Comparing Security and Privacy Attitudes Among U.S. Users of Different Smartphone and Smart-Speaker Platforms

Desiree Abrokwa, Shruti Das, Omer Akgul, and
Michelle L. Mazurek, *University of Maryland*

https://www.usenix.org/conference/soups2021/presentation/abrokwa

This paper is included in the Proceedings of the
Seventeenth Symposium on Usable Privacy and Security.

August 9–10, 2021

978-1-939133-25-0

Open access to the Proceedings of the
Seventeenth Symposium on Usable Privacy
and Security is sponsored by

Comparing Security and Privacy Attitudes Among U.S. Users of Different Smartphone and Smart-Speaker Platforms

Desiree Abrokwa, Shruti Das, Omer Akgul, and Michelle L. Mazurek
University of Maryland

Abstract

Many studies of mobile security and privacy are, for simplicity, limited to either only Android users or only iOS users. However, it is not clear whether there are systematic differences in the privacy and security knowledge or preferences of users who select these two platforms. Understanding these differences could provide important context about the generalizability of research results. This paper reports on a survey (n=493) with a demographically diverse sample of U.S. Android and iOS users. We compare users of these platforms using validated privacy and security scales (IUIPC-8 and SA-6) as well as previously deployed attitudinal and knowledge questions from the Pew Research Center. As a secondary analysis, we also investigate potential differences among users of different smart-speaker platforms, including Amazon Echo and Google Home. We find no significant differences in privacy attitudes of different platform users, but we do find that Android users have more technology knowledge than iOS users. In addition, we find evidence (via comparison with Pew data) that Prolific participants have more technology knowledge than the general U.S. population.

1 Introduction

The increasing ubiquity of mobile and IoT devices has generated significant research and development related to privacy and security tools, affordances, and preferences. For example, researchers have explored, at length, the implication of built-in permissions systems that govern mobile apps' access to location, contacts, sensors like the microphone or camera, and other potentially sensitive resources (e.g., [6, 9, 17, 33, 34, 38, 53, 64]). Much time and effort have also been spent developing and testing different smartphone authentication mechanisms (e.g., [31, 37, 43, 49, 60]). Extensive research into modern secure communication has focused on mobile messenger apps, including for example exploration of the usability of authentication ceremonies [24, 28, 41, 57, 61, 62, 66].

In the IoT ecosystem, researchers have explored issues ranging from concerns about unexpected listening and recording [32, 36, 55] to attacks requiring user interaction [29, 50], to studies of IoT privacy and security concerns more generally (e.g., [3, 15, 56, 67]), and more.

In many cases, these studies have been limited — often for simplicity or convenience — to only one mobile or IoT platform (e.g., Android or the Amazon Echo ecosystem) [5, 9, 17, 29, 34, 54, 59, 61, 64, 66]. In other cases, researchers have supported multiple platforms, at the cost of more complicated study instruments that must work in multiple settings [4, 36, 50, 62].

Given this context, it it important to know whether there are meaningful differences in privacy and security preferences, beliefs, and attitudes between users of different platforms. For example, Apple has recently marketed its products as more privacy-protective than alternatives [2]. In the past, iOS has pioneered fine-grained permission controls, including limiting location permissions to single-use or only while an app is being used [63]. In contrast, Google's largest source of income[1] is though targeted advertising, involving extensive user data collection.

We hypothesize that this distinction in business strategies could result in more privacy-sensitive consumers tending to purchase iPhones, perhaps resulting in Android users who are disproportionately unconcerned with privacy. Similar questions are also applicable to smart speaker platforms; however, market positioning related to privacy is not (yet) as clear as with smartphones. If there are indeed meaningful differences between users of different platforms, then extra work by re-

USENIX Symposium on Usable Privacy and Security (SOUPS) 2021.
August 8–10, 2021, Virtual Conference.

[1] https://abc.xyz/investor/static/pdf/2020Q4_alphabet_earnings_release.pdf

searchers to ensure their studies support multiple platforms may be critical. On the other hand, if there are not meaningful differences, then researchers can opt for simpler experimental designs with less concern about reduced generalizability.

In this paper, as our primary objective, we address these questions by surveying privacy and security attitudes among users of different mobile and IoT platforms to determine if differences exist. We use validated scales to measure security attitudes (SA-6) and privacy concern(IUIPC-8) [16, 19]. We also reuse questions previously used by the Pew Research Center (henceforth: Pew) in a nationally representative survey to ask about skepticism toward company data practices and knowledge about digital privacy and security [1]. As a secondary objective, reusing these questions allows us to compare attitudes between Prolific and nationally representative samples.

In 2014, Reinfelder et al. addressed similar questions, comparing security behaviors between Android and iOS users in Germany, finding that Android users were somewhat more privacy- and security-conscious [48]. We revisit this question to see what has changed in the intervening years, as devices have evolved and Apple has marketed privacy more heavily. In addition to smartphone platforms, we also consider the increasingly important smart-speaker platform. Further, we deliberately focus on attitudes rather than behaviors, as we expect that behaviors are more likely to be influenced by different platforms' privacy and security affordances.

To ensure a diverse sample, we recruit 493 participants using Prolific's "representative" sample feature, which approximates the U.S. population for gender, race, and age. We find no significant differences in security attitudes, privacy concern, or skepticism toward company data practices between users of different mobile or IoT platforms. We do find that Android users score slightly higher in security and privacy knowledge than iOS users. We also compare our sample to the representative Pew sample for the two Pew metrics, finding no difference in skepticism; however, our participants scored significantly higher in security and privacy knowledge, somewhat limiting the generalizability of our primary analysis.

These findings have implications for the design of future research exploring uses and preferences in mobile and IoT security and privacy. For studies purely about attitudes and preferences, ensuring cross-platform representation may not be necessary. On the other hand, for studies where knowledge may play an important role — for example, in evaluating mental models of security and privacy mechanisms — ensuring participation from both iOS and Android users may be more important.

2 Related Work

We discuss related work in two key areas: metrics for privacy and security, and studies that compare privacy or security attitudes and preferences among various populations.

Privacy and security metrics Researchers have long sought to define metrics for privacy and security attitudes as well as behavior. Several developed psychometric scales intended to measure privacy attitudes and concern. Perhaps the first such scale was the original 1991 Westin Privacy Segmentation Index, which groups respondents into privacy fundamentalists, pragmatists, and unconcerned [30]. In 1996, Smith et al. developed the Concern for Information Privacy (CFIP) scale, which measured privacy concern along multiple dimensions including collection, unauthorized secondary use, and improper access [52]. This was followed in 2004 by the IUIPC, a 10-item scale that builds on the original CFIP and measures three dimensions of privacy attitudes: control, awareness of privacy practices, and collection [35]. A number of other privacy scales have been proposed; Preibusch provides a comprehensive list and comparison [42].

Other researchers have investigated the utility and reliability of these scales. Woodruff et al. demonstrated that the Westin index is poorly predictive of privacy-relevant behavioral intentions [65]. In 2013, Preibusch's aforementioned guide reviews pros and cons of each metric before finally recommending IUIPC [42]. However, Sipior et al. and Zeng et al. obtain mixed results when re-validating the IUIPC, particularly with respect to trust in online companies and social networking, respectively [51, 68].

Most recently, Groß demonstrated that the original IUIPC-10 contains two poorly worded questions, without which the scale is significantly more reliable [19]. In this work, we adopt the resulting IUIPC-8 scale.

Other scales concern security attitudes and behaviors. The Security Behavior Intentions scale (SeBIS) by Egelman and Peer is intended to measure how well individuals comply with computer security advice from experts [14]. Faklaris et al. created and validated the six-item SA-6 scale to measure security attitudes, which may differ from (intended) behaviors [16]. Because we focus primarily on attitudes, we select SA-6 rather than SeBIS for our study.

