Users' Expectations About and Use of Smartphone Privacy and Security Settings

Alisa Frik
International Computer Science Institute; University of California
Berkeley, USA
afrik@icsi.berkeley.edu

Juliann Kim
University of California
Berkeley, USA
juliannkim@berkeley.edu

Joshua Rafael Sanchez
University of California
Berkeley, USA
joshuarafael@berkeley.edu

Joanne Ma
University of California
Berkeley, USA
joannema@berkeley.edu

ABSTRACT

With the growing smartphone penetration rate, smartphone settings remain one of the main models for information privacy and security controls. Yet, their usability is largely understudied, especially with respect to the usability impact on underrepresented socio-economic and low-tech groups. In an online survey with 178 users, we find that many people are not aware of smartphone privacy and security settings, their defaults, and have not configured them in the past, but are willing to do it in the future. Some participants perceive low self-efficacy and expect difficulties and usability issues with configuring those settings. Finally, we find that certain socio-demographic groups are more vulnerable to risks and feel less prepared to use smartphone settings to protect their online privacy and security.

CCS CONCEPTS

• **Security and privacy → Usability in security and privacy**; *Privacy protections*; Social aspects of security and privacy.

KEYWORDS

Privacy settings, security settings, information architecture, self-efficacy, digital divide, SES, cognitive interviews

ACM Reference Format:
Alisa Frik, Juliann Kim, Joshua Rafael Sanchez, and Joanne Ma. 2022. Users' Expectations About and Use of Smartphone Privacy and Security Settings. In *CHI Conference on Human Factors in Computing Systems (CHI '22), April 29-May 5, 2022, New Orleans, LA, USA.* ACM, New York, NY, USA, 24 pages. https://doi.org/10.1145/3491102.3517504

1 INTRODUCTION

Smartphones are the most commonly used type of communication technology [65], and the United States is one of the world's largest smartphone markets, with more than 275 million smartphone users, representing 80% of the country's population [67]. Thus, smartphone settings remain one of the main models for information privacy and security controls, and their usability is especially important for protecting users' privacy. For instance, those settings allow users to opt out of data tracking and ad personalization, set passcode for unlocking the screen, enable 2-factor authentication (2FA), automatic updates, etc.

However, users do not always fully understand the implications of changing privacy/security settings [9, 12]. Confusing information architecture and poor usability may make it even harder to navigate those settings [16, 73]. For example, in the latest iOS version, privacy settings are grouped under the Privacy category in the main settings menu, but there is no single category that would group the security settings. Instead, security settings are scattered across various places: software updates and AirDrop settings are in the General category, passcode is in the Face ID & Passcode category, 2FA is under Apple ID, iCloud, Media & Purchases. Such labelling and information architecture may be confusing and misleading to the users, preventing them from easily finding and changing the settings according to their preferences. However, surprisingly little research has been carried out to examine the usability of smartphone settings menus.

Moreover, prior research argues that smartphone settings were largely developed by technologists, and often contain professional jargon [44]. People that do not share the same background may find it difficult to understand this jargon and meaningfully use privacy and security settings [9, 77]. More broadly, as we discuss in more detail in Section 2, the knowledge, skills, and experience with technology in general, and privacy and security specifically, may vary across different socio-demographic groups [12, 42]. Thus, poor usability of smartphone setting menus may disproportionately affect certain vulnerable populations, e.g. children, older adults, lower income, lower education, and marginalized communities. Yet, little research has been conducted to investigate that. While some prior research focuses on specific socio-demographic groups or particular settings in isolation (e.g., screen locking [7, 50]), to the best of our knowledge no prior work offers the broad examination of users' opinions about smartphone privacy and security settings, and comparisons across socio-demographic groups. Moreover, while prior work explores the convenience of *using* certain smartphone settings (e.g. the burden of repeatedly typing a passcode to unlock

CHI '22, April 29-May 5, 2022, New Orleans, LA, USA

ACM ISBN 978-1-4503-9157-3/22/04.
https://doi.org/10.1145/3491102.3517504

the screen), it doesn't explore the perceived difficulties with *finding and enabling* those settings.

We contribute to the field of usable privacy and security by highlighting users' misconceptions and beliefs about smartphone settings, their defaults, expected impact on user experience, difficulties with finding and changing the settings, and with mapping the settings against online risks. Given the fast pace of advancement in mobile technologies and changes in smartphone settings, empirical evidence presented in this paper provides useful references for future comparisons and tracking of the evolution of users' opinions and experiences with smartphone privacy and security features. Moreover, inclusion of a diverse sample of participants revealed important insights about the impact of socio-demographic factors.

Our ultimate goal is to provide recommendations that empower users to make informed decisions about privacy and security settings in smartphones. Specifically, in this study we will focus on the following research questions:

RQ1: Are users aware of **a)** privacy and security settings available on their smartphones, and **b)** their default configurations?

RQ2: Have users configured smartphone privacy and security settings in the past?

RQ3: Do they intend to configure them in the future?

RQ4: What are users' perceptions of self-efficacy (i.e. perceived difficulty) of configuring privacy and security settings, and what difficulties do they anticipate?

RQ5: What are users' understanding of the implications of changing certain smartphone privacy/security settings, including **a)** the impact on overall user experience with their smartphones, and **b)** the perceived effectiveness in protecting from common privacy and security risks?

RQ6: What are the differences among users with different socio-economic backgrounds (e.g., age, gender identity, income, education, race and ethnicity) and digital experience in terms of their **a)** past behaviors (whether they configured smartphone privacy and security settings in the past), **b)** intentions to configure them in the future, **c)** perceived difficulty of configuring these settings, and **d)** the impact on overall user experience with their smartphones?

To this end, we conducted an online survey of 178 smartphone users with diverse backgrounds and demographics. We found that many participants are not aware of the available smartphone settings to counter privacy and security risks, and have not changed them on their devices, due to the anticipated difficulties with configuring the settings and expected negative impact on user experience. Yet, many of them are willing to change them in the future. While on average, more than half of our participants expect settings to be easy to configure, up to a third of participants anticipate difficulties with these tasks due to expected poor information architecture, lack of experience and knowledge, or technical limitations. Some participants believe that manufacturers make these settings hard to find and understand on purpose, to maximize data collection. Finally, we found that some socio-demographic groups (such as older adults, racial/ethnic minorities, and females) are particularly vulnerable to online risks, as many of them are less concerned about online privacy and security, engage less in configuring smartphone privacy and security settings, anticipate more difficulties with configuring them, and expect their negative impact on user experience. We suggest directions for future research, and provide recommendations for improving the design of smartphone privacy and security settings.

2 RELATED WORK

Since smartphones are currently the most popular internet connected technology [65, 67], privacy and security settings represent one of the most popular models for users to indicate their privacy and security preferences. Thus, their usability is crucial for ultimate protection of users' privacy and security. We first describe existing work on the usability of privacy/security settings. We then describe the opinions about, and behaviors and experiences with privacy and security among different socio-demographic groups.

2.1 Usability of privacy and security settings

The concept of usable security and privacy suggests designing security and privacy settings in a way that allows users with diverse abilities to be aware of the device's functionalities and tasks they need to perform to protect their privacy and security, to understand and successfully perform those tasks, to not make dangerous mistakes, and to be sufficiently comfortable with the interface to continue using it [75].

There is a body of literature on the usability of mobile permissions—another popular mechanism for providing users with control over their personal data collected by apps, in addition to the smartphone settings menus. For instance, some studies show that existing privacy interfaces do not provide users with sufficient amount of information and control [19, 19, 35, 40, 41]. A number of attempts have been made to improve usability of permission systems through personalized recommendations [45, 46]. Users are even willing to pay a premium to use the applications that request fewer permissions [16], indicating the importance of privacy in decision-making about app use. However, some users may not even be aware of the privacy and security options available to them in the permission systems [44, 58].

While the research on usability of *mobile app permissions* has made a lot of progress [e.g., 16, 35, 45, 47], the literature on the usability of privacy and security *settings in smartphones* is surprisingly limited. Task based study revealed limited awareness about default privacy settings in smartphones, understanding of their implications [58]. Prior work has found that almost half of the users find screen locking mechanisms on smartphones annoying [17, 30, 36]. Through prototype testing, Micallef et al. [50] found that requiring users to use PIN to unlock the screen only when the context suggests an increased risk (e.g. when location of the user changes from home to "on the move") improves the perceived usability of screen locking mechanism. Bhagavatula et al. [7] explored users' preferences, and perceptions of security and usability for biometric authentication mechanisms. However, those studies focused on a specific privacy and security setting and did not investigate the socio-demographic differences in users' experiences and opinions. Moreover, they focused on the convenience of exploitation of a security feature rather than difficulties with finding and enabling it.

Zhou et al. [77] developed and tested a prototype of a mobile app for guided configuration of smartphone privacy settings such as Find My Device, Backup, Location Blurring, and Guest mode. They

found that users (especially with higher income) are willing to have more control over privacy settings than they currently have. Older participants were less likely to search information about mobile privacy protection than younger participants. While these results motivate further investigations, they are based on app prototype tests instead of actual smartphone settings, and focus only on a small subset of privacy/security features. Moreover, while focusing on trust perceptions, information sensitivity, perceived control, and information search about privacy protections, Zhou et al. [77] do not examine participants' past behaviors and intentions to interact with security and privacy settings, awareness and beliefs about default configurations, perceived self-efficacy and impact on user experience.

Vecchiato et al. [73] proposed a tool for automated assessment of the security configurations on mobile devices and found that users rarely change factory settings. However, this study only focuses on Android devices (excluding iOS), security settings (excluding privacy), and doesn't provide insights into reasons for users' behaviors, their perceptions, opinions, and beliefs about the settings. Our study aims at closing these gaps.

2.2 Socio-demographic differences in privacy and security

Prior work has shown the evidence of privacy knowledge–belief gap [55, 56, 72]. Specifically, knowledge and self-efficacy regarding device's privacy settings affect the use of privacy-enhancing settings [12]. Thus, privacy and security knowledge and self-efficacy are crucial for one's ability to protect their online privacy and security. Yet, such knowledge, perceptions of own abilities and skills, and experience with technologies may not be equally distributed among socio-demographic groups of users.

Prior research has shown, for instance, that age, gender and education affect location tracking prevention by smartphone users [42]. Adolescents tend to disclose more personal information and use less restrictive privacy settings in online social networks that adults [74]. Compared to younger populations, older adults are particularly unaware of and vulnerable to information privacy and security risks [1, 10], have less knowledge of online security risks [23–25], use technology less frequently [11, 15, 24, 27, 39, 78], and are more often targeted for security and privacy attacks [34]. Since lack of security knowledge and experience generally correlates with riskier behaviors [31, 54, 55], populations with lower technological literacy or access to technology are especially vulnerable to online risks. A survey of German users shows that younger and less educated respondents engage in security behaviors less, but did not find similar effects for the privacy behaviors [8].

Women are found to have higher online risk perceptions and privacy concerns [21, 62], but to be slower at detecting identity fraud [69]. While women become victims of online harassment and stalking more often than men [69], they seem to engage less in protective behaviors than men [62]. Women also report lower security self-efficacy, security behaviors, levels of computer skills, and prior experience with computer security than men [2]; however, the study does not provide the evidence of whether these perceptions are accurate.

The research with Latinx undocumented immigrants revealed that this user group is more concerned about identity theft and privacy in general, and is less informed about government surveillance risks, leading to privacy resignation [26]. While some studies find that Latinx adults in the United States that are under-resourced also have low technology literacy [49], other studies argue that levels of literacy are not a sufficient explanation of socio-demographic differences in privacy and security behaviors [26].

Although digital divide research has been useful in highlighting issues with discrimination in technology, it often oversimplifies those issues by wrongly assuming that particular racial groups lack technological comprehension, instead of lacking access to technology and therefore necessary experience with it [28]. Similarly, a large survey reveals that contrary to prior assumptions, less educated people report equal or fewer incidents of privacy and security violations than more educated people; instead users' experiences are more correlated with the source of security advice they use, regardless of their socio-economic status [59]. Moreover, security education alone does not necessarily address the issues of poor security practices, since many users with moderate to high security knowledge still make poor mobile security decisions [9]. Thus, *usability* of smartphone privacy and security settings need to be improved as well to help users make informed decisions about their personal data.

Thus, there is a need for more extensive research how socioeconomic status impacts users' understanding and mitigation of online risks. To the best of our knowledge, no prior work has investigated the differences in opinions and behaviors regarding smartphone privacy and security settings among socio-demographic groups. Our work aims at providing a comprehensive overview of the perspectives of users of both major mobile operating systems—iOS and Android—regarding 19 commonly used smartphone privacy and security settings. In addition to studying the perceived impact of those settings on user experiences, our study provides insights into expected difficulties with finding and configuring those settings, awareness, prior behaviors and future intentions to configure them, opinions about their effectiveness in addressing online privacy and security concerns, and beliefs about factory defaults. Finally, it explores the differences in perspectives across various socio-demographic groups.

