect your perspective and/or behavior towards privacy policies?

55- Did you try reading the privacy policy after the attack?

56- Did you explicitly change any of your default settings for the services **before** this attack?

57- Did you explicitly change any of your default settings for the services **after** this attack?

READABILITY

58- What is the difficulty level of this paragraph based on your own perception?

59- Which of the below terms were you not familiar with before reading this paragraph?

60- Based on your understanding of the provided paragraph, why do service providers collect information like cookies, Flash cookies, session information, including page response times, download errors, length of visits to certain pages, page interaction information?

PERSPECTIVE

61- If you are using any applications by Google, do you know that google stores information such as, operating system, mobile network information including carrier name and phone number, IP address, crash reports, system activities, date, time etc.?

62- Do you think google collecting information such as operating system, mobile network information including carrier name and phone number, IP address, crash reports, system activities, date and time is necessary?

63- Are you concerned about your privacy now?

64- If you are using the amazon application, do you know that amazon stores all of your provided information like, email, password, credit card information, social security number (SSN) and driver's license?

65- Do you think collecting the above information (Email, password, credit card information, **SSN**, driver's license) by amazon is necessary?

66- Are you concerned about your privacy now?

67- Do you know that Facebook, Instagram and WhatsApp tracks your device's signals to collect information about other devices surrounding you?

68- Do you think collecting your device's signal information to determine other devices near you is necessary?

69- Are you concerned about your privacy now?

70- Do you know that if you use Facebook, Instagram, or WhatsApp and decide to delete your account, some information will still be saved. For instance, when you delete your account all the information about you including conversations you had with others will be deleted. However, another person who didn't delete their account and has a conversation history with you implies that you didn't delete all of your information from your account, as indicated by the passage below?

71- Do you think service providers retaining your information through other users is necessary even after you have deleted your account? 72- Are you concerned about your privacy now?

73- Have you found any other questionable details in the privacy policy? Please mention it.

PRIVACY POLICY LINK PLACEMENT

74- Do you think the location where the link to the privacy policy is placed on a website or mobile app has an effect on you reading the policy?

WEBSITES

75- From the figures below, Which sign up page will motivate you to read the privacy policy?

76- Do you want the privacy policy link to be placed as a footer at the bottom of every page in a given website?

77- Do you want the privacy policy link to be placed on checkout pages for online shopping where personal data including payment information is shared?

78- Do you want to have a banner or a pop-up page that shows the privacy policy when any of my information has been used?

79- Apart from the above, where do you prefer to have the privacy policy link.

MOBILE APPLICATIONS

80- Do you want to have the privacy policy of all applications in the app/google play store available before downloading it?

81- Do you want to have the privacy policy in multiple places within the application such as settings, about us, or any other menu?

82- Do you want to have the privacy policy link on check out pages, pop-ups, sign in and sign up pages?

83- Apart from the above, where do you prefer to have the privacy policy.

DESIGN

84- Do you think the design of a privacy policy interface impacts your willingness to read it?

85- Which interface from the above do you think is more user friendly?

86- Which interface from the above are you willing to read?

87- Which interfaces from the above have you seen or read before?

88- Has your previous experience with a low-quality privacy policy interface in recent years prevented you from reading privacy policies?

89- How would you improve the interface of privacy policies in order to make it more user friendly? (Optional)

SERVICE QUALITY VS PRIVACY

90- Do you think the amount of private information collected by service providers is justified?

91- If No (the amount of private information collected by the service providers is not justified), what have you done to protect your privacy?

92- If a service is tracking your full online behaviour, but in return gives you more personalized services based on your search history, location, and interests, would you be willing to give up this personalized experience to gain more privacy?

93- Have you ever used Private Browsing mode (Incognito for google chrome, private window for Firefox or Safari, Browsing InPrivate for edge)?

94- Are you willing to give up custom search results on google maps by using anonymous search to have more privacy?

TABLE 7. Distribution of the point system established to analyze the relationship between information sharing and reading privacy policies.