Security- and privacy-relevant questions also appear in regularly administered, representative-sample surveys conducted by the Pew Research Center. The center's 2019 American Trends Panel: Wave 49 features relevant questions related to Americans' knowledge of web and internet concepts, as well as questions related to skepticism (or trust) that companies will manage the data they collect appropriately [1]. We adopt subsets of these questions that align with our research goals. Including these questions allows us to compare our results to a fully representative random sample of U.S. adults.

Comparing sample populations for privacy and security Other research has sought to compare privacy and security attitudes among different populations. Kang et al. compared the privacy attitudes and behaviors of U.S. Mechanical Turk (MTurk) workers with the general U.S.

population, finding U.S. MTurk workers display heightened privacy attitudes [25]. Redmiles et al. endorse the use of MTurk workers for convenient, affordable samples. However, they highlight shortcomings when trying to generalize security and privacy perceptions of underrepresented groups (e.g. elderly, less educated) [46]. Because we employ questions from Pew, we are able to similarly compare our results to the broader U.S. population [1].

Research has also explored differences in privacy attitudes and preferences in different countries and regions. In a longitudinal study that included 25 countries, Kelley identified important regional differences in the importance people assign to privacy, as well as whether and when it is acceptable for, e.g., law enforcement organizations to violate privacy in pursuit of other goals [26]. Redmiles compared behavior after Facebook security incidents in five countries, finding some cultural differences [45]. Ion et al. noticed political and cultural attitudinal differences in mental models related to cloud computing privacy and security between Swiss and Indian communities [23]. Similarly, Harbach et al. studied more than 8,000 Android users across eight countries. Their results affirmed that cultural and demographic characteristics can strongly determine security and privacy considerations [21]. Dev et al. compared privacy concerns related to Whatsapp messaging in Saudi Arabian and Indian communities, finding likely culturally influenced behavioral differences between populations but overall similar privacy trends when considering participants within each sample [12].

Most closely related to our work are three separate 2013-2014 studies comparing security and privacy awareness between Android and iOS users. In the first, King interviewed a small sample of iPhone and Android users from San Francisco to qualitatively understand contextual design decisions that impact privacy-centered user experiences [27]. In the second, Reinfelder et al. found (among German university students) Android users were more likely to be security aware and privacy conscious [48]. Finally, Mylonas et al. investigated user mental models of application installations on different platforms among Greeks [39]. Although not the primary research objective, they provided evidence that Android users were more security aware across multiple metrics (e.g., likelihood of adopting security software).

Because of the rapid changes in smartphone technology, both hardware and software, over the last seven years, we wanted to evaluate whether these results would still hold, this time across a broad U.S. sample. Both King and Reinfelder et al. focused on behavioral patterns, such as installing security updates, consciousness of possible malware infections, and app permissions [27,48]. We instead focus on attitudinal questions, which are frequently used in studies of smartphone and IoT users [8,10,15,44]. Further, behavioral questions about, e.g., app permissions are difficult to entangle from system design affordances and nudges that may contribute to users of different platforms making different choices. Additionally, Reinfelder et al. and Mylonas et al. primarily sampled young people. In contrast, we use Prolific's "representative sample" feature to obtain participants of diverse ages across a quasi-representative U.S. sample [39,48].

Other fields have also compared Android and iOS users. Psychologists found socioeconomic factors and personality traits may contribute to smartphone preferences [20].

3 Methods

To answer our research questions, we created and distributed a survey to measure the privacy and security attitudes and perceptions of participants. The survey was approved by the University of Maryland's Institutional Review Board. Our experimental approach was also preregistered with AsPredicted. [2]

In the following subsections we discuss the survey design, our recruitment process, our data analysis approach, and the limitations of our study.

3.1 Survey

We designed a short survey measuring privacy and security attitudes and perceptions, building on various previously used and validated constructs as described in Section 2.

The survey included the SA-6 [16] and the IUIPC-8 [19], as well as four questions about skepticism toward data use by companies and seven security- and privacy-relevant knowledge questions, all taken from Pew [1]. The original Pew survey contained 10 digital knowledge questions; we used seven that are privacy- and security-relevant. For example, we selected questioned related to HTTPS, private browsing, and phishing, while deeming a question asking participants to identify a technology leader from their photo irrelevant. To distinguish the two sets of Pew questions, we refer to them going forward as the *skepticism* and *knowledge* metrics, respectively. The questions chosen for the skepticism and knowledge metrics are shown in Tables 1 and 2.

To ensure that the Pew skepticism questions could be added together for use as a single consistent metric, we tested their internal reliability with Cronbach's α, using the data collected in Pew's national survey. We obtained $\alpha = 0.83$ for the four skepticism questions: above the 0.80 threshold for "good" reliability [18].

After providing consent, participants provided their country of residence, as a confirmation of Prolific's selection criteria. As we intended to recruit only U.S. participants, those who answered with other countries were filtered out immediately.

Next, we asked for background information on participants' device(s) and how they use them. This included multiple-choice questions about how many smartphones the participant uses or owns, what purposes they use their smartphone for

[2] https://aspredicted.org/gx2v9.pdf

Item ID	Item Text
PP5A	Follow what their privacy policies say they will do with your personal information
PP5B	Promptly notify you if your personal data has been misused or compromised
PP5C	Publicly admit mistakes and take responsibility when they misuse or compromise their users' personal data
PP5D	Use your personal information in ways you will feel comfortable with

Table 1: Items related to skepticism of company data practices, drawn from the Pew Research Center American Trends Panel: Wave 49 questionnaire [1], that are included in our survey. In the survey, participants are asked: How confident are you, if at all, that companies will do the following things? Response options are a four-point Likert-type scale from very confident to not confident at all. The item IDs are those used by Pew.

(e.g., personal, work, other), the model and operating system of their primary smartphone, whether or not they own a smart speaker (and if so, which one), how frequently they use the voice assistant on their smartphone, and how frequently they use their devices (e.g., multiple times a day). Participants were asked to retrieve actual time-use data from their smartphone if applicable. Participants without a smartphone were filtered out at this point.

Next, participants answered the security and privacy perceptions questions, including SA-6, IUIPC-8, the Pew skepticism metric and the Pew knowledge metric. In keeping with their original use, we randomized the question order and answer choices within the Pew segments. We also randomized the order of the three IUIPC-8 subscales (but not the order of questions or answers within subscales). This section also included free-response questions asking participants to explain their choices for two questions; these responses were used primarily as attention checks, and participants who gave unrelated or non-responsive answers to these questions were removed from the sample.

Finally, we asked some standard demographic questions, including questions related to age, gender identity, race/ethnicity, and employment status. We also asked about tech-savviness, measured using a Likert-type question about how often the participant gives technology advice to others. The full survey text is given in Appendix B.

We implemented the survey in Qualtrics. Prior to main data collection, we conducted eleven pilot tests of the survey with a convenience sample, to validate the questions and survey flow, as well as to estimate the time required for completion (15 minutes).

3.2 Recruitment

Participants were recruited through Prolific, an online crowdsourcing platform which can be expected to produce high-quality results [40]. Participants were required to reside in the United States and be 18 or older. The study was advertised as being about "Technology Perceptions" to avoid self-selection biases related to privacy and/or attachment to different hardware vendors. We used Prolific's "representative sample" tool to increase the diversity of our sample. Prolific stratified our sample to match 95% of 2015 U.S. census values for age, gender, and race [58].