3 METHOD

We conducted an online survey using Qualtrics. We recruited participants from Prolific among the US residents who had completed at least 5 tasks with an approval rate of at least 95%, and who use Android or iOS mobile operating system. To achieve a diverse sample of participants, we used the Prolific's screening criteria for age (groups below and above 40 years old[1]) and ethnicity (White, Black, Asian, Latinx/Hispanic, and Other categories) to reach a quota of at least 15 people per age-ethnicity group. Upon accepting the task, participants were directed to a Qualtrics page to complete the survey. We obtained the IRB approval from our institution prior to

[1]We do not define people above 40 years old as older adults. We used 40 years as a threshold (representing about a half of average life expectancy in the US [37]) simply to achieve a greater sample diversity in terms of age, and we succeeded in it as shown in section 4.1.

conducting the survey. All participants provided their consent and signed the consent form before responding to the survey.

3.1 Settings selection

To survey participants about common smartphone privacy and security settings, we first generated a list of all privacy and security settings available in the latest versions of Android and iOS in August 2020. Because of the heterogeneity in use and settings availability in specific apps, we did not include app settings in our analysis to achieve more generalized results, and focused only on the settings provided by the mobile operating systems and their default browsers (Safari for iOS and Chrome for Android). We included the default browsers because they are pre-installed on all users' phones and are commonly used for information search [14].

Two researchers then independently rated the privacy and security impact of the settings from the initial list (high, medium, or low), and reached the Kupper-Hafner agreement rate of 0.56. They together discussed and resolved the disagreements, mitigating the initially low agreement rate. The selection of settings was discussed in a seminar with the group of 8 security researchers (1 professors, 3 postdocs, and 4 PhD students) from the lab; their feedback was taken into consideration, and the final selection received their approval. The final list includes 19 groups of settings (Table 1). Two of the selected settings are associated with the features that do not have equivalents in one of the mobile operating systems. Specifically, in Android there is no equivalent of iOS's AirDrop, and in iOS there is no equivalent of the Android's settings for ad personalization in Google Assistant. Moreover, there is one iOS setting (erasing the data after 10 failed passcode attempts) and one Safari setting (fraudulent website warnings) that are not available in Android and Chrome; however, due to their important privacy/security impact, we were curious about Android users' expectations and opinions on those settings and included them in the survey of Android users.

3.2 Survey

In the first part of the survey, we asked participants an open-ended question about two privacy or security risks that they worry about when using their smartphones; we encouraged them to consider different actors who may introduce the risks, including companies, governments, someone they know, strangers, etc. Then we asked them to describe, without looking at their phones, any settings currently available on their smartphones that they could configure to address each of the privacy/security risks they mentioned; we advised them to write 'N/a' if they thought there are no settings to protect against such risks. The goal of this part was to elicit unaided recall of risks and settings.

In the second part of the survey, we selected 3 of the 19 smartphone privacy and security settings at random and iteratively asked participants questions about them: whether they believe the setting is an existing option on their smartphone, what is its default configuration, how difficult or easy would it be to configure this setting, and reasons why it would be difficult. We also asked whether they have ever configured this setting before, intentions to configure it in the future, what privacy or security risks would this setting protect them from, how worried they are about privacy/security risks, the perceived effectiveness of the setting against these risks, and the expected impact of configuring the settings on the overall user experience with the smartphone.

Finally, we asked participants about demographics (including age, gender, ethnicity, education, income, employment status), digital skills and IT-related education or work experience. We also asked them about their use of smartphone, mobile browsers, password managers, face recognition authenticating features, and model and operating system of their smartphones. The full survey instrument can be found in Appendix B. (We will refer to the questions from the survey as Q followed by the number of the question, e.g. "Q7" throughout the paper.) We ran a small pilot ($N = 10$) using think-aloud method with non-expert users to assess the clarity of the survey, and received positive feedback.

3.3 Analysis

Regression analysis. For statistical analysis, we used logistic regressions for categorical data, ordered logistic regressions for ordinal data (Likert scales), and ordinary least square regressions for the continuous variables. The panel data structure was defined and the regression analysis took into consideration the nested structured of the data. As logistic regression coefficients do not have intuitive real world interpretations, we also estimated the Odds Ratios (OR) and reported them in the Results section to further assist the comprehension of our findings.

We used the following variables in our analysis:

- Awareness about the settings (Q5), categorical.
- Beliefs about defaults (Q6), categorical.
- Past behaviors—whether participants configured settings in the past (Q9), categorical.
- Intentions to configure the settings in the future (Q12), ordinal (Likert scale).
- Perceived difficulty to configure settings (Q7), ordinal (Likert scale).
- Perceived negative impact of settings on user experience (Q11), ordinal (Likert scale).
- Perceived effectiveness of settings against risks (Q13), ordinal (Likert scale).
- Perceived worry about the risks (Q15), ordinal (Likert scale).
- Index of the level of privacy and security concerns—an index constructed from the responses to Q15 using factor analysis (with eigenvalue over 1, Cronbach's *alpha* = .89), continuous.
- Age (Q23), continuous.
- Gender (Q24), categorical.
- Race/ethnicity (Q29), categorical.
- Education (Q30), ordinal.
- Income (Q27), ordinal.
- iOS users (Q1), binary: 1 for iOS users, 0 for Android users.
- Duration of experience with current OS (Q2), ordinal.
- Frequency of smartphone use (Q19), ordinal.
- Browser (Q18), categorical.
- Use of face recognition to unlock (Q22), binary: 1 if the participant reported using face recognition (Face ID, FaceUnlock) to unlock their smartphone, and 0 otherwise.
- Technical background (Q31), binary: 1 if the participant has education or work experience in computer science, software

Table 1: Privacy and security settings used in the survey. Asterisk (*) indicates the settings not available on Android/Chrome mobile browser, but which were still shown to the Android users.

Setting	Description shown to iOS users	Description shown to Android users
Location services	Turn off location services	
Passcode	Create a passcode to unlock the smartphone and authorizes actions like payments or password autofill	
Face unlock	Only allow the use of face recognition to unlock the smartphone if you are looking at the screen	
Notification preview	Allow the smartphone to show a preview of the notification content only when it is unlocked	
Automatic updates	Turn on automatic updates of the smartphone's operating system	
Erase data*	Turn on erasing of all data on the smartphone after 10 failed passcode attempts	
Contact tracing	Disable COVID-19 contact tracing	
Ad personalization	Limit ad tracking and ad personalization on your smartphone	
Two-factor authentication	Enable two-factor authentication for your *iCloud* account	Enable two-factor authentication for your *Google* account
Analytics	Deny analytics of usage and data on your *iCloud* account	Deny analytics of usage and data on your *Google* account
Voice commands	Don't allow the smartphone to listen for *"Hey Siri"* commands	Don't allow the smartphone to listen for *"Hey Google"* commands
Storing audio	Storing audio recordings of your *Siri* and Dictation interactions	Don't allow storing audio recordings of your *Google Assistant* interactions
Password reuse	View passwords that have been re-used on other websites in your smartphone's *Safari* browser	View passwords that have been re-used on other websites in your smartphone's *Chrome* browser
Pop-ups	Block pop-up windows on websites in your smartphone's *Safari* browser	Block pop-up windows on websites in your smartphone's *Chrome* browser
Website warnings*	Turn on fraudulent website warnings in the smartphone's *Safari* browser	Turn on fraudulent website warnings in the smartphone's *Chrome* browser
Cookies	Block all cookies in the smartphone's *Safari* browser	Block all cookies in the smartphone's *Chrome* browser
Browser tracking	Limit tracking of your activity in the smartphone's *Safari* browser	Limit tracking of your activity in the smartphone's *Chrome* browser
Voice assistant ad personalization	-	Limit ad tracking and ad personalization in Google Assistant
Airdrop	Allow only your contacts to share files with you over AirDrop	-

engineering, app development or other technical field, and 0 otherwise.

Qualitative analysis. To analyze the free-text responses, using thematic analysis, two researchers independently developed the codebooks for each of the open-ended questions based on all the responses. Then they discussed and merged the codebooks. They applied the final codebooks to the responses. Kupper-Hafner inter-rater agreement metric for multiple attribute responses was used to assess the reliability [43]. The agreement rate for the responses about risks was 0.58 and about settings was 0.89. The lower rate of agreement stems from the complexity and multiple attribute nature of the responses about risks (e.g. identity theft can be categorized as a social engineering attack, unauthorized financial transaction, and unauthorized remote access risks; when coders apply a subset of codes, the agreement rate decreases). The coders mitigated low agreement rate by discussing and resolving all the disagreements, eventually ensuring the high reliability of the results.

3.4 Limitations

As with any research, our study has a number of limitations. First, we used self-reported answers, thus the generalisability of our results is potentially limited by social desirability and overconfidence bias, i.e. participants could have overestimated their awareness of smartphone settings and self-efficacy in configuring them. However, it means that our findings illustrate a lower bound, and in reality users might be even less aware of or able to configure privacy and security settings in smartphones. The purpose of this survey was to elicit users' recall, awareness, expectations and beliefs about risks and settings. Asking users to look it up in their phones would have undermined the validity of those measures and mental models.

Future work (currently in progress) will complement survey results with the behavioral data from the cognitive interviews, where participants will be asked to find and configure the settings using their personal devices, contributing insights about the actual abilities to do so, associated difficulties and usability issues.

Second, our sample size is limited, but diverse in demographics. Crowdsourcing platforms is a commonly accepted recruitment method for academic research, producing reliable results [5]. Crowdsourcing platforms such as Prolific do not guarantee full representativeness of the global population of smartphone users. However, prior research has demonstrated that Prolific is a reliable platform for conducting research in HCI [18], and that Prolific participants are more diverse, less dishonest, more attentive, and produced higher data quality than Mturk and CrowdFlower participants [57]. Moreover, in our study, we aimed at recruiting a *diverse* rather than representative sample of users, because our goal was to assess if certain socio-economic factors affect the responses, not to estimate the distribution or prevalence of responses in the population or to study a particular group in isolation. Sample balancing helped us to mitigate further the potential shortcomings of the limited representativeness. Future work is called to validate the results with a larger sample and in more realistic environment (e.g., field experiment or usability study in which users are asked to configure the settings).

Third, our selection of settings was large but still limited; future work is invited to explore users' perspectives on other privacy and security settings in smartphones and mobile apps.

4 RESULTS

We recruited 178 participants from Prolific crowdsourcing platform at the end of October 2020. On average, participants spent 20 minutes on completing the survey, and received USD 2.5 as compensation. We obtained an average of 28 responses per setting, which is considered acceptable for statistical analysis [33, 48].

4.1 Participants

Our participants are between 18 and 73 years old (mean=37, SD=13); 63% are female, 35% are male, with the rest equally split between those who prefer to self-identify or not to answer about their gender. Regarding ethnicity, 28% self-identify as White, 19% as Hispanic/Latinx, 17% as Black, 17% as Asian, 13% have a mixed ethnicity, 4% have other ethnicity, and 2% prefer not to answer. All participants use English in their daily lives and/or in their smartphone settings. Most participants (73%) don't have IT-related background. Table 2 summarizes participants' education, employment, and income to provide further insight into the demographic composition of the sample.[2]

All participants use their smartphones every day, and 93% use their current mobile operating system for more than 2 years. Sixty percent of participants are Android users, and the rest are iOS users, which is representative of the 60/40 mobile OS market share distribution in 2019 in the US [13] but is the reverse of 39/61 distribution in 2020 [66]. However, because our goal was to recruit a set of participants diverse in terms of age and ethnicity rather than representative of smartphone users in general, we do not expect the same distribution of income, education, employment and other socio-demographic characteristics in our sample as in the general population of smartphone users. The default mobile browsers are most commonly used: 74% of our Android users primarily use Chrome, 79% of our iOS users primarily use Safari. More than 80% of participants find it easy to perform most of the smartphone tasks we asked them about, except ordering a ride using an app (16% have not tried doing it), scheduling an appointment with a doctor using a health portal app on a smartphone (28% have not tried doing it), and developing a smartphone app (75% have not tried doing it, and 24% find it difficult).

[2]Income divided by the number of household members produced same results as total household income, so for simplicity, we used the latter in the regressions analysis.

Table 2: Participant characteristics based on survey responses.