Question	Points
On an average, how many hours do you spend online per day?	
Less than 4 hours	1
4 hours to 10 hours	2
More than 10 hours	3
What online services do you use? (Select all that apply)	
Social networking, Communication, email (e.g., Facebook, Gmail, Instagram, Yahoo mail)	1
Entertainment (e.g., YouTube, Netflix, Hotstar)	1
Retail (e.g., Amazon, Walmart, Target)	1
Gaming (e.g., GameSpot, Destructoid, PlayStation Now, Stadia)	1
Health (e.g., health insurance, hospital websites)	1
Food (e.g., dominos, A fork and a penil, sethlui.com)	1
Transport (e.g., Uber, Cardoor, Car Rental)	1
Banking, Finance, Payment, Investments (e.g., MutualBank, bankofamerica.com, chase.com)	1
Education (e.g., Coursera, Udemy, Udacity, TED)	1
Cryptocurrencies (e.g., Binance, Coinbase, Bitfinex)	1
Backup and Sync (e.g., Dropbox, Google Sync, iCloud)	1
Developer (e.g., SlashDot, Reddit Programming, DZone)	1
Government, legal (e.g., USA.gov, Healthfinder.gov, Whitehouse.gov)	1
Cloud Computing, IoT, Remote access (e.g., TeamViewer, UltraVNC, Amazon Alexa)	1
Other	1
What kind of information do you share on social media with other people? (Select all that apply)	
Photos, videos and documents of yourself and your friends	1
Daily activities	1
Posts and links to things you like	1
Places you visited	1
Ideas and opinions	1
Your interests such as, books, music and TV shows	1
Personal events	1
Current location	1
Other	1

TABLE 8. Distribution of the point system of the participants background and the security knowledge and practices.

Question	Points
What is the highest level of education you have completed?	
Some High School	1
High School Graduate: diploma or equivalent	2
Some college, no degree	3
Associate's or technical degree	4
Bachelor's degree	5
Graduate degree (Masters, Doctorate, etc.)	6
Which of the following best describes your primary occupation?	
Computer Engineering or IT Professional	5
Engineer in other field	4
Medical (e.g., doctor, nurse, dentist)	4
Legal (e.g., lawyer, paralegal)	4
Education or Science	4
Business, Management, or Financial	4
Administrative Support (e.g., secretary, assistant)	4
Graduate student	3
College student	3
Art, Writing, or Journalism	2
Retired	1
Unemployed	1
Skilled Labor	1
Service	1
Do you have any experience working in the field of cybersecurity?	
Yes	4
No	0
Do you use antivirus on any of your devices?	
Yes	1
No	0
Which of these passwords do you prefer to use?	
football	1
1234567890	1
acidanthera	2
aa123456@	3
jbdkfdjll34904@*Ed4G2+	4
What is meant by the lock symbol next to google.com in the figure below?	
The website is using HTTPS and the connection is secure	1
The website is using HTTP and the connection is not secure	0
I don't know	0
Do you use Two-Factor Authentication (2FA) for any online services?	
Yes	1
No	0
Do you use a Password-Manager?	
Yes	1
No	0
Have you ever personally encrypted any of your files to defend against malicious people?	
Yes	2
No	0
What is the privacy setting for most of your social media accounts?	
Public	0
Private	1
Mixed	1
Have you ever changed the default privacy settings on any of your accounts?	
Yes	1
No	0

ABOUT SURVEY

95- Are you now willing to read the privacy policy?

****NOTE: If the answer for the question 95 in no: Go to not willing to read block**

NOT WILLING TO READ

96- Would you be willing to read the privacy policy if it was more user friendly and easier to read?

97- Would you read the privacy policy if it is mandatory to read before you could sign up for a service?

98- Would you be willing to read a privacy policy if you had the option to selectively decline parts of the it that you do not agree with?

99- Now that you know about the risks associated with privacy policies, why do you still prefer not to read them? (Select all that apply)

APPENDIX C
TABLES

See Tables 7 and 8.

REFERENCES

[1] I. D. Corporation. *IDC's Global DataSphere Forecast Shows Continued Steady Growth in the Creation and Consumption of Data*. Accessed: May 8, 2020. [Online]. Available: https://www.idc.com/getdoc.jsp?containerId=prUS46286020

[2] B. Fung. *Facebook Will Pay an Unprecedented $5 Billion Penalty Over Privacy Breaches*. Accessed: Jul. 25, 2019. [Online]. Available: https://www.idc.com/getdoc.jsp?containerId=prUS46286020

[3] C. Duffy. *Google Agrees to Pay $13 Million in Street View Privacy Case*. Accessed: Jul. 25, 2019. [Online]. Available: https://www.cnn.com/2019/07/22/tech/google-street-view-privacy-lawsuit-settlement/index.html

[4] S. Lee. *LinkedIn to Pay $13 Million* in Suit *Settlement for Excessively Spamming Users*. Accessed: Oct. 15, 2015. [Online]. Available: https://www.newsweek.com/linkedin-13-million-class-action-lawsuit-emails-379975