Participants who completed the survey with valid responses were compensated with $3.00. The survey took on average 12.4 minutes, resulting in average compensation of of $14.56/hour. Responses were collected in December 2020.

3.3 Analysis

We analyzed our data using four linear regression models, with dependent variables for each privacy/security metric: SA-6, IUIPC-8, the Pew skepticism metric, and the Pew knowledge metric. For SA-6, IUIPC-8, and the skepticism metric, we summed participants' Likert responses. For the knowledge metric, participants were scored 0 to 7 based on how many questions they answered correctly.

For all four models, the independent variables included smartphone platform (iOS or Android) and smart-speaker platform (Amazon Echo, Google Home, other, none). Other covariates included age, gender, daily estimated smartphone use time, whether or not the smartphone was rooted/jailbroken, and how often participants give tech advice (used as a proxy for tech savviness). For parsimony, we binned tech advice responses into two categories: *less often* (never rarely, sometimes) and *more often* (often, almost always). We similarly binned gender into men and *non-men* (women and other genders), because very few participants reported other genders. These variables are summarized in Table 3.

To obtain our four models, we perform model selection based on Akaike Information Criterion (AIC), which strikes a balance between how well models explain the dependent variables and over-fitting [7]. For each dependent variable, we fit regressions with smartphone and smart-speaker platforms (the main variables of interest) as well as all possible combinations of the other covariates. We report only the model with the lowest AIC for each metric.

We aimed to recruit 500 participants. Power analysis for linear regression (assuming that all our potential IVs would be included) shows that 500 participants is sufficient to detect approximately small[3] effects ($f^2 = 0.032$) [11].

We note one deviation from our preregistered analysis plan. We initially planned to fit eight regression models: one for

[3] Cohen claims $f^2 > 0.02$ would capture "small", $f^2 > 0.15$ would capture "medium" effect sizes.

Item ID	Item text	Correct answer
KNOW1	If a website uses cookies, it means that the site …	Can track your visits and activity on the site
KNOW2	Which of the following is the largest source of revenue for most major social media platforms?	Allowing companies to purchase advertisements on their platforms
KNOW3	When a website has a privacy policy, it means that the site …	Has created a contract between itself and its users about how it will use their data
KNOW4	What does it mean when a website has "https://" at the beginning of its URL, as opposed to "http://" without the "s"?	Information entered into the site is encrypted
KNOW5	Where might someone encounter a phishing scam?	All of the above (In an email, on social media, in a text message, on a website)
KNOW7	The term "net neutrality" describes the principle that …	Internet service providers should treat all traffic on their networks equally
KNOW8	Many web browsers offer a feature known as "private browsing" or "incognito mode." If someone opens a webpage on their computer at work using incognito mode, which of the following groups will NOT be able to see their online activities?	A coworker who uses the same computer

Table 2: Security- and privacy-relevant digital knowledge questions, drawn from the Pew Research Center American Trends Panel: Wave 49 questionnaire [1]. All questions are multiple-choice. The item IDs are those used by Pew.

Variable	Explanation	Baseline
Main variables of interest:		
Smartphone OS	Whether the participant is an iOS or Android user	iOS
Smart speaker	Whether the participant owns a smart speaker, and which	Amazon Echo device
Demographic covariates:		
Tech advice	Whether the participant is asked for tech advice, binned into less often or more often	Less often
Device rootedness	Whether or not the participant's device is rooted or jailbroken	Not rooted
Screen-time estimate	Self-reported hours of daily phone use	–
Age	The participant's age	–
Gender	Gender, binned into men and non-men (women and other genders)	Non-man

Table 3: Independent variables (**IVs**) used in our regressions, including main variables of interest (mobile and smart-speaker platforms) as well as demographic covariates. Baselines are listed for categorical variables. Section 3.3 details the regressions.

each combination of dependent variable (SA-6, IUIPC, skepticism metric, knowledge metric) and platform (smartphone OS and smart-speaker type). We made this plan because we assumed that relatively few participants in the initial "representative sample" from Prolific would own smart speakers; we intended to augment our sample with a second batch recruited from Prolific specifically on the basis of smart-speaker ownership. Because we didn't want to combine these two incompatible samples, we intended to model smartphone and smart-speaker platforms separately. However, we were pleasantly surprised to find that more than one third of our "representative" sample were smart-speaker owners. Rather than obtain a less representative sample, we opted to use only the initial sample and to include both platform types in our four regression models. Using fewer models reduces the complexity of our analysis and enables holistic comparison that accounts for all factors at once.

We also added one secondary analysis not described in our pre-registration: We compare our participants' responses to the Pew questions to the nationally representative Pew data for the same questions. This comparison allows us to explore how well the "representative" Prolific feature captured the broader U.S. population (albeit with a time lag). For these comparisons, after establishing that the data was not normally distributed (Shapiro-Wilk $p < 0.001$), we use non-parametric, two-tailed Mann-Whitney U tests, one for each Pew metric. Since the Pew scales are used in two analyses each (one regression and one MWU), we adjust the relevant p-values with Bonferroni correction.

3.4 Limitations

Our study has several limitations, most of which are common to this type of research. Although we used Prolific's "represen-

tative sample" [4] tool to diversify our sample, our participants are still on average more educated than the U.S. population. Our sample also severely underrepresents, compared to the U.S. population, people who identify as Hispanic or Latino; the Prolific stratification does not incorporate this ethnicity information. Additionally, we compared the results for the Pew scales to a representative sample of the U.S. population. This indicated that while Prolific users have similar privacy concerns, they have more privacy and security knowledge than the broader population.

Survey responses were only collected from Prolific users in the United States. We focused on the United States to avoid confounds related to availability and popularity of different devices, as well as cultural differences, inherent in comparing multiple countries. However, our results cannot necessarily generalize to non-U.S. populations.

We use self-report metrics, which are vulnerable to biases such as social desirability and acquiescence. However, prior work suggests self-reporting can provide useful data on security and privacy questions [13,47]. Further, we expect these biases to affect users of different smartphone and smart-speaker platforms similarly, enabling comparison among groups.

4 Results

In this section, we first describe our survey participants. We then detail the results of our regressions comparing platform users across each security or privacy metric. Finally, we compare our sample to the nationally representative Pew sample for context. Overall, we found no differences across platforms in privacy attitudes, but we found that Android users scored higher than iOS users on the Pew knowledge metrics. Our sample did not differ significantly from the Pew sample in skepticism toward company data practices, but our participants scored higher on the knowledge metric.

4.1 Participants

In December 2020, we used Prolific to recruit 500 participants currently residing in the U.S. We discarded five for off-topic or unresponsive free-text responses, one for being outside the U.S., and one who skipped an optional question that was required for our analysis. The remaining 493 participants served as our final sample for analysis.

Of the 493 participants, 285 use Android and 208 use iOS on their primary smartphone. In total, 175 participants use smart speakers, including 95 who only use an Amazon Echo, 54 who only use Google Home, and 26 who use some other smart speaker or use multiple brands.

Demographics within our Android, iOS, and total samples are given in Table 4. Because we used Prolific's "representative sample" feature, our overall sample is fairly representative of the U.S. for gender, age, and race. Other demographics, however, suffer from typical crowdsourcing biases, including insufficient Hispanic/Latinx representation and more education than the U.S. population overall[5]. The plurality of participants report giving tech advice "sometimes."