Individual characteristics	N	%
Education level		
Less than high school diploma	2	1.1%
Completed high school/GED	17	9.6%
Some college but no degree	47	26.4%
Associate's degree	22	12.4%
Bachelor's degree	62	34.8%
Master's degree	24	13.5%
Doctoral degree, JD, or equivalent	4	2.2%
Employment		
Employed full time	76	42.7%
Unemployed looking for work	28	15.7%
Student	22	12.4%
Employed part time	21	11.8%
Unemployed not looking for work	12	6.7%
Retired	7	3.9%
Employed part or full time & Student	5	2.8%
Disabled	3	1.7%
Homemaker	2	1.1%
Self-employed	2	1.1%
Household income		
Less than $10,000	16	9.0%
$10,001-20,000	13	7.3%
$20,001-30,000	24	13.5%
$30,001-50,000	32	18.0%
$50,001-70,000	34	19.1%
$70,001-100,000	18	10.1%
$100,001-150,000	21	11.8%
$150,001-200,000	8	4.5%
$200,001-300,000	4	2.2%
More than $300,000	1	0.6%
Preferred not to answer	7	3.9%

4.2 Free-text responses about privacy and security risks and settings

We first asked participants about smartphone privacy and security risks that worry them (Q3), and what settings are supposed to help them mitigate those risks (Q4). We asked these open-ended questions before we provided the multiple-choice questions to explore participants' awareness of risks and settings using unaided recall method, to avoid priming effects and imposing our categorisation of risks and settings on them. Each of the 178 respondents provided

2 responses about risks and about settings, thus we provide the count of *occurrences* rather than the count of participants.

Risks. Most frequently (102 times) respondents mentioned the concerns about *unauthorized remote access*, for instance via a hacking attack, spyware or malware, virus, data breach, or compromised passwords; some participants were particularly worried about unauthorized access to their smartphone's microphone and camera.

Second most common risk was associated with the *data gathering by companies* (mentioned 63 times). Only a few participants elaborated that the gathered data can be sold or used for marketing or targeted advertising, while the majority of participants did not mention the purpose of data collection (e.g. *"Apps obtaining personal info"*, P48). *Data gathering by governments* was mentioned less often (27 times), and *data gathering by individuals* (e.g. someone they know) was mentioned only twice. Particularly participants were concerned about collection of their location data (mentioned 17 times) by companies, governments, and unspecified actors. Participants mentioned *tracking* without specifying the entity gathering the data 19 times.

Participants were also worried about *unauthorised financial transactions* (27 times) and *identity theft* (12 times), *social engineering attacks* (14 times), and *unauthorized physical access* to the device (10 times). Other risks were mentioned infrequently, or without an adequate level of detail (e.g. *"privacy violation"*, P50).

Settings. To mitigate the risks they are worried about, most often participants proposed strategies aiming at *controlling data collection* (69 times), such as restricting access permissions, and turning off smartphone features like voice assistants or location services. Some participants acknowledged the trade-offs between such strategies and convenience or device's and app's abilities to function without these permissions: *"There is a setting to prevent locations sharing but many apps will not work unless given permission"* (P19).

Second most popular group of strategies was associated with *avoiding behaviors* (48 times) rather than configuring settings. It included avoiding suspicious apps and websites, and insecure networks, limiting data storage (for instance, not saving financial details, erasing personal data from the smartphone, etc.), limiting risky online activities (e.g. not visiting privacy sensitive websites from the phone, not opening attachments and links from unknown senders, not answering calls from unknown numbers, etc.).

Several strategies were associated with *authentication management* (36 times), including good password hygiene, using 2-factor authentication (2FA), password managers, and disabling password autofill features.

Some mentioned privacy- and security-enhancing *software* (30 times), including antivirus, call and ad blockers, backup tools, secure payment mechanisms, and multi-purpose security tools, like Lookout, LifeLock, or Malwarebytes.[3]

Rarely people mentioned specific *security strategies* (16 times), such as updating software, using encrypted services, VPN, or turning off automatic downloading of apps and software. Only 5 times participants mentioned turning on *warnings and notices*, possibly because they do not protect against the risks *per se*, but rather provide transparency and inform users about the violations.

Almost half of the time, participants said that they do not know what smartphone settings would address their concerns. We discuss the implications of avoiding behaviors and participants' unawareness about the protection strategies in Section 5.

4.3 Awareness about the settings

To answer **RQ1a**, we asked participants to indicate, without looking at their phones, whether they believe various settings are an existing option on their smartphones (Q5). Overall, we founds that many participants were not aware of the existing settings or incorrectly believed to have access to the settings they don't have (Figure 1).

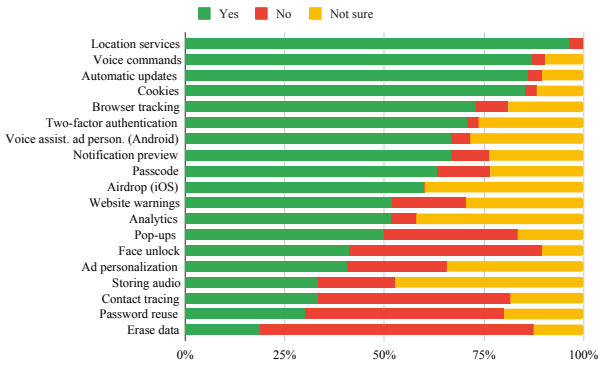

Figure 1: Awareness about the settings: participants' beliefs about whether the settings are an existing option on their smartphones (Q6).

Some participants had incorrect beliefs about what settings they have access to in their phones. For instance, erasing data from the phone after 10 failed passcode attempts is an existing setting on iOS, but only 20% of iOS users were aware of it. In contrast, this setting doesn't exist on Android, but about 20% of Android users incorrectly assumed they have such a setting. Similarly, half of Android users incorrectly believed they can turn on fraudulent website warnings in mobile Chrome browser, despite this feature not being currently available in Chrome.

Many participants were also not aware of the existing settings. Less than half of users were aware of their ability to opt out from storing audio recordings of their interactions with smartphone voice assistants, opt out from ad personalization, view passwords reused in their default mobile browser, and opt out from Bluetooth-enabled COVID contact tracing. Only about half of users were aware about the existing options to block pop-ups in the browser, and opt out of analytics. Only about 60% of users were aware of the seemingly common passcode feature for locking the smartphone screen.

Other settings were more familiar to the participants. For example, among those, who use face recognition to unlock the smartphone, about 70% of participants were aware of the setting that allows to use it only if they are looking at the screen. The majority of users were also aware of location services settings, automatic

[3]https://www.lookout.com, https://www.lifelock.com/, and https://www.malwarebytes.com.

updates, blocking of cookies and browser tracking, and control listening to voice assistant commands.

4.4 Beliefs about defaults

To answer **RQ1b**, we asked participants, if they just bought a phone and had not changed any settings yet, what do they think would be the default configuration of those settings (Q6). Most of the participants possess correct assumptions about the default settings limiting tracking practices in their smartphones, but many hold incorrect beliefs about the authentication and ad personalization settings defaults (Figure 2).

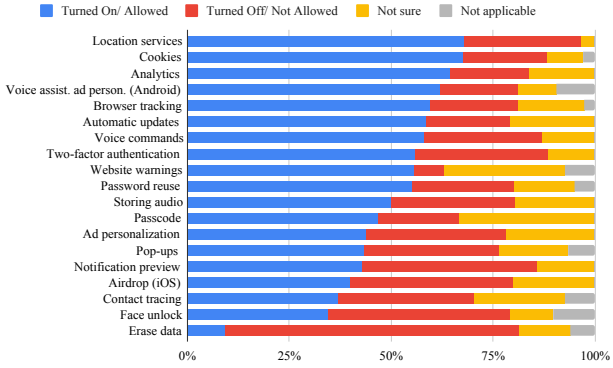

Figure 2: Beliefs about defaults: participants' beliefs about what are the settings' default configurations (Q6).

Some participant hold incorrect beliefs about the authentication settings. About half of participants believe that passcode is turned on by default, and even more believe that 2FA is on, although in reality they need to set up both features. Moreover, 55% of participants expect their default mobile browsers to notify them about passwords reused across different websites. In reality, while both Chrome and Safari browsers monitor it, users need to check such security recommendations in the settings, as no notification system has been implemented in these mobile browsers at the time of the study.

A quarter of both OS user groups possess incorrect beliefs about ad personalization practices in their mobile operating systems as well. Ad personalization practices differ between iOS and Android: iOS has started to require permission for ad personalization, which is otherwise disabled (i.e. to opt in), starting from the release of iOS 14 in fall 2020. In contrast, Android users are required to opt out of ad personalization, which is otherwise on by default.

However, most of the participants possess correct assumptions about tracking practices in their smartphones. Specifically, the majority of participants believe that analytics, cookies, and browser tracking is on by default; yet, about 20% of participants incorrectly believe it is off. Moreover, 37% of participants incorrectly believe that COVID contact tracing is enabled by default.

4.5 Past behaviors and intent to change the settings

To answer **RQ2** and **RQ3**, we asked participants if they have ever configured the settings on their smartphones (Q9; responses summarized in Figure 3) and whether they are willing to do it in the future (Q12; responses summarized in Figure 4), respectively. While many users said they haven't configured certain settings in the past, especially the ones they were not aware of, they were willing to do it in the future. It indicated the importance of settings discoverability on users' engagement with those settings.

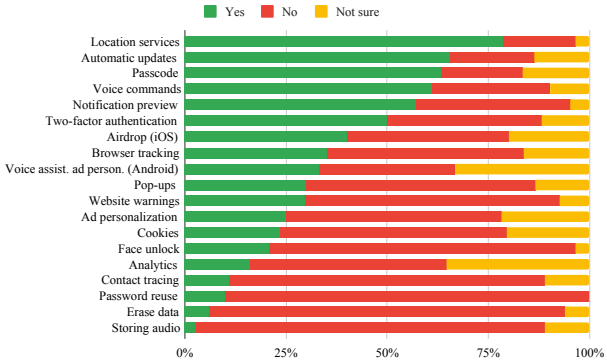

Figure 3: Past behaviors: whether participants have configured the settings in the past (Q9).

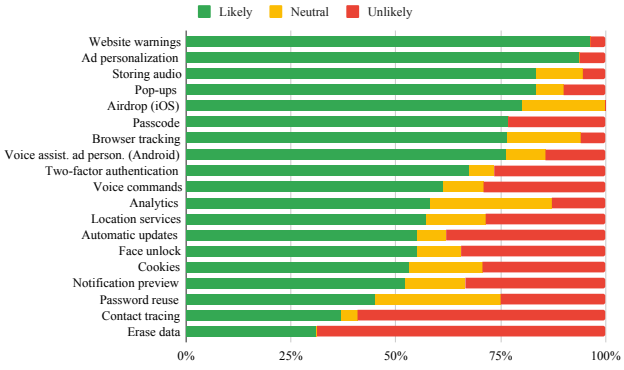

Figure 4: Intentions to configure the settings in the future (Q12).

We found that many participants have not configured such settings as erasing data after 10 failed passcode attempts, viewing passwords that have been re-used on other websites, enabling attention feature in face unlock, and disabling storing audio recordings of interactions with smartphone voice assistants. These are also the settings that many participants were not aware of, as shown in Figure 1. Although more than 80% of participants have not configured those settings, many said that they have intentions to do it in the future.

Similar trend is observed for the OS-specific settings: while 40% of iOS users have restricted sharing permissions in Airdrop, 80% said they are willing to do it in the future. Similarly, only 33.3% of Android users have opted out of voice assistant ad personalization, but 76.2% said they are willing to do it in the future. Interestingly, although Android users currently don't have access to the feature that erases data after 10 failed passcode attempts, 20% of them said they are willing to turn it on, if they had such a choice. Similarly, despite this setting is currently unavailable in Chrome browser, 94.4% of Android users said they would be willing to turn on fraudulent website warnings in Chrome if it was available. In contrast, although this option exists in Safari, 44.4% of iOS users have not turned it on. Yet, all iOS users said they are willing to enable fraudulent website warnings in the future.

Regarding online tracking, between 38% and 65% of participants have not blocked cookies, pop-ups, ad personalization, analytics, and browsing tracking on their smartphones in the past. Although participants don't intend to increase blocking cookies and analytics, many intend to limit ad personalization (93.8%) and browser tracking (76.5%), and block pop-ups in the future (83.3%).

Smaller proportion of users said they have not enabled private notification previews on their smartphones (38%), and have not disabled voice commands (30%). However, more than half of participants said they are willing to enable those settings in the future.

Past behaviors and future intentions are more aligned for the Bluetooth COVID contact tracing settings. Over 60% of participants said they have not enabled it on their smartphones in the past, and over half of participants are not willing to do it in the future either.

Finally, consistently positive past behaviors and future intentions are observed for the remaining settings. About 60-80% of participants have enabled automatic updates on their phones, created passcodes to unlock the phone, and disabled location services in the past, and are likely to use it in the future as well.