[5] K. Komando. *Your Apps Know Where You Were Last Night, and They're Not Keeping it Secret*. Accessed: Dec. 19, 2019. [Online]. Available: https://www.YouT1:Yourphonereallyislisteningin

[6] J. Cox. *How the U.S. Military Buys Location Data from Ordinary Apps*. Accessed: Nov. 16, 2020. https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x

[7] J. Valentino-Devries, N. Singer, and A. Krolik. *Your Apps Know Where YouWere Last Night, and They're Not Keeping it Secret*. Accessed: Dec. 10, 2018. [Online]. Available: https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html

[8] G. Dance and J. Valentino-Devries. *Have a Search Warrant for Data? Google Wants You to Pay*. Accessed: Jan. 24, 2020. [Online]. Available: https://www.nytimes.com/2020/01/24/technology/google-search-warrants-legal-fees.html%201/25

[9] J. G. Cabañas, A. Cuevas, A. Arrate, and R. Cuevas, "Does Facebook use sensitive data for advertising purposes?" *Commun. ACM*, vol. 64, no. 1, pp. 62–69, Dec. 2020, doi: 10.1145/3426361.

[10] J. G. Cabañas, A. Cuevas, and R. Cuevas, "Unveiling and quantifying Facebook exploitation of sensitive personal data for advertising purposes," in *Proc. 27th USENIX Secur. Symp. (USENIX Secur.)*. Baltimore, MD, USA, Aug. 2018, pp. 479–495. [Online]. Available: https://www.usenix.org/conference/usenixsecurity18/presentation/cabanas

[11] A. N. Charlie Warzel. *Google's 4,000-Word Privacy Policy is a Secret History of the Internet*. Accessed: Jul. 10, 2019. [Online]. Available: https://www.nytimes.com/interactive/2019/07/10/opinion/google-privacy-policy.html

[12] L. Rainie, S. Kiesler, R. Kang, M. Madden, M. Duggan, S. Brown, and L. Dabbish, "Anonymity, privacy, and security online," *Pew Res. Center*, vol. 5, 2013.

[13] E. Rader, "Awareness of behavioral tracking and information privacy concern in Facebook and Google," in *Proc. 10th Symp. Usable Privacy Secur. (SOUPS)*, 2014, pp. 51–67.

[14] L. Agarwal, N. Shrivastava, S. Jaiswal, and S. Panjwani, "Do not embarrass: Re-examining user concerns for online tracking and advertising," in *Proc. 9th Symp. Usable Privacy Secur.*, 2013, pp. 1–13.

[15] B. Knijnenburg and D. Cherry, "Comics as a medium for privacy notices," in *Proc. 15th Symp. Usable Privacy Secur. (SOUPS)*. Denver, CO, USA: USENIX Assoc., Jun. 2016. [Online]. Available: https://www.usenix.org/conference/soups2016/workshop-program/wfpn/presentation/knijnenburg

[16] A. I. Anton, J. B. Earp, Q. He, W. Stufflebeam, D. Bolchini, and C. Jensen, "Financial privacy policies and the need for standardization," *IEEE Secur. Privacy*, vol. 2, no. 2, pp. 36–45, Mar. 2004.

[17] M. A. Graber, D. M. D. Alessandro, and J. Johnson-West, "Reading level of privacy policies on internet health web sites," *J. Family Pract.*, vol. 51, no. 7, p. 642, 2002.

[18] I. Pollach, "What's wrong with online privacy policies?" *Commun. ACM*, vol. 50, no. 9, pp. 103–108, Sep. 2007.

[19] E. Luger, S. Moran, and T. Rodden, "Consent for all: Revealing the hidden complexity of terms and conditions," in *Proc. SIGCHI Conf. Hum. Factors Comput. Syst.*, 2013, pp. 2687–2696.

[20] G. H. M. Laughlin, "Smog grading-a new readability formula," *J. Reading*, vol. 12, no. 8, pp. 639–646, 1969.

[21] C. Jensen and C. Potts, "Privacy policies as decision-making tools: An evaluation of online privacy notices," in *Proc. SIGCHI Conf. Hum. Factors Comput. Syst.*, 2004, pp. 471–478.

[22] R. Flesch and A. J. Gould, *The Art of Readable Writing*, vol. 8. New York, NY, USA: Harper, 1949.