		Android (%)	iOS (%)	Total (%)
Gender	Women	50.5	51.0	50.7
	Men	48.4	47.6	48.1
	Non-binary and other	1.1	1.5	1.2
Age	18-27	14.0	24.0	18.3
	28-37	19.7	16.8	18.5
	38-47	18.2	14.9	16.8
	48-57	17.2	18.3	17.6
	58+	30.9	26.0	28.8
Hispanic origin	No	95.8	91.8	94.1
	Yes	4.2	8.2	5.9
Race	White	74.0	73.3	73.7
	Black or African Amer.	15.5	11.5	13.8
	Asian	6.1	11.1	8.2
	Amer. Ind. or AK Native	2.7	1.8	2.3
	Nat. Hawaiian or Pac. Isl.	0.3	0.5	0.4
Education	Completed H.S. or below	13.0	5.3	9.7
	Some college, no degree	25.3	22.6	24.1
	Associate's degree	12.6	4.8	9.3
	Bachelor's degree	27.7	36.1	31.2
	Master's degree or higher	14.4	25.0	18.9
Employment status	Employed full-time	34.4	37.5	35.6
	Employed part-time	13.0	13.5	13.2
	Self-employed	13.0	12.5	12.8
	Retired	15.8	13.9	15.0
	Unemployed	7.7	6.7	7.3
	Student	5.6	9.6	7.3
Tech advice	Almost always	5.6	6.7	6.1
	Often	20.3	19.2	19.9
	Sometimes	41.4	43.3	42.2
	Rarely	28.1	24.5	26.6
	Never	4.6	6.3	5.3

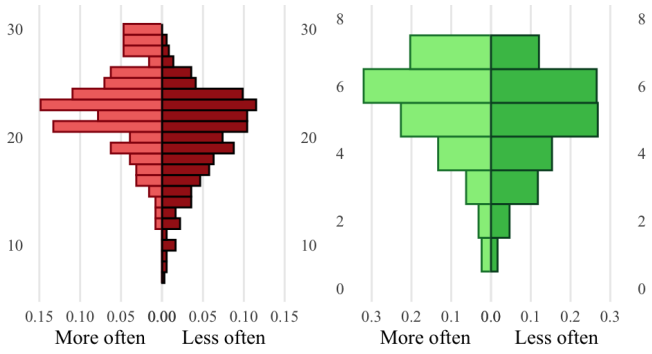
Table 4: Participant demographics. Percentages may not add to 100% due to multiple selection and item non-response; some categories with small percentages are elided.

Our results show some demographic differences between smartphone users. Our Android users tend to be older and less educated than their iOS counterparts. Our iOS sample has higher proportions of Asian and Hispanic people, but a noticeably smaller proportion of Black people. There are also some notable differences in educational attainment between the populations, with iOS users tending to have more education.

In addition to asking participants for their daily screen-time estimates, we asked participants who were able to report their actual daily screen-time averages (visible under "Screen Time" settings on iOS and "Digital Wellbeing" on some An-

[4] https://researcher-help.prolific.co/hc/en-gb/articles/360019236753-Representative-Samples-on-Prolific

[5] https://www.census.gov/acs/www/data/data-tables-and-tools/data-profiles/2019



(a) SA-6 (b) Pew knowledge

Figure 1: Comparison of SA-6 and Pew knowledge metric responses for participants who give tech advice more and less often. The Y-axis shows the range of possible values for each scale; the X-axis shows the fraction of total participants with each score. Both comparisons show a significant difference.

SA-6	β	$CI_{95\%}$	T-value	p-value
Smartphone (vs. iOS)				
Android	0.0	[-0.7, 0.8]	0.070	0.945
Smart speaker (vs. Amazon)				
Google	−0.4	[-1.8, 1.0]	−0.600	0.549
Other	−0.9	[-2.7, 0.8]	−1.026	0.306
None	−0.1	[-1.0, 0.9]	−0.196	0.845
Covariates				
Tech advice: More often	2.5	[1.7, 3.4]	5.901	< 0.001*
Rootedness: Not rooted	−1.1	[-2.6, 0.4]	−1.482	0.139
Gender: Man	−0.9	[-1.7,-0.2]	−2.533	0.012*

Table 5: Final regression table for SA-6. Adj. $R^2 = 0.08$. *Statistically significant.

droid models). Self-reported daily screen time was 4.5 hours ($\sigma = 3.7$, min=0, max=20). Participants on average (calculated from 225 participants who were able to provide both an estimate and the smartphone report) underestimated their screen time by 27.4 minutes ($\sigma = 147.3$). This corresponds to 10% error in screen-time use. Distribution of the error can be found in Figure 4 of Appendix A.

4.2 Comparing platforms

We fit four regression models, one each for our privacy and security metrics. These models included both smartphone and smart-speaker platform, as well as other demographic covariates. We report, in turn, on each of the final best-fit models.

Security attitude (SA-6) First, we analyze responses to the SA-6 security attitude scale. Potential scores on this scale range from 6–30, with higher numbers indicating a more positive attitude toward security behaviors. Overall, our participants scored an average of 20.7 ($\sigma = 4.2$, min=7, max=30).

By definition, our final regression model (Table 5) includes both smartphone (Android mean=20.8; iOS mean=20.7) and smart-speaker platform (Amazon Echo mean=20.9; Google Home mean=20.8; Other mean=20.4; None mean=20.7), but neither factor is significant. Figure 2a illustrates the similarity between iOS and Android participants for this metric.

The only two significant covariates were tech advice and gender. As shown in Figure 1a, those who give tech advice "often" or "almost always" were associated with a 2.5-point increase in positive attitude ($p < 0.001$), compared to those who do not. It's intuitively reasonable that increased tech-savviness would correlate with more interest in security. This also aligns with findings in the original SA-6 paper that the scale correlates with tech-savviness, confidence in using computers, and digital literacy [16].

In a smaller effect, men were associated with an 0.9-point decrease in positive attitude toward security compared to non-men ($p = 0.012$). Rootedness was also retained in the final model, but did not show a statistically significant effect.

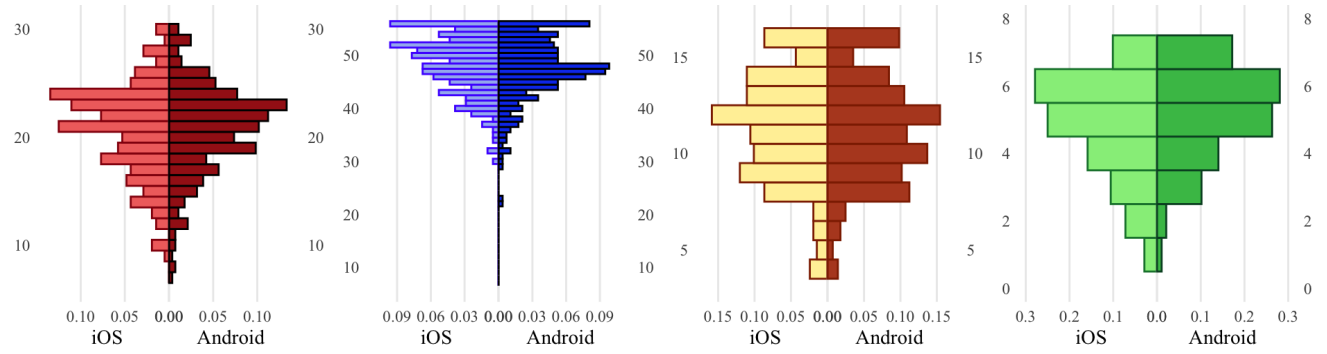
IUIPC-8	β	$CI_{95\%}$	T-value	p-value
Smartphone (vs. iOS)				
Android	−0.9	[-1.9, 0.2]	−1.624	0.105
Smart speaker (vs. Amazon)				
Google	−1.4	[-3.4, 0.5]	−1.418	0.157
Other	−0.4	[-2.9, 2.2]	−0.274	0.784
None	1.0	[-0.3, 2.4]	1.517	0.130
Covariates				
Rootedness: Not Rooted	1.6	[-0.6, 3.7]	1.449	0.148
Screen-time Estimate	−0.2	[-0.3, 0.0]	−2.223	0.027*
Age	0.0	[-0.0, 0.1]	1.510	0.132

Table 6: Final regression table for IUIPC. Adj. $R^2 = 0.04$. *Statistically significant.