Factors influencing Behaviors. To answer **RQ6a**, we estimated the Odds Ratios (OR) for the statistically significant results ($p < 0.05$) based on the ordered logistic regression reported in Table 5 in Appendix A. We find that, on average, older participants configure the settings less than younger people by 2%. Hispanic/Latinx participants configure the settings 50% less than participants, who self-identify as White. Moreover, those, who anticipate difficulties with configuring the settings, or their negative impact on user experience, configure the settings less by 34% and 13%, respectively. People who primarily use Firefox mobile browser reported to have configured the settings 2.3 times more often than Chrome users. No significant effects were found for other variables, including for the level of smartphone skills.

Factors influencing Intentions. To answer **RQ6b**, we estimated the Odd Ratios (OR) for the statistically significant results ($p < 0.05$) based on the ordered logistic regression reported in Table 6 in Appendix A. We find that, overall, when controlled for demographics and smartphone usage characteristics (Model 2), Safari users are 58% less willing to configure settings than Chrome users ($p = .013$). Non-working students are 2.53 times more willing to configure settings than participants, who are employed at least part-time ($p = .004$). Participants, who have already configured smartphone settings in the past are 32% less willing to do it in the future ($p = .000$); this is not surprising since their settings are already configured according to their preferences (Model 3). Participants, who anticipate negative impact on their user experience still have positive intentions to change the settings in the future. No significant effects were found for other variables, including age, gender, education, income, race/ethnicity, and the level of smartphone skills.

4.6 Perceived difficulty of changing the settings

To answer **RQ4** we analyzed participants' responses about the perceived difficulty of changing the settings (Q7), which are summarized in Figure 5. In general, more than 60% of participants expect that it will be easy for them to configure the settings.

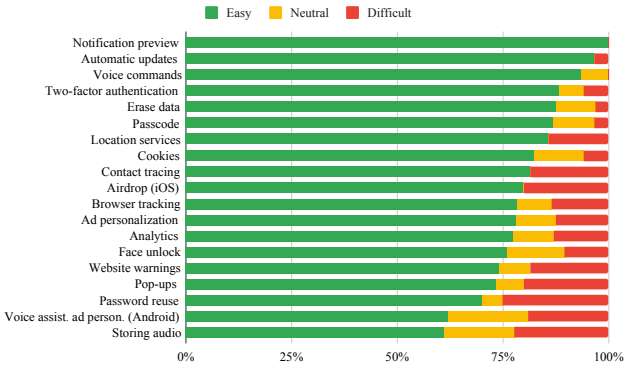

Figure 5: Perceived difficulty of configuring the settings (Q7).

No participants at all believe it will be hard to enable private notification previews or disable voice commands. Only about 3% of participants expect difficulties with enabling automatic updates and data erasure after 10 failed passcode attempts. Only a few participants also expect difficulties with disabling location services (14.3%) and with configuring the authentication settings, including 2FA (5.9%), attention features for face unlock (10.3%) and passcode for unlocking the screen (3.3%).

Regarding the tracking technologies, less than 20% of participants expect difficulties with disabling browser tracking, ad personalization, analytics, cookies, and Google voice assistant ad personalization.

Among the settings that least amount of users expect to be easy to configure, 19-25% of participants anticipate some difficulties with opting out of storing audio of their interactions with the smartphone, COVID contact tracing, and restricting Airdrop permissions, as well as configuring mobile browser settings (including blocking pop-ups, viewing reused passwords, and turning on fraudulent website warnings).

Factors influencing perceived difficulty. To answer **RQ6c**, we estimated the Odds Ratios (OR) for the statistically significant results ($p < 0.05$) based on the ordered logistic regression (Table 7 in Appendix A). We find that, overall, when considering only the demographics explanatory variables (Model 1), older participants expect configuring settings to be 1.6% more difficult than younger

participants (this effect, however, is not confirmed in Model 2 and 3, when we control for other factors). Compared to White, biracial participants perceive settings to be 3.24 more difficult to configure. Participants who use their current operating system for longer period of time or use smartphone more frequently are 37% and 63% less likely to expect difficulties with configuring the settings, respectively. Participants with less advanced smartphone skills, i.e. those who find it difficult to develop an app, also find it 23% more difficult to configure the settings.

Reasons for the perceived difficulty. We asked participants why they believe it will be difficult to configure the settings (Q8). Their responses fall into three main groups: anticipated difficulties with finding the setting, perceived lack of knowledge and experience, and technical limitations. Because some participants provided multiple reasons per setting, and for up to 3 different settings, we report occurrences (the number of times the reason was mentioned), instead of the number of people who mentioned it.

Among the anticipated **difficulties with finding the setting**, 22 times participants said they are *not sure where they should even start looking for it*, 17 times participants expected generally *poor information architecture* (e.g. confusing or complex structure of the settings menu with multiple subcategories, vague labels and explanations, and otherwise not intuitive user interface that is hard to navigate without researching additional information). Some participants specifically believe that *manufacturers made it intentionally hard to find and change the settings* (e.g. to maximize data collection and profit) and mentioned it 21 times. Interestingly, one participant complained that interface changes between the OS versions (e.g. the position of the location services settings) makes it even harder to find: *"Because it's buried and has been in several different locations in Android versions,"* (P4). Another participant acknowledged the difficulty of changing the privacy unfriendly defaults: *"Based on previous experience it has been complicated to change the presets on the phone,"* (P14).

The perceived **lack of knowledge and experience** was associated with *low familiarity with the specific setting* (12 times) (including unawareness of its existence or not being sure about how this setting works), *absence of experience with configuring the setting* in the past (9 times), and *generally low self-efficacy* often referred to as being "not tech savvy" (8 times). Interestingly, one participant raised concerns about not being able to assess the success in configuring the setting effectively: *"I am not sure how to limit activity tracking or if what I do would even be effective,"* (P63).

Technical limitations were mentioned only 6 times, when participants did not have either a particular setting in their OS version or smartphone model (e.g., facial recognition for unlocking the screen), or region (e.g., contact tracing not available in a particular state). Some participants lack other resources necessary for enabling a setting, such as phone or internet service to receive the second-factor code: *"Currently my phone service is off, and you can't configure two factor authentication without SMS or calls,"* (P26).

The rest of the reasons were classified as "other" and included 5 responses about the usefulness of keeping the setting enabled (rather than a reason why it would be difficult to disable), and 12 unclear or non-informative responses (e.g. "not sure", "I don't know", etc).

The distribution of reasons is not the same among the settings. note that participants were asked to explain the reason for difficulty only if they judged that setting difficult, thus the reported totals are different between settings. For most settings, anticipated difficulties with configuration are primarily associated with the hardship of finding the settings (e.g. regarding disabling storing audio recordings of the interactions with the smartphone voice assistants (11/14 times), and limiting ad-tracking (7/7 times)). In contrast, poor information architecture was mentioned in only 1 out of 7 responses about anticipated difficulties with enabling face recognition for unlocking the smartphone; instead, 3 times participants said they simply do not have this feature and 3 other times they didn't provide a clear reason for it. The usefulness of keeping the setting enabled was mentioned only for browser cookies (2/5 times), COVID contact tracing (2/6) times, and location services (1/4 times), and not any other settings.

4.7 Perceived impact of settings on user experience

To answer **RQ5a**, we asked participants how would the configuration of the settings affect their overall experience of using their smartphones—their user experience, or UX (Q11). Figure 6 summarizes the responses. Most participants anticipate positive impact on their user experience from limiting tracking and increasing browsing safety. However, some settings, such as erasing data after 10 failed passcode attempts, disabling location services, and hiding notifications previews would negatively affect the experience of many participants (29-38%) by limiting the important usability aspects of their everyday smartphone use.

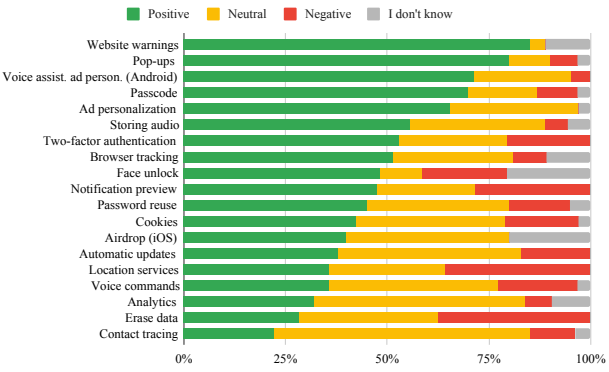

Figure 6: Perceived impact of settings on user experience (Q11).

Some participants (10-20%) expect negative UX impact also after configuring settings related to authentication, including enabling attention feature in face unlock, passcode to unlock the screen, 2FA, and viewing reused passwords.

In contrast, participants expect predominantly positive impact on their overall user experience after limiting tracking and increasing browsing safety, for example by enabling website warnings, limiting ad personalization on the web and in the Google voice assistant,

disabling pop-ups, browser tracking, and not allowing to store audio recordings of the interactions with the voice assistants.

Few participants have positive (and predominantly neutral) expectations regarding contact tracing, disabling analytics and voice commands, and enabling automatic updates.

Finally, about 20% of participants don't know how enabling attention feature for face unlock and limiting Airdrop sharing audience to contacts only would affect their user experience. Lack of such understanding may negatively affect the adoption of these features.

Factors influencing perceived impact of settings on user experience. To answer **RQ6d**, we estimated the Odds Ratios (OR) for the statistically significant results ($p < 0.05$) based on the ordered logistic regression (Table 8 in Appendix A). We find that, overall, biracial participants are 2.43 times more likely and participants who have longer experience with their current OS are 66% more likely to expect negative impact of configuring the settings on their UX. Those with the technical background are 37% less likely to expect the negative impact on UX.

4.8 Effectiveness of settings against risks

To answer **RQ5b**, we asked participants about the perceived effectiveness of the smartphone settings against the online privacy and security risks (Q13). Their responses are summarized in Table 3. Most participants hold correct beliefs about what settings are effective against the particular online risks. However, some settings (especially website warnings and anti-tracking features) are incorrectly mapped against the risks, which indicates incorrect threat models or wrong assumptions of what settings would protect against those risks. In this section we focus on those cases, as they indicate the especially useful areas for potential improvements.

Common incorrect beliefs are related to the website warnings. Many participants believe that website warnings would be effective against *unsolicited advertising* (59.3%), *harassment* (such as bullying, stalking, blackmailing, doxxing, or release of personal information online by someone) (51.9%), *unauthorized physical access* (51.9%), *data gathering by government* (33.3%), and *data gathering by individuals* (e.g. by intimate partner, family member, friend, etc.) (40.7%).

Anti-tracking settings also caused a lot of confusion. More than half of participants incorrectly believe that opting out of ad personalization would protect them against *unauthorized remote access* (e.g. in case of a hacking or ransomware attack, virus, or other malware) (56.3%) and *social engineering attacks* (e.g. scam, phishing) (65.6%). Despite limited ad personalization primarily affecting the *type* of ads rather than the *amount* of ads, many participants believe that it would protect them from *unsolicited advertising* (e.g. spam) (84.4%). Further, 41.2% of participants incorrectly believe that blocking cookies is effective against *social engineering attacks*,and many believe that disabling analytics would protect them against *unauthorized remote access* (35.5%) and *data gathering by government* (48.4%). Although ad libraries may indeed pose privacy and security risks [e.g., 3, 52, 68], disabling ad personalizationa and analytics alone does not protect against unauthorized remote access. Instead automatic software updates are considered to be effective against this risk by security experts [60].

Other settings were also associated with some occasional incorrect assumptions. For example, 40% of participants incorrectly believe that checking what passwords are reused on other websites would be effective against *harassment*. Almost a quarter (23.8%) of participants incorrectly believe that hiding notification preview when the phone is locked is not effective against *data gathering by companies*, and that blocking pop-ups (30.0%) are effective against *data gathering by individuals*. Over a third of participants incorrectly believe that 2FA (38.3%) and automatic updates (37.9%) are not effective against *unauthorized financial transactions*. Only 20% of iOS users believe that allowing solely the contacts to share files over Airdrop (instead of 'everyone') would be effective in protecting from *objectionable content* and *harassment*, although in reality it is an effective strategy.

4.9 Perceived worry about the risks

We asked participants how much they worry about various privacy and security risks (Q15). Overall participants are worried about all of the online risks mentioned in the survey (Table 4 in Appendix A). They worry the most about unauthorized financial transactions, inadvertent disclosure of information, unauthorized remote access, and data gathering by companies and governments. They worry less about data gathering by individuals, unsolicited objectionable content, harassment, and unsolicited advertising. Only up to 1.1% of participants are unfamiliar with the risks we asked about in the survey.

We also constructed an index of privacy and security concerns using factor analysis (with eigenvalue over 1, Cronbach's $alpha = .89$), and ran a regression on demographic and usage characteristics (Table 9 in Appendix A). We found that older, female, biracial (White-Hispanic/Latinx) participants, non-working students, participants with longer experience with their current OS, technical background, or who use face unlock are less concerned about privacy and security risks.