[23] R. W. Proctor, M. A. Ali, and K.-P.-L. Vu, "Examining usability of web privacy policies," *Int. J. Hum.-Comput. Interact.*, vol. 24, no. 3, pp. 307–328, Mar. 2008.

[24] J. Bonneau and S. Preibusch, "The privacy jungle: On the market for data protection in social networks," in *Economics of Information Security and Privacy*. Boston, MA, USA: Springer, 2010, pp. 121–167.

[25] M. Tabassum, A. Alqhatani, M. Aldossari, and H. Richter Lipford, "Increasing user attention with a comic-based policy," in *Proc. CHI Conf. Hum. Factors Comput. Syst.*, Apr. 2018, pp. 1–6.

[26] C. Fiesler and B. Hallinan, "'We Are the product': Public reactions to online data sharing and privacy controversies in the media," in *Proc. CHI Conf. Hum. Factors Comput. Syst.*, 2018, pp. 1–13.

[27] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner, "Android permissions: User attention, comprehension, and behavior," in *Proc. 8th Symp. Usable Privacy Secur.*, 2012, pp. 1–14.

[28] I. Shklovski, S. D. Mainwaring, H. H. Skúladóttir, and H. Borgthorsson, "Leakiness and creepiness in app space: Perceptions of privacy and mobile app use," in *Proc. SIGCHI Conf. Hum. Factors Comput. Syst.*, 2014, pp. 2347–2356.

[29] F. Shih, I. Liccardi, and D. Weitzner, "Privacy tipping points in smartphones privacy preferences," in *Proc. 33rd Annu. ACM Conf. Hum. Factors Comput. Syst.*, Apr. 2015, pp. 807–816.

[30] M. Schreiner and T. Hess, "Examining the role of privacy in virtual migration: The case of WhatsApp and Threema," in *Proc. 21st Amer. Conf. Inf. Syst.*, Puerto Rico, 2015, pp. 3696–3706.

[31] P. G. Leon, B. Ur, Y. Wang, M. Sleeper, R. Balebako, R. Shay, L. Bauer, M. Christodorescu, and L. F. Cranor, "What matters to users? Factors that affect users' willingness to share information with online advertisers," in *Proc. 9th Symp. Usable Privacy Secur.*, 2013, pp. 1–12.

[32] J. P. Carrascal, C. Riederer, V. Erramilli, M. Cherubini, and R. de Oliveira, "Your browsing behavior for a big mac: Economics of personal information online," in *Proc. 22nd Int. Conf. World Wide Web*, 2013, pp. 189–200.

[33] H. Xu, T. Dinev, J. Smith, and P. Hart, "Information privacy concerns: Linking individual perceptions with institutional privacy assurances," *J. Assoc. Inf. Syst.*, vol. 12, no. 12, pp. 798–824, Dec. 2011.

[34] T. Ermakova, A. Baumann, B. Fabian, and H. Krasnova, "'Privacy policies and users' trust: Does readability matter?" in *Proc. 20th Amer. Conf. Inf. Syst. (AMCIS)*. Savannah, GA, USA: Assoc. Inf. Syst., Aug. 2014. [Online]. Available: http://aisel.aisnet.org/amcis2014/HumanComputerInteraction/GeneralPresentations/14 and https://dblp.org/rec/conf/amcis/ErmakovaBFK14.bib

[35] H. Habib, Y. Zou, A. Jannu, N. Sridhar, C. Swoopes, A. Acquisti, L. F. Cranor, N. Sadeh, and F. Schaub, "An empirical analysis of data deletion and opt-out choices on 150 websites," in *Proc. 15th Symp. Usable Privacy Secur. (SOUPS)*, 2019, pp. 387–406.