Privacy concern (IUIPC-8) Next, we consider responses to the IUIPC-8, which measures privacy concern. Potential scores range from 8–56, with higher scores indicating higher levels of privacy concern. Our participants scored on average 47.7 ($\sigma = 5.9$, min=22, max=56), indicating that they tend to be more privacy sensitive than not.

As with SA-6, we see no significant differences based on smartphone (Android mean=47.3; iOS mean=48.1) or smart-speaker platform (Amazon Echo mean=47.2; Google Home mean=45.3; other mean=46.8; None mean=48.3). Figure 2b illustrates the similarity of responses across the two smartphone platforms and Table 6 shows the final regression model.

In fact, we find only one significant factor: estimated screen time on the primary smartphone, depicted in Figure 5a of Appendix A. Each additional 5 hours of daily screen time is associated with a drop of 1.0 points in privacy concern



(a) SA-6 (b) IUIPC-8 (c) Pew skepticism (d) Pew knowledge

Figure 2: Comparison between iOS and Android users on all metrics. The Y-axis shows the range of possible values for each scale; the X-axis shows the fraction of total participants with each score. Only the Pew knowledge metric shows a significant difference between platforms.

($p = 0.027$). It is perhaps unsurprising that participants who spend more time on their smartphones exhibit lower privacy concern, possibly due to habituation. Age and whether or not the participant had rooted their device were retained in the final model but did not show significant effects.

Skepticism toward companies (Pew) We next examine participants' skepticism toward companies' data management practices. Potential scores on this metric range from 4–16, with higher scores indicating more skepticism and lower scores indicating more trust. Participants scored on average 11.3 ($\sigma = 2.8$, min=4, max=16).

On this metric, also, we see no significant differences based on smartphone (Android mean=11.2; iOS mean=11.3) or smart-speaker (Amazon Echo mean=11.5; Google Home mean=11.1; Other mean=10.8; None mean=11.3) platform in the final model (Table 7). This lack of difference is illustrated in Figure 2c.

As with IUIPC, the only significant factor in the model was screen time. Each additional five hours of screen time per day is associated with a 1.0-point drop in skepticism ($p < 0.001$). This aligns with the similar finding for IUIPC: more screen time, and presumably more habituation, is associated with less concern about data practices (Figure 5b of Appendix A). Age is again included in the final model but not significant.

Security and privacy knowledge (Pew) Finally, we analyzed results from the Pew knowledge metric. Participants could score from 0–7 on this metric, corresponding to the number of questions they answered correctly. Our participants scored on average 5.0 ($\sigma = 1.5$, min=0, max=7).

The final model (Table 8) estimates that Android users are likely to score 0.4 points higher on this correctness quiz than iOS users ($p = 0.004$), meaning they have somewhat more security and privacy knowledge (Android mean=5.1; iOS mean=4.8). This difference is fairly small, but may reflect Apple's reputation of making products that are easy to use even for people with very limited technological skills. This

Pew Skepticism	β	$CI_{95\%}$	T-value	p-value
Smartphone (vs. iOS)				
Android	0.0	[-0.4, 0.5]	0.191	1.000
Smart speaker (vs. Amazon)				
Google	−0.4	[-1.3, 0.5]	−0.884	0.754
Other	−0.6	[-1.8, 0.6]	−0.952	0.683
None	−0.3	[-1.0, 0.3]	−1.046	0.593
Covariates				
Screen-time Estimate	−0.2	[-0.3,−0.1]	−5.861	< 0.001*
Age	0.0	[-0.0, 0.0]	−1.554	0.242

Table 7: Final regression table for the Pew skepticism metric. Adj. $R^2 = 0.06$. *Statistically significant. All p-values reflect Bonferroni correction.

difference can be seen in Figure 2d, which shows more Android users at the high end and more iOS users at the low end of scores. We found no significant differences among smart-speaker owners on this metric, either (Amazon Echo mean=5.1; Google Home mean=5.2; Other mean=4.5; None mean=4.9).

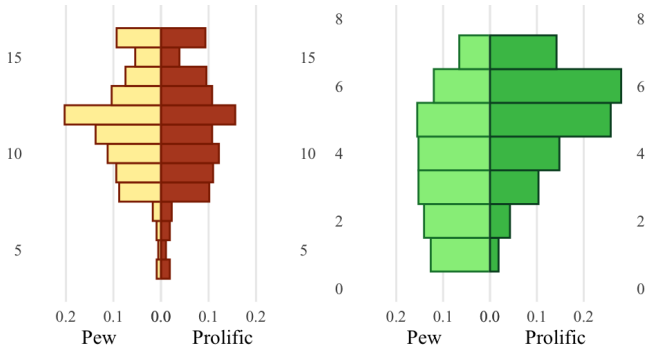
Three demographic covariates appear as significant factors in this model. Giving tech advice "often" or "almost always" (depicted in Figure 1b) correlates with an 0.4-point increase in score ($p = 0.027$); this makes intuitive sense. On the other hand, each additional five hours of screen time is associated with an 0.5-point drop in knowledge scores ($p < 0.001$). This aligns with our results on the other metrics showing that more screen time is associated with lower privacy concern and skepticism.

We also see a small but significant effect for age: each 10 years of additional age correspond to an estimated 0.1-point drop in correctness score ($p = 0.012$)[6]. It is perhaps unsur-

[6]The age coefficient (β) shown in table 7 and 8 is rounded down to 0.0;

Pew Knowledge	β	$CI_{95\%}$	T-value	p-value
Smartphone (vs. iOS)				
Android	0.4	[0.2, 0.7]	3.136	0.004*
Smart speaker (vs. Amazon)				
Google	−0.1	[-0.6, 0.4]	−0.238	1.000
Other	−0.6	[-1.3, 0.0]	−1.917	0.112
None	−0.2	[-0.5, 0.1]	−1.136	0.513
Covariates				
Tech advice: More often	0.4	[0.1, 0.7]	2.474	0.027*
Screen-time Estimate	−0.1	[-0.1, 0.0]	−4.588	< 0.001*
Age	0.0	[-0.0, 0.0]	−2.753	0.012*
Gender: Man	−0.2	[-0.5, 0.1]	−1.540	0.248

Table 8: Final regression table for the Pew knowledge metric. Adj. $R^2 = 0.08$. *Statistically significant. All p-values reflect Bonferroni correction.



(a) Pew Skepticism (b) Pew Knowledge

Figure 3: Comparison between Pew participants and our Prolific participants. The populations show significant difference in privacy/security knowledge.

prising that older people have on average slightly less security and privacy knowledge. We attribute the relatively small effect size in part to Prolific participants; in prior work, older crowdworkers and digital panel participants were unusually tech savvy for their age [46].

4.3 Comparing our participants to a nationally representative sample

An added benefit of reusing Pew questions is that we can compare responses from our sample to Pew's nationally representative sample (n=4225) [1].

Figure 3a compares our sample to the Pew sample on the skepticism metric. We find no significant difference between the two populations (MWU, $p = 0.120$).

Figure 3b illustrates responses to the knowledge metric from the two samples. Our Prolific participants tended to score higher, indicating more security and privacy knowledge (MWU, $p < 0.001$). The location-shift estimate, a measure of effect size related to median [22], is 2.0, indicates that our participants tend to score about two points higher out of seven.