5 DISCUSSION AND CONCLUSIONS

Overall, our participants were aware of and concerned with privacy and security risks, but half of the time they did not know or possessed incorrect beliefs about what smartphone settings can protect them against these risks (Section 4.2), how effective they are (Section 4.8), whether they are available on their smartphones (Section 4.3), or what are their default configurations (Section 4.4). Many participants reported not having configured privacy and security settings on their phones, due to anticipated difficulties with configuring the settings and expected negative impact on user experience. However, many of them were willing to do it in the future, possibly because prior to the study they were simply not aware of those settings.

Some privacy and security settings may impose additional usability costs. For example, enabling two-factor-authentication or screen-locking passcode will require users to spend more time to log in or access their smartphone. Thus, after weighing the security benefits against the usability costs, users may decide to not enable certain settings. While users' *informed* decisions not to enable a privacy or security setting is completely valid, lack of understanding necessary to make these informed decisions is problematic. Our results show that all participants were worried about all the online risks, but many did not know how to address them, or incorrectly

Table 3: Perceived ineffectiveness of privacy and security settings against the risks (Q13). The responses were rated on a 7-point Likert scale (from 1 'Very Effective' to 7 'Very Ineffective'; "I don't know" responses are excluded from this table). In the table, green color represents the settings that were deemed effective against the risks (mean>4), and red represents the settings that were deemed ineffective (mean<4).

Settings	Mean scores of effectiveness against risks										
	Data gather. by companies	Data gather. by governments	Data gather. by individuals	Spam	Objectionable content	Harassment	Scam	Financial risks	Physical access	Remote access	Personal data disclosure
Location	2.93	4.29	3.59	4.29	5.12	3.85	4.38	4.93	4.76	4.68	3.93
Audio storing	2.92	3.26	3.31	3.58	4.58	4.45	3.75	4.09	4.68	4.31	2.78
Ad tracking	2.10	4.07	4.13	2.29	3.58	4.66	3.20	4.10	4.65	4.10	2.45
2FA	5.00	4.81	3.06	5.19	4.88	4.33	3.91	3.27	2.94	2.53	3.56
Password reuse	4.95	5.32	3.80	5.11	4.84	4.58	3.89	3.05	4.53	3.42	3.47
Notification preview	5.26	5.25	2.57	4.95	4.11	4.25	4.11	3.53	3.10	4.59	2.50
Updates	4.70	4.84	4.68	4.89	4.63	5.00	4.28	3.96	4.48	2.85	3.89
Airdrop	4.25	4.75	5.50	4.25	4.00	4.00	5.00	4.75	4.25	2.75	5.25
Popups	3.10	4.66	4.87	2.47	3.67	4.79	3.13	3.59	4.77	3.45	3.57
Voice commands	3.19	3.63	3.76	3.71	4.33	4.67	4.26	4.19	4.50	4.00	2.87
Passcode	5.13	5.00	3.77	5.29	5.31	4.45	4.92	2.90	2.31	4.33	4.07
Face unlock	5.41	5.68	2.74	5.70	5.35	4.74	5.08	3.38	1.58	4.24	3.92
Tracking	2.59	3.67	3.52	3.79	4.52	4.29	4.15	4.13	4.49	4.19	3.28
Warning	3.28	4.38	4.08	3.28	3.16	3.88	2.41	2.33	3.85	3.12	2.58
Analytics	3.03	4.00	4.07	4.07	4.58	4.67	4.13	4.69	4.81	4.07	3.19
Contact tracing	3.56	3.07	3.56	4.44	4.92	4.08	5.08	4.83	4.56	4.84	3.46
Erase data	5.32	4.84	2.52	5.56	5.72	4.50	4.90	3.72	2.06	4.21	3.74
Cookies	2.26	3.50	3.93	2.94	4.45	4.48	3.97	3.80	4.94	4.00	3.06
Voice assist. ad track.	2.00	4.40	3.95	2.30	3.90	5.05	3.62	4.86	5.40	4.86	2.67

assumed that they are already addressed by default. Low comprehension of the threat models and strategies for mitigating the risks, and low awareness of the settings and their defaults may lead to users' overconfidence, insufficient vigilance in assessing and insufficient effort in protection against the potential harm from online privacy and security risks. These conditions can eventually lead to users' inadequate protection against those risks. Thus, we argue that it is not enough to just offer privacy and security settings in the smartphones. It is also important to provide the appropriate level of user education about the settings and what risks they aim to mitigate.

Participants often proposed to rely on the strategies aiming at *avoiding* risky behaviors rather than deploying more reliable privacy or security protections (Section 4.2). First, it means that unaddressed privacy and security concerns may lead users to simply limit their activities (e.g. avoiding downloading apps, visiting certain websites, using online payments, etc.), resulting in negative economic effects. Similar conclusions were reached in [22] about older adults limiting their online activities due to privacy and security concerns. Thus, ensuring privacy and security should be prioritised by the technological companies if they want users to continue using their devices and services, and not limit their activities due to privacy and security concerns. Second, avoiding suspicious websites or apps may not be effective in protecting against the risks, as they depend on users' ability to recognise such suspicious content. Moreover, insecure networks or certain activities (like online banking) may be hard to avoid in certain situations, for example when travelling or if there is no access to a safer alternative at home. Thus, users need to be better informed about the effective strategies for protecting their personal data without necessarily limiting their online activities. Moreover, some participants (especially among iOS users) incorrectly mapped smartphone settings against the risks (Section 4.8), suggesting that users lack understanding of threat models or privacy/security implications of various settings. Future work is called to investigate users' mental models about smartphone privacy and security settings and identify reasons for misconceptions about their effectiveness against certain online risks.

While on average, more than half of participants expected settings to be easy to configure, up to a third of participants anticipated difficulties with these tasks, due to poor information architecture,

lack of experience and knowledge, or technical limitations, such as limited phone service or regional restrictions (Section 4.6). These findings are in line with Ramokapane et al. [58]. Interestingly, many participants believe that manufacturers and service providers make the settings hard to find on purpose and set privacy unfriendly defaults in order to maximize their revenue. Such beliefs undermine users' trust in manufacturers' good intentions. Thus, by making settings easy to find and configure, smartphone manufacturers will not only protect users' privacy and security, but also build trust relationship with them and possibly obtain a competitive advantage over less privacy-concerned competitors. Finally, some participants expected negative impact from disabling location services, and configuring authentication settings (and thus making the authentication process more cumbersome or long) and other settings on their overall user experience with the smartphone. Thus, users expect usability issues not only during search and configuration of privacy and security settings, but also during their use.

5.1 Socio-demographic differences

With respect to RQ6, specifically, we found some differences among socio-demographic groups' perspectives on smartphone privacy and security settings. Specifically, higher age is associated with less frequent engagement with privacy and security settings, elevated expectations of difficulties with configuring them, and lower concern about privacy and security risks. This evidence supports prior findings about older adults being less aware of online risks [23, 24] and engaging less in privacy- and security-protective behaviors than younger users [70, 76].

Hispanic/Latinx participants reported less frequent engagement with privacy and security settings. Biracial participants had less privacy and security concerns, and were more likely to expect difficulties with configuring smartphone privacy and security settings and their negative impact on user experience. Females were also less concerned about privacy and security risks. Finally, we found that participants, who use their smartphone less frequently (e.g. once a day vs multiple times a day) anticipate more difficulties with configuring the settings, and users who anticipate such difficulties engage less in configuring privacy and security settings on their smartphones.

Interestingly, we found that age and race/ethnicity have a statistically significant impact on the past behaviors of configuring the smartphone privacy and security settings (RQ6a), but not on the intentions to do so in the future (RQ6b). It can be related to the fact that various socio-demographic groups may be similarly willing to configure their privacy and security settings, but differences in self-efficacy, smartphone experience, knowledge and skills prevents some of them from actually enabling the settings. Future work can empirically validate this hypothesis and further explore the impact of other socio-demographic and socio-economic factors on privacy and security behaviors and experiences.

These findings suggest that certain socio-demographic groups may feel less prepared or willing to use smartphone settings to protect their information privacy and security. Thus, user education and interventions increasing the perceived self-efficacy are especially important for infrequent users and those with low esteem of their personal technical abilities.

5.2 Recommendations

It is important to address the issues with awareness and discoverability, especially for the demographic groups that struggle with it the most. Given its popularity [65], smartphones could be a useful point of intervention for educating users about available privacy and security protections. Instead of relying on users to find the settings on their own, mobile operating systems could design prompts that would periodically remind users about the available settings. For example, Google[4] and Facebook[5] offer Privacy Checkups that guide users through the available settings and explain the different options. We recommend similar checkups to be used in smartphones as well.

In addition to informing users about the availability of settings, it is important to further address the comprehension of the implications of the settings configurations. For example, user interfaces of the settings menus could be improved to communicate more clearly against what risks each of the settings protect users, and how it may affect their user experience, as many of our participants were not sure about such implications. These modifications would improve the transparency about the privacy and security implications of each setting and help users evaluate the potential trade-offs between protection and convenience, and eventually make more informed decisions. Prior work has repeatedly shown the relevance of such trade-offs in smartphone applications [6, 61] and even IoT devices [63].

To further improve usability, our results suggest manufacturers to set privacy friendly defaults and in case of interface or labelling changes between the OS versions, inform users about them. We also encourage manufacturers to clearly say what additional resources (e.g. 2FA token, Internet connection, updating to the next software version) are required in order to enable certain privacy/security settings, and what are the alternatives (e.g. using SMS as the second factor if users do not have stable mobile Internet connection to receive it over email).

To address the misconceptions about effectiveness, as several participants acknowledged, feedback loop about whether the configured settings are effective in protecting them would increases the perceived usefulness of those settings, and further increase user trust in manufacturer's good intentions and attempts at protecting users' personal information. Feedback loops has been shown effective in security domain, such as in antivirus [29] and IoT [32] technologies.

Moreover, we encourage future research and smartphone manufacturers to engage diverse groups of people in user studies to refine wording and information architecture of the privacy and security settings. Future research is called to develop generalizable recommendations for effective privacy and security settings design, relying on empirical evidence, benchmarketing, and existing Human-Computer Interaction (HCI) guidelines [e.g., 38, 51, 71].

We found some evidence of differences in opinions about smartphone privacy and security settings among socio-demographic groups. We encourage future research to ensure the diversity of their participant pools to further investigate the differences, and

[4]https://myaccount.google.com/intro/privacycheckup?hl=en
[5]https://www.facebook.com/help/443357099140264

possibly include the exploration of cultural differences. We also recommend considering the identified differences in tailoring the information and education materials for vulnerable socio-demographic groups. Prior work on privacy and security attitudes and behaviors of those groups can also be useful in tailoring the materials (e.g. see [64] about lower income populations, [22, 23, 53] about older adults, [4, 20] about foster youth, etc.).

ACKNOWLEDGMENTS

This work was supported by by a grant from the Center for Long-Term Cybersecurity (CLTC) at U.C. Berkeley, by National Science Foundation grants CNS-1514211 and CNS-1528070, by the National Security Agency's Science of Security program. Opinions, findings, and conclusions are those of the authors and do not necessarily reflect the views of the funders.

REFERENCES

[1] Keith B Anderson. 2004. *Consumer fraud in the United States: An FTC survey.* Federal Trade Commission.

[2] Mohd Anwar, Wu He, Ivan Ash, Xiaohong Yuan, Ling Li, and Li Xu. 2017. Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior* 69 (2017), 437–443.

[3] Michael Backes, Sven Bugiel, and Erik Derr. 2016. Reliable third-party library detection in android and its security applications. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. 356–367.

[4] Karla Badillo-Urquiola, Scott Harpin, and Pamela Wisniewski. 2017. Abandoned but not forgotten: Providing access while protecting foster youth from online risks. In *Proceedings of the 2017 Conference on Interaction Design and Children*. 17–26.

[5] Tara S Behrend, David J Sharek, Adam W Meade, and Eric N Wiebe. 2011. The viability of crowdsourcing for survey research. *Behavior research methods* 43, 3 (2011), 800–813.

[6] Alastair R Beresford, Andrew Rice, Nicholas Skehin, and Ripduman Sohan. 2011. Mockdroid: trading privacy for application functionality on smartphones. In *Proceedings of the 12th workshop on mobile computing systems and applications*. 49–54.

[7] Rasekhar Bhagavatula, Blase Ur, Kevin Iacovino, Su Mon Kywe, Lorrie Faith Cranor, and Marios Savvides. 2015. Biometric authentication on iphone and android: Usability, perceptions, and influences on adoption. (2015).

[8] Tom Biselli and Christian Reuter. 2021. On the Relationship between IT Privacy and Security Behavior: A Survey among German Private Users. (2021).

[9] Frank Breitinger, Ryan Tully-Doyle, and Courtney Hassenfeldt. 2020. A survey on smartphone user's security choices, awareness and education. *Computers & Security* 88 (2020), 101647.