[36] B. Fabian, T. Ermakova, and T. Lentz, "Large-scale readability analysis of privacy policies," in *Proc. Int. Conf. Web Intell.*, Aug. 2017, pp. 18–25.
[37] T. Linden, R. Khandelwal, H. Harkous, and K. Fawaz, "The privacy policy landscape after the GDPR," *Proc. Privacy Enhancing Technol.*, vol. 2020, no. 1, pp. 47–64, Jan. 2020.
[38] R. W. Reeder, L. Bauer, L. F. Cranor, M. K. Reiter, K. Bacon, K. How, and H. Strong, "Expandable grids for visualizing and authoring computer security policies," in *Proc. 26th Annu. CHI Conf. Hum. Factors Comput. Syst. (CHI)*, 2008, pp. 1473–1482.
[39] H. R. Lipford, A. Besmer, and J. Watson, "Understanding privacy settings in Facebook with an audience view," in *Proc. UPSEC*, vol. 8, 2008, pp. 1–8.
[40] J. Watson, M. Whitney, and H. R. Lipford, "Configuring audience-oriented privacy policies," in *Proc. 2nd ACM Workshop Assurable Usable Secur. Configuration (SafeConfig)*, 2009, pp. 71–78.
[41] H. R. Lipford, J. Watson, M. Whitney, K. Froiland, and R. W. Reeder, "Visual vs. compact: A comparison of privacy policy interfaces," in *Proc. SIGCHI Conf. Hum. Factors Comput. Syst.*, 2010, pp. 1111–1114.
[42] F. Schaub, R. Balebako, A. L. Durity, and L. F. Cranor, "A design space for effective privacy notices," in *Proc. 11th Symp. Usable Privacy Secur. (SOUPS)*, 2015, pp. 1–17.
[43] S. B. Barnes, "A privacy paradox: Social networking in the United States," *First Monday*, vol. 11, no. 9, Sep. 2006. [Online]. Available: https://firstmonday.org/ojs/index.php/fm/article/view/1394, doi: 10.5210/fm.v11i9.1394.
[44] S. Kokolakis, "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon," *Comput. Secur.*, vol. 64, pp. 122–134, Jan. 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404815001017
[45] A. L. Young and A. Quan-Haase, "Privacy protection strategies on Facebook," *Inf., Commun. Soc.*, vol. 16, no. 4, pp. 479–500, May 2013, doi: 10.1080/1369118X.2013.777757.
[46] V. K. Tuunainen, O. Pitkänen, and M. Hovi, "Users' awareness of privacy on online social networking sites-case Facebook," in *Proc. Bled*, 2009, p. 42.
[47] P. Nyoni and M. Velempini, "Privacy and user awareness on Facebook," *South Afr. J. Sci.*, vol. 114, nos. 5–6, pp. 1–5, May 2018.
[48] A. Acquisti and R. Gross, "Imagined communities: Awareness, information sharing, and privacy on the Facebook," in *Proc. Int. Workshop Privacy Enhancing Technol.* Springer, 2006, pp. 36–58.
[49] S. Stieger, C. Burger, M. Bohn, and M. Voracek, "Who commits virtual identity suicide? Differences in privacy concerns, internet addiction, and personality between Facebook users and quitters," *Cyberpsychol., Behav., Social Netw.*, vol. 16, no. 9, pp. 629–634, Sep. 2013.
[50] J. Caramujo and A. M. R. D. Silva, "Analyzing privacy policies based on a privacy-aware profile: The Facebook and LinkedIn case studies," in *Proc. IEEE 17th Conf. Bus. Informat.*, Jul. 2015, pp. 77–84.
[51] E. Hargittai and A. Marwick, "'What can I really do?' Explaining the privacy paradox with online apathy," *Int. J. Commun.*, vol. 10, p. 21, Jul. 2016.
[52] F. Schaub, A. Marella, P. Kalvani, U. Blase, C. Pan, E. Forney, and L. F. Cranor, "Watching them watching me: Browser extensions' impact on user privacy awareness and concern," in *Proc. NDSS Workshop Usable Secur.*, 2016, pp. 1–10.
[53] G. R. Milne and M. J. Culnan, "Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices," *J. Interact. Marketing*, vol. 18, no. 3, pp. 15–29, 2004.
[54] V. Groom and R. Calo, "Reversing the privacy paradox: An experimental study," Social Sci. Res. Netw., Rochester, NY, USA, 2011. Accessed: Oct. 26, 2021. [Online]. Available: https://papers.ssrn.com/abstract=1993125
[55] J. A. Obar and A. Oeldorf-Hirsch, "The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services," *Inf., Commun. Soc.*, vol. 23, no. 1, pp. 128–147, 2018.
[56] A. J. Berinsky, G. A. Huber, and G. S. Lenz, "Evaluating online labor markets for experimental research: Amazon. com's mechanical Turk," *Political Anal.*, vol. 20, no. 3, pp. 351–368, 2012.
[57] A. Berinsky, G. Huber, and G. Lenz, "Using mechanical turk as a subject recruitment tool for experimental research," *Submitted Rev.*, 2011. Accessed: Oct. 26, 2021. [Online]. Available: https://www.researchgate.net/publication/228415550_Using_Mechanical_Turk_as_a_Subject_Recruitment_Tool_for_Experimental_Research
[58] K. Walters, D. A. Christakis, and D. R. Wright, "Are mechanical Turk worker samples representative of health status and health behaviors in the US?" *PLoS ONE*, vol. 13, no. 6, 2018, Art. no. e0198835.
[59] J. K. Goodman, C. E. Cryder, and A. Cheema, "Data collection in a flat world: The strengths and weaknesses of mechanical Turk samples," *J. Behav. Decis. Making*, vol. 26, no. 3, pp. 213–224, Jul. 2013.
[60] E. M. Redmiles, S. Kross, and M. L. Mazurek, "How well do my results generalize? Comparing security and privacy survey results from MTurk, web, and telephone samples," in *Proc. IEEE Symp. Secur. Privacy (SP)*, San Francisco, CA, USA, May 2019, pp. 1326–1343, doi: 10.1109/SP.2019.00014.
[61] E. M. Redmiles, S. Kross, and M. L. Mazurek, "How well do my results generalize? Comparing security and privacy survey results from MTurk, Web, and telephone samples," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2019, pp. 1326–1343.
[62] R. Kang, S. Brown, L. Dabbish, and S. Kiesler, "Privacy attitudes of mechanical Turk workers and the US public," in *Proc. 10th Symp. Usable Privacy Secur. (SOUPS)*. Menlo Park, CA, USA, Jul. 2014, pp. 37–49. [Online]. Available: https://www.usenix.org/conference/soups2014/proceedings/presentation/kang
[63] *Google Privacy Policy–Privacy & Terms*. Accessed: Oct. 26, 2021. [Online]. Available: https://policies.google.com/privacy?hl=en-U.S
[64] *Amazon Privacy Notice*. Accessed: Oct. 26, 2021. [Online]. Available: https://www.amazon.com/gp/help/customer/display.html?nodeId=202056900
[65] *Facebook Data Policy*. Accessed: Oct. 26, 2021. [Online]. Available: https://www.facebook.com/policy.php
[66] Z. Group. *Zillow Privacy Policy*. Accessed: Oct. 26, 2021. https://www.zillowgroup.com/terms-of-use-privacy-policy/zg-privacy-policy
[67] *Uber Privacy Notice*. Accessed: Oct. 26, 2021. [Online]. Available: https://www.uber.com/global/es/privacy/notice/
[68] *Data Policy*. Accessed: Oct. 26, 2021. [Online]. Available: https://www.facebook.com/policy.php