5 Discussion

We used a survey with a quasi-representative sample to compare privacy and security perceptions across users of smartphone platforms (Android and iOS) as well as smart-speaker platforms (Google Home, Amazon Echo, another platform, or none). We find no significant differences in attitudes toward security, privacy, or company data practices. We do, however, find that Android users are somewhat more knowledgeable about digital security and privacy. On the other hand, differences in smartphone screen time are significantly negatively correlated with all of our metrics except security attitudes: more screen time is associated with less privacy concern, less skepticism, and less security/privacy knowledge. In a similar result, giving tech advice more often is positively correlated with positive security attitudes and more privacy/security knowledge.

These results have several implications for future research into tools and interfaces for mobile and IoT privacy and security. It may be low-effort to incorporate users of different platforms into survey or interview studies. However, cross-platform support is more challenging for research that involves new tools, such as testing an agent for managing app permissions, or field-type studies in which participants use smart devices in their homes for a period of time.

With respect to smartphones, our results suggest that studies that chiefly involve attitudes and preferences — for example, studies related to app permission choices or preferences for potentially invasive tracking and advertising — may not need to take differing platforms into account. On the other hand, we did find differences in security and privacy knowledge, which implies that cross-platform support may be important when a user's knowledge is expected to be a key factor. These could include studies evaluating knowledge or mental models related to secure communications or tracking and inferencing, as well as studies relating to adoption of various privacy- and anonymity-enhancing technologies.

Our results about screen time and tech advice also have research design implications. Many researchers already tend to (at least partially) control for tech-savviness in participants. Our results support this practice, while suggesting that screen time may be an equally or even more important variable to consider.

With respect to smart-speaker platforms, we found no significant differences in any of our metrics. This suggests that, for now, cross-platform differences are not critical for security and privacy research on smart speakers. It remains an open

when multiplied by 10, it rounds to 0.1.

question whether this result extends to other kinds of IoT devices. It is similarly unclear whether this result will remain stable over time, as the market for IoT devices becomes more mature.

Our work also has implications for crowdsourced samples. Comparing our sample to a U.S.-representative sample from Pew, we find that our participants express similar skepticism toward data practices, but are noticeably more digitally knowledgeable than the general U.S. population. The lack of difference in skepticism provides hope that the gap in privacy attitudes noted by Kang et al. in 2014 is shrinking as digital habits and devices become further entrenched [25]. On the other hand, we confirm prior results that web survey panels, even when more or less demographically representative, still provide participants who are disproportionately tech-savvy for their demographics [46]. We therefore encourage researchers to continue to recognize this limitation in generalizability, and to consider alternate means of recruiting, if feasible, when tech-savviness is important to the research question(s) being addressed.

Finally, we suggest researchers also measure other potential differences between the user populations we investigate in this study. Specifically, we emphasize the need for behavioral studies to complement our self-report data, and to explore differences between attitudes and behaviors that may relate to available privacy or security affordances.

6 Conclusion

In this study, we conducted a security and privacy survey using previously validated metrics in order to examine whether there are important differences in attitudes between users of different smartphone and smart-speaker platforms. Using a quasi-representative sample, we found no differences in attitudes among these groups. However, we found that Android users tend to have more security and privacy knowledge than iOS users. We also found that more daily screen time is associated with less privacy concern, less skepticism of company data practices, and less security and privacy knowledge. By comparing our sample to a nationally representative dataset from Pew, we can observe that our quasi-representative sample has similar skepticism to the general U.S. population, but more security and privacy knowledge. These results can provide guidance for designing — and context for interpreting — future studies on technology platforms.

7 Acknowledgments

The authors would like to thank participants who took part in our survey as well as the anonymous reviewers for constructive comments and suggestions. This paper results from the SPLICE research program, supported by a collaborative award from the National Science Foundation (NSF) SaTC Frontiers program under award number 1955805. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of NSF. Any mention of specific companies or products does not imply any endorsement by the authors, by their employers, or by the NSF.

References

[1] American Trends Panel Wave 49, 2019. https://www.pewresearch.org/internet/dataset/american-trends-panel-wave-49.

[2] Data privacy day at Apple: Improving transparency and empowering users. 2021. https://www.apple.com/newsroom/2021/01/data-privacy-day-at-apple-improving-transparency-and-empowering-users.

[3] Noura Abdi, Kopo M. Ramokapane, and Jose M. Such. More than smart speakers: Security and privacy perceptions of smart home personal assistants. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. USENIX Association, August 2019.

[4] Ruba Abu-Salma, Kat Krol, Simon Parkin, Victoria Koh, Kevin Kwan, Jazib Mahboob, Zahra Traboulsi, and M. Angela Sasse. The Security Blanket of the Chat World: An Analytic Evaluation and a User Study of Telegram. In *2nd European Workshop on Usable Security (EuroUSEC)*. Internet Society, NDSS Symposium, 2017.

[5] Omer Akgul, Wei Bai, Shruti Das, and Michelle L. Mazurek. Evaluating In-Workflow Messages for Improving Mental Models of End-to-End Encryption. In *USENIX Security Symposium*, 2021.

[6] Bram Bonné, Sai Teja Peddinti, Igor Bilogrevic, and Nina Taft. Exploring decision making with Android's runtime permission dialogs using in-context surveys. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. USENIX Association, July 2017.

[7] Hamparsum Bozdogan. Model Selection and Akaike's Information Criterion (AIC): The General Theory and Its Analytical Extensions. *Psychometrika*, 1987.

[8] Alex Braunstein, Laura Granka, and Jessica Staddon. Indirect Content Privacy Surveys: Measuring Privacy Without Asking About It. *SOUPS 2011 - Proceedings of the 7th Symposium on Usable Privacy and Security*, 2011. https://dl.acm.org/doi/10.1145/2078827.2078847.

[9] Pern Hui Chia, Yusuke Yamamoto, and N. Asokan. Is this App Safe? A Large Scale Study on Application Permissions and Risk Signals. In *Proceedings of the 21st International Conference on World Wide Web*, 2012.

[10] Erika Chin, Adrienne Porter Felt, Vyas Sekar, and David Wagner. Measuring User Confidence in Smartphone Security and Privacy. SOUPS '12. Association for Computing Machinery, 2012. https://doi.org/10.1145/2335356.2335358.

[11] Jacob Cohen. *Statistical Power Analysis for the Behavioral Sciences*. Academic Press, 2013.

[12] Jayati Dev, Pablo Moriano, and L. Jean Camp. Lessons learnt from comparing WhatsApp privacy concerns across Saudi and Indian populations. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. USENIX Association, August 2020.

[13] Serge Egelman, Marian Harbach, and Eyal Peer. Behavior Ever Follows Intention? A Validation of the Security Behavior Intentions Scale (SeBIS). In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 2016.

[14] Serge Egelman and Eyal Peer. Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS). In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. Association for Computing Machinery, 2015. https://doi.org/10.1145/2702123.2702249.

[15] Pardis Emami Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Cranor. Exploring How Privacy and Security Factor into IoT Device Purchase Behavior. In *CHI '19: Proceedings of CHI Conference on Human Factors in Computing Systems*, 2019. https://dl.acm.org/doi/10.1145/3290605.3300764.

[16] Cori Faklaris, Laura A. Dabbish, and Jason I. Hong. A Self-Report Measure of End-User Security Attitudes (SA-6). In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. USENIX Association, 2019. https://www.usenix.org/conference/soups2019/presentation/faklaris.

[17] Adrienne Porter Felt, Kate Greenwood, and David Wagner. The Effectiveness of Application Permissions. In *2nd USENIX Conference on Web Application Development (WebApps 11)*. USENIX Association, June 2011.