[10] Jean Camp and Kay Connelly. 2008. Beyond consent: Privacy in ubiquitous computing (Ubicomp). *Digital Privacy: Theory, Technologies, and Practices* (2008), 327–343.

[11] BD Carpenter and S Buday. 2007. Computer use among older adults in a naturally occurring retirement community. *Computers in Human Behavior* 23, 6 (2007), 3012–3024.

[12] Robert E Crossler and France Bélanger. 2019. Why Would I Use Location-Protective Settings on My Smartphone? Motivating Protective Behaviors and the Existence of the Privacy Knowledge–Belief Gap. *Information Systems Research* 30, 3 (2019), 995–1006.

[13] Device Atlas. 2019. Android v iOS market share 2019. (2019). https://deviceatlas.com/blog/android-v-ios-market-share#us Accessed 11 February 2021.

[14] Device Atlas. 2019. The most popular mobile browsers. (2019). https://deviceatlas.com/blog/the-most-popular-mobile-browsers Accessed 11 January 2021.

[15] Kerry Dobransky and Eszter Hargittai. 2016. Unrealized potential: Exploring the digital disability divide. *Poetics* 58 (2016), 18–28.

[16] Serge Egelman, Adrienne Porter Felt, and David Wagner. 2013. Choice architecture and smartphone privacy: There'sa price for that. In *The economics of information security and privacy*. Springer, 211–236.

[17] Serge Egelman, Sakshi Jain, Rebecca S Portnoff, Kerwell Liao, Sunny Consolvo, and David Wagner. 2014. Are you ready to lock?. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. 750–761.

[18] Peer Eyal, Rothschild David, Gordon Andrew, Evernden Zak, and Damer Ekaterina. 2021. Data quality of platforms and panels for online behavioral research. *Behavior Research Methods* (2021), 1–20.

[19] Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. 2012. Android permissions: User attention, comprehension, and behavior. In *Proceedings of the eighth symposium on usable privacy and security*. 1–14.

[20] Dale Fitch. 2012. Youth in foster care and social media: A framework for developing privacy guidelines. *Journal of Technology in Human Services* 30, 2 (2012), 94–108.

[21] Joshua Fogel and Elham Nehmad. 2009. Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in human behavior* 25, 1 (2009), 153–160.

[22] Alisa Frik, Leysan Nurgalieva, Julia Bernd, Joyce Lee, Florian Schaub, and Serge Egelman. 2019. Privacy and security threat models and mitigation strategies of older adults. In *Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019)*.

[23] V. Garg, L. Lorenzen-Huber, L. J. Camp, and K. Connelly. 2012. Risk Communication Design for Older Adults. *Gerontechnology* 11, 2 (2012), 166–173.

[24] Galen A Grimes, Michelle G Hough, Elizabeth Mazur, and Margaret L Signorella. 2010. Older adults' knowledge of Internet hazards. *Educational Gerontology* 36, 3 (2010), 173–192.

[25] Galen A Grimes, Michelle G Hough, and Margaret L Signorella. 2007. Email end users and spam: Relations of gender and age group to attitudes and actions. *Computers in Human Behavior* 23, 1 (2007), 318–332.

[26] Tamy Guberek, Allison McDonald, Sylvia Simioni, Abraham H Mhaidli, Kentaro Toyama, and Florian Schaub. 2018. Keeping a low profile? Technology, risk and privacy among undocumented immigrants. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–15.

[27] Michael Haight, Anabel Quan-Haase, and Bradley A Corbett. 2014. Revisiting the digital divide in Canada: The impact of demographic factors on access to the Internet, level of online activity, and social networking site usage. *Information, Communication & Society* 17, 4 (2014), 503–519.

[28] Amber M Hamilton. 2020. A genealogy of critical race and digital studies: Past, present, and future. *Sociology of Race and Ethnicity* 6, 3 (2020), 292–301.

[29] Ryan Hand, Michael Ton, and Eric Keller. 2013. Active security. In *Proceedings of the Twelfth ACM Workshop on Hot Topics in Networks*. 1–7.

[30] Marian Harbach, Emanuel Von Zezschwitz, Andreas Fichtner, Alexander De Luca, and Matthew Smith. 2014. It's a hard lock life: A field study of smartphone (un) locking behavior and risk perception. In *10th Symposium On Usable Privacy and Security ({SOUPS} 2014)*. 213–230.

[31] Eszter Hargittai and Eden Litt. 2013. New strategies for employment? Internet skills and online privacy practices during people's job search. *IEEE Security & Privacy* 11, 3 (May 2013), 38–45. https://doi.org/10.1109/MSP.2013.64

[32] Christina Hochleitner, Cornelia Graf, Dominik Unger, Manfred Tscheligi, and ICTS Center. 2012. Making devices trustworthy: Security and trust feedback in the internet of things. In *Fourth International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use (IWSSI/SPMU)*.

[33] Robert V Hogg, Elliot A Tanis, and Dale L Zimmerman. 1977. *Probability and statistical inference*. Vol. 993. Macmillan New York.

[34] Michelle G Hough. 2004. Exploring elder consumers interactions with information technology. *Journal of Business & Economics Research (JBER)* 2, 6 (2004).

[35] Qatrunnada Ismail, Tousif Ahmed, Kelly Caine, Apu Kapadia, and Michael Reiter. 2017. To permit or not to permit, that is the usability question: Crowdsourcing mobile apps' privacy permission settings. *Proceedings on Privacy Enhancing Technologies* 2017, 4 (2017), 119–137.

[36] Markus Jakobsson, Elaine Shi, Philippe Golle, and Richard Chow. 2009. Implicit authentication for mobile devices. In *Proceedings of the 4th USENIX conference on Hot topics in security*, Vol. 1. USENIX Association, 25–27.

[37] Ortaliza Jared, Giorlando Ramirez, Venkatesh Satheeskumar, and Krutika Amin. [n.d.]. ([n. d.]).

[38] Eric J Johnson, Suzanne B Shu, Benedict GC Dellaert, Craig Fox, Daniel G Goldstein, Gerald Häubl, Richard P Larrick, John W Payne, Ellen Peters, David Schkade, et al. 2012. Beyond nudges: Tools of a choice architecture. *Marketing Letters* 23, 2 (2012), 487–504.

[39] Sydney Jones and Susannah Fox. 2009. *Generations online in 2009*. Technical Report. Pew Internet & American Life Project, Washington, DC.

[40] Patrick Gage Kelley, Sunny Consolvo, Lorrie Faith Cranor, Jaeyeon Jung, Norman Sadeh, and David Wetherall. 2012. A conundrum of permissions: installing applications on an android smartphone. In *International conference on financial cryptography and data security*. Springer, 68–79.

[41] Patrick Gage Kelley, Lorrie Faith Cranor, and Norman Sadeh. 2013. Privacy as part of the app decision-making process. In *Proceedings of the SIGCHI conference on human factors in computing systems*. 3393–3402.

[42] Paul E Ketelaar and Mark Van Balen. 2018. The smartphone as your follower: The role of smartphone literacy in the relation between privacy concerns, attitude and behaviour towards phone-embedded tracking. *Computers in Human Behavior* 78 (2018), 174–182.

[43] Lawrence L Kupper and Kerry B Hafner. 1989. On assessing interrater agreement for multiple attribute responses. *Biometrics* (1989), 957–967.

[44] Jialiu Lin, Shahriyar Amini, Jason I Hong, Norman Sadeh, Janne Lindqvist, and Joy Zhang. 2012. Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. In *Proceedings of the 2012 ACM*

conference on ubiquitous computing. 501–510.

[45] Jialiu Lin, Bin Liu, Norman Sadeh, and Jason I Hong. 2014. Modeling users' mobile app privacy preferences: Restoring usability in a sea of permission settings. In *10th Symposium On Usable Privacy and Security ({SOUPS} 2014)*. 199–212.

[46] Bin Liu, Mads Schaarup Andersen, Florian Schaub, Hazim Almuhimedi, Shikun Aerin Zhang, Norman Sadeh, Yuvraj Agarwal, and Alessandro Acquisti. 2016. Follow my recommendations: A personalized privacy assistant for mobile app permissions. In *Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016)*. 27–41.

[47] Bin Liu, Jialiu Lin, and Norman Sadeh. 2014. Reconciling mobile app privacy and usability on smartphones: Could user privacy profiles help?. In *Proceedings of the 23rd international conference on World wide web*. 201–212.

[48] David Machin, Michael J Campbell, Say Beng Tan, and Sze Huey Tan. 2018. *Sample sizes for clinical, laboratory and epidemiology studies*. John Wiley & Sons.

[49] Mary Madden. 2017. Privacy, security, and digital inequality: How technology experiences and resources vary by socioeconomic status, race, and ethnicity. *Data & Society, Sep* (2017).

[50] Nicholas Micallef, Mike Just, Lynne Baillie, Martin Halvey, and Hilmi Güneş Kayacik. 2015. Why aren't users using protection? investigating the usability of smartphone locking. In *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services*. 284–294.

[51] Robert Münscher, Max Vetter, and Thomas Scheuerle. 2016. A review and taxonomy of choice architecture techniques. *Journal of Behavioral Decision Making* 29, 5 (2016), 511–524.

[52] Patrick Mutchler, Adam Doupé, John Mitchell, Chris Kruegel, and Giovanni Vigna. 2015. A large-scale study of mobile web app security. In *Proceedings of the Mobile Security Technologies Workshop (MoST)*. 50.

[53] Leysan Nurgalieva, Alisa Frik, Francesco Ceschel, Serge Egelman, and Maurizio Marchese. 2019. Information design in an aged care context: Views of older adults on information sharing in a care triad. In *Proceedings of the 13th EAI international conference on pervasive computing technologies for healthcare*. 101–110.

[54] Gizem Öğütçü, Özlem Müge Testik, and Oumout Chouseinoglou. 2016. Analysis of personal information security behavior and awareness. *Computers & Security* 56 (2016), 83–93.

[55] Yong Jin Park. 2013. Digital Literacy and Privacy Behavior Online. *Communication Research* 40, 2 (2013), 215–236. https://doi.org/10.1177/0093650211418338

[56] Yong Jin Park, Scott W Campbell, and Nojin Kwak. 2012. Affect, cognition and reward: Predictors of privacy protection online. *Computers in Human Behavior* 28, 3 (2012), 1019–1027.

[57] Eyal Peer, Laura Brandimarte, Sonam Samat, and Alessandro Acquisti. 2017. Beyond the Turk: Alternative platforms for crowdsourcing behavioral research. *Journal of Experimental Social Psychology* 70 (2017), 153–163.

[58] Kopo M Ramokapane, Anthony C Mazeli, and Awais Rashid. 2019. Skip, Skip, Skip, Accept!!!: A Study on the Usability of Smartphone Manufacturer Provided Default Features and User Privacy. *Proc. Priv. Enhancing Technol.* 2019, 2 (2019), 209–227.

[59] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. 2017. Where is the digital divide? a survey of security, privacy, and socioeconomics. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 931–936.

[60] Elissa M Redmiles, Noel Warford, Amritha Jayanti, Aravind Koneru, Sean Kross, Miraida Morales, Rock Stevens, and Michelle L Mazurek. 2020. A comprehensive quality evaluation of security and privacy advice on the web. In *29th {USENIX} Security Symposium ({USENIX} Security 20)*. 89–108.

[61] Scott J Savage and Donald M Waldman. 2015. Privacy tradeoffs in smartphone applications. *Economics Letters* 137 (2015), 171–175.

[62] Kim Bartel Sheehan. 1999. An investigation of gender differences in on-line privacy concerns and resultant behaviors. *Journal of Interactive Marketing* 13, 4 (1999), 24–38.

[63] Rayman Preet Singh, Benjamin Cassell, Srinivasan Keshav, and Tim Brecht. 2018. TussleOS: Managing privacy versus functionality trade-offs on IoT devices. *ACM SIGCOMM Computer Communication Review* 46, 3 (2018), 1–8.

[64] Manya Sleeper, Tara Matthews, Kathleen O'Leary, Anna Turner, Jill Palzkill Woelfer, Martin Shelton, Andrew Oplinger, Andreas Schou, and Sunny Consolvo. 2019. Tough Times at Transitional Homeless Shelters: Considering the Impact of Financial Insecurity on Digital Security and Privacy. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–12.

[65] StatCounter. 2020. Mobile Operating System Market Share United States Of America. (2020). https://gs.statcounter.com/os-market-share/mobile/united-states-of-america/2020 Accessed 11 January 2021.

[66] StatCounter. 2020. Mobile Operating System Market Share United States of America. (2020). https://gs.statcounter.com/os-market-share/mobile/united-states-of-america/2020 Accessed 11 January 2021.