DUHA IBDAH (Member, IEEE) received the bachelor's degree in network engineering and security from the Jordan University of Science and Technology and the master's degree in computer and information science from the University of Michigan, Dearborn, where she is currently pursuing the Ph.D. degree with the Computer and Information Department. Prior to joining, the University of Michigan, she worked as a Network Engineer at Cisco Systems. Her research interests include privacy, systems security, and networking.

NADA LACHTAR (Member, IEEE) received the bachelor's degree in network engineering and security from the Jordan University of Science and Technology and the master's degree in computer and information science from the University of Michigan, Dearborn, where she is currently pursuing the Ph.D. degree with the Computer and Information Department. Her research interests include the area of malware detection, systems security, data privacy, and applied machine learning.

SATYA MEENAKSHI RAPARTHI received the master's degree in computer and information science from the University of Michigan, Dearborn. She is currently a Cybersecurity Engineer at Ford Motor Company, Dearborn, MI, USA. Her responsibilities include developing secure standards for key material, vehicle access, diagnostics and vehicle to cloud communication. Prior to joining her master's, she worked at Accenture as an Application Development Analyst, where she was responsible developing and building database applications. Her research interests include automotive security, privacy, and networking.

ANYS BACHA (Member, IEEE) is currently an Assistant Professor with the University of Michigan. He leads the Security and Systems Laboratory which focuses on advancing the state-of-the-art in mobile and computer systems to address important challenges in security, applied machine learning, and energy efficiency. His research contributions have been published in top tier venues where, his work received various prestigious awards. Furthermore, his industry impact is demonstrated through several U.S. and World patents. Prior to joining academia, he spent over 13 years in the industry where, he worked in different research and development roles on a variety of subsystems spanning the hardware, firmware, and operating systems layers. He led multiple interdisciplinary efforts that include driving architectural changes into next generation Intel processors that are necessary to meet the demands of emerging workloads. During his tenure at Hewlett-Packard, he led a group of engineers on a multi-million dollar scalable computing project that broke world records in performance, in 2015 and 2014.