[18] Joseph A. Gliem and Rosemary R. Gliem. Calculating, Interpreting, and Reporting Cronbach's Alpha Reliability Coefficient for Likert-Type Scales. Midwest Research-to-Practice Conference in Adult, Continuing, and Community Education, 2003.

[19] Thomas Groß. Validity and Reliability of the Scale Internet Users' Information Privacy Concern (IUIPC). PETs Symposium, 2020. https://petsymposium.org/2021/files/papers/issue2/popets-2021-0026.pdf.

[20] Friedrich M. Götz, Stefan Stieger, and Ulf-Dietrich Reips. Users of the main smartphone operating systems (iOS, Android) differ only little in personality. *PLOS ONE*, 2017. https://doi.org/10.1371/journal.pone.0176921.

[21] Marian Harbach, Alexander De Luca, Nathan Malkin, and Serge Egelman. *Keep on Lockin' in the Free World: A Multi-National Comparison of Smartphone Locking*. Association for Computing Machinery, 2016. https://doi.org/10.1145/2858036.2858273.

[22] Myles Hollander, Douglas A. Wolfe, and Eric Chicken. *Nonparametric Statistical Methods*, volume 751. John Wiley & Sons, 2013.

[23] Iulia Ion, Niharika Sachdeva, Ponnurangam Kumaraguru, and Srdjan Čapkun. Home is Safer than the Cloud! Privacy Concerns for Consumer Cloud Storage. In *Proceedings of the Seventh Symposium on Usable Privacy and Security*, SOUPS '11. Association for Computing Machinery, 2011. https://doi.org/10.1145/2078827.2078845.

[24] Ronald Kainda, Ivan Flechais, and Andrew William Roscoe. Usability and security of out-of-band channels in secure device pairing protocols. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, 2009.

[25] Ruogu Kang, Stephanie Brown, Laura Dabbish, and Sara Kiesler. Privacy Attitudes of Mechanical Turk Workers and the U.S. Public. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*. USENIX Association, 2014. https://www.usenix.org/conference/soups2014/proceedings/presentation/kang.

[26] Patrick Kelley. Privacy, measurably, isn't dead. USENIX Association, February 2021.

[27] Jennifer King. How Come I'm Allowing Strangers to Go Through My Phone? Smartphones and Privacy Expectations. *SSRN Electronic Journal*, 2012.

[28] Arun Kumar, Nitesh Saxena, Gene Tsudik, and Ersin Uzun. A comparative study of secure device pairing methods. *Pervasive and Mobile Computing*, 2009.

[29] Deepak Kumar, Riccardo Paccagnella, Paul Murley, Eric Hennenfent, Joshua Mason, Adam Bates, and Michael Bailey. Skill squatting attacks on Amazon Alexa. In *27th USENIX Security Symposium (USENIX Security 18)*. USENIX Association, August 2018.

[30] Ponnurangam Kumaraguru and Lorrie Cranor. Privacy indexes : A Survey of Westin's Studies. 2005. https://www.cs.cmu.edu/~ponguru/CMU-ISRI-05-138.pdf.

[31] Imane Lamiche, Guo Bin, Yao Jing, Zhiwen Yu, and Abdenour Hadid. A continuous smartphone authentication method based on gait patterns and keystroke dynamics. *Journal of Ambient Intelligence and Humanized Computing*, 2019.

[32] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. Alexa, are you listening? Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. *Proc. ACM Hum.-Comput. Interact.*, 2(CSCW), November 2018.

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

[34] Bin Liu, Mads Schaarup Andersen, Florian Schaub, Hazim Almuhimedi, Shikun (Aerin) Zhang, Norman Sadeh, Yuvraj Agarwal, and Alessandro Acquisti. Follow My Recommendations: A Personalized Privacy Assistant for Mobile App Permissions. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. USENIX Association, June 2016.

[35] Naresh K. Malhotra, Sung S. Kim, and James Agarwal. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research*, 2004. https://doi.org/10.1287/isre.1040.0032.

[36] Nathan Malkin, Joe Deatrick, Allen Tong, Primal Wijesekera, Serge Egelman, and David Wagner. Privacy Attitudes of Smart Speaker Users. *Proceedings on Privacy Enhancing Technologies*, 2019.

[37] Philipp Markert, Daniel V. Bailey, Maximilian Golla, Markus Dürmuth, and Adam J. Aviv. This pin can be easily guessed: Analyzing the security of smartphone unlock pins. In *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2020.

[38] Kristopher Micinski, Daniel Votipka, Rock Stevens, Nikolaos Kofinas, Michelle L. Mazurek, and Jeffrey S. Foster. User interactions and permission use on Android. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 2017.

[39] Alexios Mylonas, Anastasia Kastania, and Dimitris Gritzalis. Delegate the smartphone user? Security awareness in smartphone platforms. *Computers & Security*, 2013. https://doi.org/10.1016/j.cose.2012.11.004.

[40] Eyal Peer, Laura Brandimarte, Sonam Samat, and Alessandro Acquisti. Beyond the Turk: Alternative platforms for crowdsourcing behavioral research. *Journal of Experimental Social Psychology*, 2017.

[41] Adrian Perrig and Dawn Song. Hash visualization: A new technique to improve real-world security. In *International Workshop on Cryptographic Techniques and E-Commerce*, volume 25, 1999.

[42] Sören Preibusch. Guide to measuring privacy concern: Review of survey and observational instruments. *International Journal of Human-Computer Studies*, 2013.

[43] Lina Qiu, Alexander De Luca, Ildar Muslukhov, and Konstantin Beznosov. Towards understanding the link between age and smartphone authentication. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 2019.

[44] Prashanth Rajivan and Jean Camp. Influence of privacy attitude and privacy cue framing on Android app choices. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. USENIX Association, 2016. https://www.usenix.org/conference/soups2016/workshop-program/wpi/presentation/rajivan.

[45] Elissa M. Redmiles. "Should I worry?" A cross-cultural examination of account security incident response. *CoRR*, abs/1808.08177, 2018. http://arxiv.org/abs/1808.08177.

[46] Elissa M. Redmiles, Sean Kross, and Michelle L. Mazurek. How well do my results generalize? Comparing security and privacy survey results from mturk, web, and telephone samples. In *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2019.

[47] Elissa M. Redmiles, Ziyun Zhu, Sean Kross, Dhruv Kuchhal, Tudor Dumitras, and Michelle L. Mazurek. Asking for a Friend: Evaluating Response Biases in Security User Studies. CCS '18. Association for Computing Machinery, 2018. https://doi.org/10.1145/3243734.3243740.

[48] Lena Reinfelder, Zinaida Benenson, and Freya Gassmann. Differences between Android and iPhone Users in Their Security and Privacy Awareness. In *Proceedings of the 11th International Conference on Trust, Privacy and Security in Digital Business*. Springer, 2014. https://link.springer.com/chapter/10.1007/978-3-319-09770-1_14.

[49] Raina Samuel, Philipp Markert, Adam J. Aviv, and Iulian Neamtiu. Knock, Knock. Who's There? On the security of LG's knock codes. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. USENIX Association, August 2020.

[50] Faysal Hossain Shezan, Hang Hu, Jiamin Wang, Gang Wang, and Yuan Tian. Read between the lines: An empirical measurement of sensitive applications of voice personal assistant systems. In *Proceedings of The Web Conference 2020*, 2020.

[51] Janice Sipior, Burke Ward, and Regina Connolly. Empirically assessing the continued applicability of the IUIPC construct. *Journal of Enterprise Information Management*, 26, 2013.