[67] Statista. [n.d.]. U.S. smartphone market – Statistics and Facts. ([n. d.]). https://www.statista.com/topics/2711/us-smartphone-market/

[68] Ryan Stevens, Clint Gibler, Jon Crussell, Jeremy Erickson, and Hao Chen. 2012. Investigating user privacy in android ad libraries. In *Workshop on Mobile Security Technologies (MoST)*, Vol. 10. Citeseer.

[69] Javelin Strategy. 2009. Latest Javelin Research Shows Identity Fraud Increased 22 Percent, Affecting Nearly Ten Million Americans: But Consumer Costs Fell Sharply by 31 Percent. *press release. February* 9 (2009).

[70] Jiang Tao and Hu Shuijing. 2016. The Elderly and the Big Data: How Older Adults Deal with Digital Privacy. In *2016 International Conference on Intelligent Transportation, Big Data & Smart City*. IEEE, 285–288.

[71] Richard H Thaler, Cass R Sunstein, and John P Balz. 2013. Choice architecture. *The behavioral foundations of public policy* (2013), 428–439.

[72] Sabine Trepte, Tobias Dienlin, and Leonard Reinecke. 2014. Risky behaviors: How online experiences influence privacy behaviors. *Von Der Gutenberg-Galaxis Zur Google-Galaxis. From the Gutenberg Galaxy to the Google Galaxy* (2014).

[73] Daniel Vecchiato, Marco Vieira, and Eliane Martins. 2015. A security configuration assessment for android devices. In *Proceedings of the 30th Annual ACM Symposium on Applied Computing*. 2299–2304.

[74] Michel Walrave, Ini Vanwesenbeeck, and Wannes Heirman. 2012. Connecting and protecting? Comparing predictors of self-disclosure and privacy settings use between adolescents and adults. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 6, 1 (2012).

[75] Alma Whitten and J Doug Tygar. 1999. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0.. In *USENIX Security Symposium*, Vol. 348. 169–184.

[76] Eva-Maria Zeissig, Chantal Lidynia, Luisa Vervier, Andera Gadeib, and Martina Ziefle. 2017. Online privacy perceptions of older adults. In *International Conference on Human Aspects of IT for the Aged Population*. Springer, 181–200.

[77] Yun Zhou, Alexander Raake, Tao Xu, and Xuyun Zhang. 2017. Users' perceived control, trust and expectation on privacy settings of smartphone. In *International Symposium on Cyberspace Safety and Security*. Springer, 427–441.

[78] Kathryn Zickuhr and Mary Madden. 2012. *Older adults and Internet use*. Technical Report. Pew Internet & American Life Project.

A DESCRIPTIVE RESULTS AND LOGISTIC REGRESSION ANALYSIS

Table 4: Perceived worry about the privacy and security risks (Q15 in the survey; 7-point Likert scale). Mean values exclude "I'm not familiar with this risk" responses.

		Frequency of responses, %			
Risk	Mean	Unconcerned	Neutral	Concerned	Unfamiliar
Data gathering by individuals	4.30	35.96	12.36	51.12	0.56
Unsolicited objectionable content	4.48	29.21	16.85	52.81	1.12
Harassment	4.52	31.46	14.04	54.49	0.00
Unsolicited advertising (e.g. spam)	4.78	21.35	17.42	62.24	0.00
Social engineering attacks (e.g. scam, phishing)	5.15	16.29	8.99	74.16	0.56
Unauthorized physical access to (and control over) the device	5.22	20.22	6.74	73.03	0.00
Data gathering by governments	5.42	11.80	11.24	75.84	1.12
Data gathering by companies (e.g. for marketing purposes, selling data)	5.46	11.24	8.43	80.34	0.00
Unauthorized remote access to (and control over) the device	5.55	14.04	4.49	80.90	0.56
Inadvertent disclosure of personal information	5.87	6.74	4.49	87.64	1.12
Unauthorized financial transactions	5.99	7.87	3.93	88.20	0.00

Table 5: Logistic regression on whether participants configured settings in the past ($N = 178$). Q9 in the survey.

	(1)	(2)	(3)
Age	-0.0252**	-0.0222*	-0.0206*
	[-0.04,-0.01]	[-0.04,-0.00]	[-0.04,-0.00]
Gender (Male omitted)			
Female	0.00620	0.116	0.0305
	[-0.37,0.38]	[-0.28,0.51]	[-0.39,0.45]
Other	-0.169	-0.0243	-0.181
	[-2.65,2.31]	[-2.77,2.72]	[-2.94,2.57]
Non-disclosed	0.410	0.544	0.416
	[-1.49,2.31]	[-1.51,2.60]	[-1.76,2.59]
Race/ethnicity (White omitted)			
Biracial: White and Hispanic/Latinx	-0.0218	-0.0471	-0.155
	[-0.71,0.66]	[-0.74,0.65]	[-0.88,0.57]
Hispanic/Latinx	-0.709**	-0.697*	-0.691*
	[-1.24,-0.18]	[-1.25,-0.15]	[-1.27,-0.11]
Asian	-0.213	-0.240	-0.0613
	[-0.76,0.33]	[-0.80,0.32]	[-0.66,0.54]
Black	-0.345	-0.346	-0.339
	[-0.89,0.20]	[-0.92,0.22]	[-0.94,0.26]
Other biracial	-0.00415	-0.0568	0.454
	[-0.84,0.84]	[-0.90,0.79]	[-0.51,1.42]
Other or non-disclosed	-0.184	-0.229	-0.271
	[-1.15,0.78]	[-1.26,0.80]	[-1.34,0.79]
Education	-0.0299	-0.0563	-0.0435
	[-0.18,0.12]	[-0.22,0.10]	[-0.21,0.12]
Income	-0.00511	-0.00856	-0.0262
	[-0.10,0.09]	[-0.10,0.09]	[-0.13,0.07]
iOS users (Android users omitted)		-0.142	-0.220
		[-0.88,0.60]	[-0.99,0.55]
Duration of experience with current OS		0.156	0.120
		[-0.33,0.65]	[-0.40,0.64]
Frequency of smartphone use		0.183	-0.161
		[-0.91,1.28]	[-1.29,0.97]
Browser (Chrome omitted)			
Safari		0.236	0.258
		[-0.54,1.02]	[-0.55,1.07]
Firefox		0.797*	0.831*
		[0.10,1.49]	[0.09,1.57]
DuckDuckGo		0.184	-0.0115
		[-0.81,1.18]	[-1.04,1.02]
Other		0.126	0.395
		[-0.64,0.89]	[-0.44,1.23]
Use of face recognition to unlock		-0.00333	0.000251
		[-0.16,0.15]	[-0.16,0.16]
Technical background		0.319	0.119
		[-0.10,0.74]	[-0.33,0.57]
Perceived difficulty to configure settings			-0.416***
			[-0.56,-0.27]
Perceived negative impact of settings on UX			-0.135*
			[-0.26,-0.01]
χ^2	31.02*	39.65*	75.87***

95% confidence intervals in brackets
$^{+}$ $p < 0.1$, * $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Table 6: Ordered logistic regression on intentions to configure settings ($N = 178$). Q12 in the survey.

	(1)	(2)	(3)
Age	0.00462	0.00186	0.000953
	[-0.01,0.02]	[-0.01,0.02]	[-0.02,0.02]
Gender (Male omitted)			
Female	0.129	0.0261	0.166
	[-0.21,0.47]	[-0.33,0.38]	[-0.23,0.56]
Other	0.263	-0.297	0.673
	[-1.78,2.30]	[-2.60,2.01]	[-1.59,2.93]
Non-disclosed	-1.257	-1.539	-0.334
	[-3.83,1.31]	[-4.21,1.14]	[-3.00,2.33]
Race/ethnicity (White omitted)			
Biracial: White and Hispanic/Latinx	0.515	0.522	0.381
	[-0.13,1.16]	[-0.13,1.17]	[-0.29,1.05]
Hispanic/Latinx	0.143	0.125	-0.0505
	[-0.33,0.61]	[-0.36,0.61]	[-0.58,0.48]
Asian	-0.264	-0.330	-0.521^{+}
	[-0.76,0.23]	[-0.84,0.18]	[-1.08,0.04]
Black	0.0109	-0.0460	0.0393
	[-0.47,0.50]	[-0.55,0.46]	[-0.51,0.59]
Other biracial	0.279	0.433	-0.205
	[-0.49,1.05]	[-0.35,1.21]	[-1.05,0.64]
Other or non-disclosed	-0.595	-0.801^{+}	-0.679
	[-1.42,0.23]	[-1.68,0.08]	[-1.68,0.32]
Education	0.0552	0.0429	0.0274
	[-0.08,0.19]	[-0.10,0.19]	[-0.13,0.18]
Income	-0.0452	-0.0371	0.00168
	[-0.13,0.04]	[-0.12,0.05]	[-0.09,0.09]
iOS users (Android users omitted)		0.494	0.205
		[-0.15,1.14]	[-0.49,0.90]
Duration of experience with current OS		0.270	-0.00000645
		[-0.10,0.64]	[-0.40,0.40]
Frequency of smartphone use		-0.562	0.360
		[-1.57,0.44]	[-0.84,1.56]
Browser (Chrome omitted)			
Safari		-0.857*	-0.279
		[-1.54,-0.18]	[-1.01,0.45]
Firefox		-0.417	-0.491
		[-1.06,0.22]	[-1.19,0.21]
DuckDuckGo		-0.0137	-0.00467
		[-0.92,0.89]	[-0.95,0.94]
Other		-0.117	-0.230
		[-0.82,0.59]	[-1.02,0.56]
Use of face recognition to unlock		-0.0680	-0.0355
		[-0.21,0.08]	[-0.19,0.12]
Technical background		-0.211	0.197
		[-0.60,0.17]	[-0.22,0.61]
Perceived difficulty to configure settings			0.0974
			[-0.04,0.23]
Past behavior with configuring settings			-0.391***
			[-0.60,-0.19]
Perceived negative impact of settings on UX			1.265***
			[1.10,1.43]
χ^2	25.48^{+}	40.45*	369.8***

Table 7: Ordered logistic regression on perceived difficulty of configuring settings ($N = 178$). Q7 in the survey.

	(1)	(2)
Age	0.0155*	0.0134
	[0.00,0.03]	[-0.00,0.03]
Gender (Male omitted)		
Female	-0.222	-0.360+
	[-0.57,0.13]	[-0.72,0.00]
Other	-0.795	-0.306
	[-2.79,1.20]	[-2.61,2.00]
Non-disclosed	0.993	1.284
	[-1.05,3.04]	[-0.89,3.46]
Race/ethnicity (white omitted)		
Biracial: White and Hispanic/Latinx	-0.172	-0.0760
	[-0.83,0.48]	[-0.75,0.59]
Hispanic/Latinx	0.0699	0.0939
	[-0.41,0.55]	[-0.40,0.59]
Asian	0.393	0.436
	[-0.11,0.90]	[-0.10,0.97]
Black	-0.0590	-0.164
	[-0.55,0.43]	[-0.67,0.35]
Other biracial	0.930*	1.176**
	[0.10,1.76]	[0.33,2.02]
Other or non-disclosed	-0.502	-0.267
	[-1.35,0.35]	[-1.18,0.65]
Education	-0.0235	-0.00577
	[-0.16,0.12]	[-0.15,0.14]
Income	-0.0230	-0.0157
	[-0.11,0.06]	[-0.10,0.07]
iOS users (Android users omitted)		-0.362
		[-1.04,0.32]
Duration of experience with current OS		-0.453*
		[-0.84,-0.06]
Frequency of smartphone use		-0.998*
		[-1.96,-0.03]
Browser (Chrome omitted)		
Safari		0.0416
		[-0.68,0.76]
Firefox		-0.198
		[-0.83,0.44]
DuckDuckGo		-0.492
		[-1.43,0.45]
Other		-0.452
		[-1.14,0.24]
Use of face recognition to unlock		0.0817
		[-0.06,0.23]
Technical background		-0.406*
		[-0.79,-0.02]
χ^2	44.50***	64.00***

95% confidence intervals in brackets
+ $p < 0.1$, * $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Table 8: Ordered logistic regression on the perceived negative impact of settings on user experience ($N = 178$). Q11 in the survey.

	(1)	(2)
Age	-0.000911	-0.00248
	[-0.02,0.01]	[-0.02,0.01]
Gender (Male omitted)		
Female	0.0398	-0.0489
	[-0.30,0.38]	[-0.41,0.31]
Other	-0.466	-0.684
	[-2.33,1.40]	[-2.86,1.49]
Non-disclosed	-1.107	-2.062^{+}
	[-3.20,0.99]	[-4.29,0.16]
Race/ethnicity (White omitted)		
Biracial: White and Hispanic/Latinx	0.163	0.0544
	[-0.49,0.82]	[-0.62,0.73]
Hispanic/Latinx	-0.0955	-0.0946
	[-0.57,0.38]	[-0.59,0.40]
Asian	-0.0363	-0.0992
	[-0.52,0.45]	[-0.60,0.41]
Black	-0.0906	-0.127
	[-0.59,0.41]	[-0.65,0.40]
Other biracial	0.805*	0.890*
	[0.04,1.57]	[0.11,1.67]
Other or non-disclosed	-0.102	-0.242
	[-0.91,0.71]	[-1.10,0.62]
Education	-0.0239	-0.0292
	[-0.17,0.12]	[-0.18,0.12]
Income	-0.0528	-0.0349
	[-0.14,0.03]	[-0.12,0.05]
iOS users (Android users omitted)		0.343
		[-0.31,0.99]
Duration of experience with the current OS		0.505**
		[0.12,0.89]
Frequency of smartphone use		-0.722
		[-1.71,0.27]
Browser (Chrome omitted)		
Safari		-0.646^{+}
		[-1.33,0.04]
Firefox		0.0993
		[-0.52,0.72]
DuckDuckGo		-0.284
		[-1.25,0.69]
Other		0.528
		[-0.17,1.23]
Use of face recognition to unlock		-0.0466
		[-0.19,0.10]
Technical background		-0.469*
		[-0.85,-0.09]
χ^2	17.52	41.88*

95% confidence intervals in brackets

$^{+}$ $p < 0.1$, * $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Table 9: Ordinary least square regression on the index of the level of privacy and security concerns ($N = 178$). Q15 in the survey.

	(1)	(2)
Age	-0.00991***	-0.0102***
	[-0.01,-0.01]	[-0.01,-0.01]
Gender (Male omitted)		
Female	-0.103***	-0.108***
	[-0.16,-0.05]	[-0.16,-0.05]
Other	0.675***	0.419*
	[0.32,1.02]	[0.05,0.79]
Non-disclosed	0.127	0.291
	[-0.23,0.48]	[-0.06,0.64]
Race/ethnicity (White omitted)		
Biracial: White and Hispanic/Latinx	-0.283***	-0.303***
	[-0.39,-0.17]	[-0.41,-0.20]
Hispanic/Latinx	0.439***	0.445***
	[0.36,0.52]	[0.37,0.52]
Asian	0.563***	0.550***
	[0.48,0.65]	[0.47,0.63]
Black	0.187***	0.325***
	[0.10,0.27]	[0.24,0.41]
Other biracial	0.313***	0.271***
	[0.19,0.44]	[0.15,0.39]
Other or non-disclosed	0.632***	0.705***
	[0.49,0.78]	[0.56,0.85]
Education	0.00963	0.0517***
	[-0.01,0.03]	[0.03,0.07]
Income	0.00853	0.000957
	[-0.01,0.02]	[-0.01,0.01]
iOS users (Android users omitted)		0.231***
		[0.12,0.34]
Duration of experience with current OS		-0.244***
		[-0.31,-0.18]
Frequency of smartphone use		1.348***
		[1.19,1.51]
Browser (Chrome omitted)		
Safari		0.00542
		[-0.11,0.12]
Firefox		0.159**
		[0.06,0.26]
DuckDuckGo		0.0788
		[-0.07,0.22]
Other		-0.147**
		[-0.25,-0.04]
Use of face recognition to unlock		-0.0234*
		[-0.05,-0.00]
Technical background		-0.0912**
		[-0.15,-0.03]
Constant	0.123+	-1.686***
	[-0.01,0.25]	[-2.10,-1.27]
χ^2		

95% confidence intervals in brackets
+ $p < 0.1$, * $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

B SURVEY INSTRUMENT

Part 1.

Q1. What is the operating system on your personal smartphone? (1=iOS (only on Apple's iPhones); 2=Android (e.g. on Samsung, Huawei, Google, Xiaomi, etc.); 3=Other; 4=I'm not sure)

Q2. In total, how long have you been using smartphones that run this operating system (total time, including phones you previously owned)? (1=Less than 1 month; 2=2-5 months; 3=6-11 months; 4=1-2 years; 5=More than 2 years)

Q3. Introduce any two privacy or security risks you worry about when using your smartphone. (Consider different actors who may introduce the risks, including companies, governments, someone you know, strangers, etc.) (open-text: OpenRisk1, OpenRisk2)

Q4. Without checking your phone, describe any settings currently available on your smartphone that you could configure to address the following privacy/security risk: [Risk1/Risk2]. Type 'N/a' if you think there aren't any. (open-text: OpenSetting1, OpenSetting2)

Part 2.

Well done! In the next part of the survey you will be asked to answer a series of questions about three different smartphone privacy and security settings.

Think about the following smartphone setting: "[Setting]"

Q5. Without looking at your phone, please indicate whether you believe this setting is an existing option on your smartphone. (1=Yes; 2=No; 3=Not Sure)

Q6. If you just bought a phone with this setting as an existing option and had not changed any settings yet, what do you think would be the default configuration of it? (1=Turned on / Allowed; 2=Turned off / Not Allowed; 3=Not sure; 4=Not applicable)

Q7. How difficult or easy would it be for you to configure this setting? (1=Very Easy; 2=Easy; 3=Somewhat Easy; 4=Neither Difficult Nor Easy; 5=Somewhat Difficult; 6=Difficult; 7=Very Difficult)

Q8. Why do you think it won't be easy for you to configure this setting? (open-text)

Q9. Before taking this survey, have you ever configured this setting on your smartphone? (1=Yes; 2=No; 3=Not Sure)

Q10. Which privacy or security risks would this smartphone setting protect you from? (open-text)

Q11. If you configure this setting, how would it affect your overall experience of using your smartphone? (1=Very Negatively; 2=Negatively; 3=Somewhat Negatively; 4=Neutral; 5=Somewhat Positively; 6=Positively; 7=Very Positively; 8=I don't know)

Q12. How likely would you configure this setting? (1=Extremely Unlikely; 2=Unlikely; 3=Somewhat Unlikely; 4=Neither Likely Nor Unlikely; 5=Somewhat Likely; 6=Likely; 7=Extremely Likely)

Q13. To what extent do you think configuring this smartphone setting would be effective in protecting you from the risks below? (1=Very Effective; 2=Effective; 3=Somewhat Effective; 4=Neither Effective Nor Ineffective; 5=Somewhat Ineffective; 6=Ineffective; 7=Very Ineffective; 8=I don't know)

a) Data gathering by companies (e.g. for marketing purposes, selling data)
b) Data gathering by governments
c) Data gathering by individuals (e.g. by intimate partner, family member, friend, etc.)
d) Unsolicited advertising (e.g. spam)
e) Unsolicited objectionable content (e.g. hate speech, fake news, sexually explicit, violent, or otherwise inappropriate content)
f) Harassment (e.g. bullying, stalking, blackmailing, doxxing, release of your personal information online by someone)
g) Social engineering attacks (e.g. scam, phishing)
h) Unauthorized financial transactions
i) Unauthorized physical access to (and control over) the device (e.g. in case of a theft or if someone gains a physical access to the smartphone)
j) Unauthorized remote access to (and control over) the device (e.g. in case of a hacking or ransomware attack, virus, or other malware)
k) Inadvertent disclosure of personal information

Q14. Do you have any additional comments about this setting? (open-text)

Part 3.

Q15. How much do you agree or disagree with each of the following statements? "I worry about... (1=Strongly disagree; 2=Disagree; 3=Somewhat disagree; 4=Neutral; 5=Somewhat agree; 6=Agree; 7=Strongly agree; 8='I'm not familiar with this risk)

a) Data gathering by companies (e.g. for marketing purposes, selling data)
b) Data gathering by governments
c) Data gathering by individuals (e.g. by intimate partner, family member, friend, etc.)
d) Unsolicited advertising (e.g. spam)

e) Unsolicited objectionable content (e.g. hate speech, fake news, sexually explicit, violent, or otherwise inappropriate content)
f) Harassment (e.g. bullying, stalking, blackmailing, doxxing, release of your personal information online by someone)
g) Social engineering attacks (e.g. scam, phishing)
h) Unauthorized financial transactions
i) Unauthorized physical access to (and control over) the device (e.g. in case of a theft or if someone gains a physical access to the smartphone)
j) Unauthorized remote access to (and control over) the device (e.g. in case of a hacking or ransomware attack, virus, or other malware)
k) Inadvertent disclosure of personal information

Q16. Please indicate how easy or difficult it is for you to engage in each of the following behaviors. If you have not tried to perform a task or do not know what it is, please mark 'I have not tried' or 'I do not know,' regardless of whether or not you think you might be able to perform the task if you tried/knew. (1=Very easy, 2=Easy; 3=Somewhat easy; 4=Neutral; 5=Somewhat difficult; 6=Difficult; 7=Very difficult; 8=I have not tried; 9=I don't know)

a) To use the Internet to search for information on a smartphone
b) To send a text message from a smartphone
c) To use a smartphone for entertainment (watch movies, listen to music, read, play games, etc.)
d) To make a video call on a smartphone
e) To create a smartphone app
f) To schedule an appointment with a doctor using a health portal app on a smartphone
g) To download an app on a smartphone
h) To order food using an app on a smartphone
i) To order a car ride using an app on a smartphone
j) To transfer money to another person using an app on a smartphone

Q17. A password manager is a software application that is used to store and manage the passwords that a user has for various online accounts in an encrypted format and provide secure access to all the password information with the help of a master password. Do you use a password manager on your smartphone to store and manage your passwords? (1=No; 2=Yes, I use the password manager built in my smartphone; 3=Yes, I use a third-party password manager (e.g. Lastpass, Dashlane, 1Password, Bitwarden, etc.); 4=Other; 5=I'm not sure)

Q18. What browser do you primarily use on your smartphone? (1=Safari; 2=Chrome; 3=Firefox; 4=DuckDuckGo; 5=Other)

Q19. How often do you use your smartphone? (1=Many times a day; 2=Once or twice a day; 3=At least once a week but not every day; 4=Less than once a week)

Q20. What is the model name of your smartphone? (open-text)
For iOS users: To check, on your smartphone go to Settings > General > About > Model Name. (Note that the menu may look different on your device.)
For Android users: To check, on your smartphone, go to Settings > About phone > Model & hardware. (Note that the menu may look different on your device.)

Q21. What is the current operating system software version of your smartphone? (open-text)
For iOS users: To check, on your smartphone go to Settings > General > About > Software Version. (Note that the menu may look different on your device.)
For Android users: To check, on your smartphone go to Settings > General > About > Android Version. (Note that the menu may look different on your device.)

Q22. Do you use face recognition (Face ID, FaceUnlock) to unlock your smartphone? (1=Yes; 2=No; 3=Not sure; 4=I don't have Face ID on my smartphone)

Part 4.
Q23. What is your age?

Q24. What is the gender you most identify with? (1=Male; 2=Female; 3=I prefer to self-identify; 4=I prefer not to answer)

Q25. What language do you primarily use in your daily life? (1=English; 2=Spanish; 3=Mandarin; 4=Hindi; 5=Other (please specify); 6=Prefer not to answer)

Q26. What is the language of the settings of your personal smartphone? (1=English; 2=Spanish; 3=Mandarin; 4=Hindi; 5=Other (please specify); 6=Prefer not to answer)

Q27. What is your average annual household income, including all earners in your household (after tax)? Your answers will be kept confidential. (1=USD $10,000 or less; 2=USD $10,001-20,000; 3=USD $20,001-30,000; 4=USD $30,001-50,000; 5=USD $50,001-70,000; 6=USD $70,001-100,000; 7=USD $100,001-150,000; 8=USD $150,001-200,000; 9=USD $200,001-300,000; 10=USD $300,001 or more; 11=Prefer not to answer)

Q28. How many people (including you) live in your family household?

Q29. How would you describe your race and ethnicity? Choose all that apply. (1=White; 2=Black or African American; 3=Asian or Asian American; 4=Hispanic or Latinx; 5=Native Hawaiian or Pacific Islander; 6=American Indian or Alaska Native; 7=Middle Eastern or North African; 8=Other (please specify); 9=Prefer not to answer)

Q30. What is the highest level of education you have completed up to now? (1=Less than high school diploma/GED; 2=Completed high school/GED; 3=Some college but no degree; 4=Associate's degree; 5=Bachelor's degree; 6=Master's degree; 7=Doctoral degree, JD, or equivalent; 8=Other; 9=Prefer not to answer)

Q31. Do you have education or work experience in any of the following fields (choose all that apply)? (1=Computer science; 2=Software engineering; 3=App development; 4=Other technical field; 5=None of the above)

Q32. What is your current employment status? (1=Employed full time; 2=Employed part time; 3=Unemployed looking for work; 4=Unemployed not looking for work; 5=Retired; 6=Student; 7=Other)

Q33. Do you have comments or anything to say about the survey or study in general? (open-text)