[52] H. Jeff Smith, Sandra J. Milberg, and Sandra J. Burke. Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly*, 1996. http://www.jstor.org/stable/249477.

[53] Daniel Smullen, Yuanyuan Feng, Shikun Aerin Zhang, and Norman Sadeh. The best of both worlds: Mitigating trade-offs between accuracy and user burden in capturing mobile app privacy preferences. *Proceedings on Privacy Enhancing Technologies*, 2020.

[54] Peter Story, Daniel Smullen, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. From Intent to Action: Nudging Users Towards Secure Mobile Payments. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. USENIX Association, August 2020.

[55] Madiha Tabassum, Tomasz Kosiński, Alisa Frik, Nathan Malkin, Primal Wijesekera, Serge Egelman, and Heather Richter Lipford. Investigating users' preferences and expectations for always-listening voice assistants. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, December.

[56] Madiha Tabassum, Tomasz Kosinski, and Heather Richter Lipford. "I don't own the data": End user perceptions of smart home device data practices and risks. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. USENIX Association, August 2019.

[57] Joshua Tan, Lujo Bauer, Joseph Bonneau, Lorrie Faith Cranor, Jeremy Thomas, and Blase Ur. Can unicorns help users compare crypto key fingerprints? In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 2017.

[58] Prolific Team. Representative Samples FAQ. 2019. https://researcher-help.prolific.co/hc/en-gb/articles/360019238413-Representative-Samples-FAQ.

[59] Güliz Seray Tuncay, Jingyu Qian, and Carl A. Gunter. See No Evil: Phishing for Permissions with False Transparency. In *29th USENIX Security Symposium (USENIX Security 20)*. USENIX Association, August 2020.

[60] Sebastian Uellenbeck, Markus Dürmuth, Christopher Wolf, and Thorsten Holz. Quantifying the security of graphical passwords: The case of Android unlock patterns. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, 2013.

[61] Elham Vaziripour, Devon Howard, Jake Tyler, Mark O'Neill, Justin Wu, Kent Seamons, and Daniel Zappala. I Don't Even Have to Bother Them! Using Social Media to Automate the Authentication Ceremony in Secure Messaging. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 2019.

[62] Elham Vaziripour, Justin Wu, Mark O'Neill, Daniel Metro, Josh Cockrell, Timothy Moffett, Jordan Whitehead, Nick Bonner, Kent Seamons, and Daniel Zappala. Action Needed! Helping Users Find and Complete the Authentication Ceremony in Signal. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. USENIX Association, August 2018.

[63] Zack Whittaker. iOS 13: Here are the new security and privacy features you need to know. *TechCrunch*, 2019.

[64] Primal Wijesekera, Joel Reardon, Irwin Reyes, Lynn Tsai, Jung-Wei Chen, Nathan Good, David Wagner, Konstantin Beznosov, and Serge Egelman. Contextualizing privacy decisions for better prediction (and protection). In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 2018.

[65] Allison Woodruff, Vasyl Pihur, Sunny Consolvo, Laura Brandimarte, and Alessandro Acquisti. Would a Privacy Fundamentalist Sell Their DNA for $1000 ... If Nothing Bad Happened as a Result? The Westin Categories, Behavioral Intentions, and Consequences. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*. USENIX Association, 2014. https://www.usenix.org/conference/soups2014/proceedings/presentation/woodruff.

[66] Justin Wu, Cyrus Gattrell, Devon Howard, Jake Tyler, Elham Vaziripour, Daniel Zappala, and Kent Seamons. "Something isn't secure, but I'm not sure how that translates into a problem": Promoting autonomy by designing for understanding in Signal. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, 2019.

[67] Eric Zeng, Shrirang Mare, and Franziska Roesner. End user security and privacy concerns with smart homes. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. USENIX Association, July 2017.

[68] Miaoyi Zeng, Shuaifu Lin, and D. Armstrong. Are All Internet Users' Information Privacy Concerns (IUIPC) Created Equal? 2020. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1048&context=trr.

A Additional plots

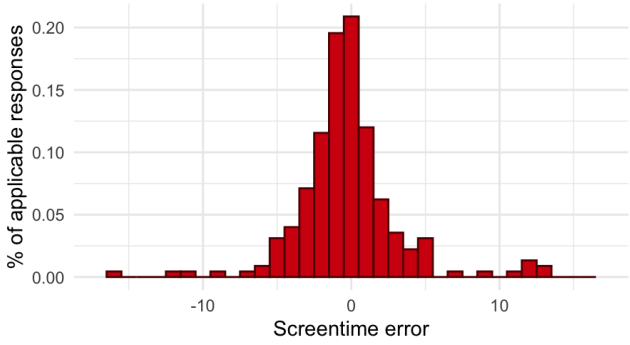
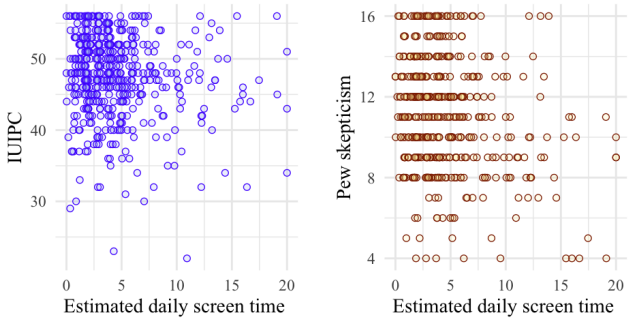
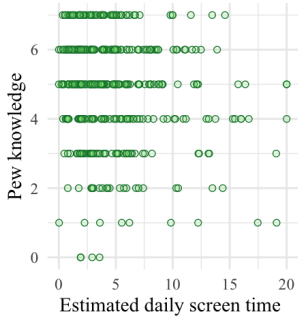


Figure 4: Histogram of differences in participant daily screen-time estimates vs. system screen-time report. The plot includes data from 225 (88 Android, 137 iOS) participants who provided both.



(a) IUIPC-8 (b) Pew skepticism



(c) Pew knowledge

Figure 5: Higher screen-time estimate was associated with lower IUIPC-8, Pew skepticism, and Pew knowledge scales.

B Survey Questionnaire

Consent and validation

1. *Consent form is shown, and consent is given*
2. In what country do you currently reside?
    - ○ United Kingdom
    - ○ United States
    - ○ Ireland
    - ○ Germany
    - ○ France
    - ○ Spain
    - ○ Other

    End survey if not United States
3. Please enter your Prolific ID here:
    [Free text]

Part 1: Device Background Screener Questions

1. How many smartphones do you currently own and use?
    - ○ 0
    - ○ 1
    - ○ 2+

    End survey if 0 is selected
2. For what purposes do you use your smartphone devices? Select all that apply. *[Displayed if "How many smartphones do you currently own and use?" 2+ Is Selected]*
    - ○ Personal
    - ○ Work
    - ○ Other: [Free text]
3. Please consider your PERSONAL smartphone device to be your primary device for the remainder of this survey. *[Displayed if "For what purposes do you use your smartphone devices? Select all that apply." Personal Is Selected AND "How many smartphones do you currently own and use?" 2+ Is Selected]*

    Page Break
4. Please consider your WORK smartphone device to be your primary device for the remainder of this survey. *[Displayed if "For what purposes do you use your smartphone devices? Select all that apply." Personal Is Not Selected AND "How many smartphones do you currently own and use?" 2+ Is Selected]*

    Page Break
5. How frequently do you use a voice assistant on your primary smartphone? (i.e. Hey Siri, OK Google, etc.)
    - ○ Multiple times a day
    - ○ Almost once a day
    - ○ A few times a week
    - ○ A few times a month
    - ○ Almost never
6. Which Operating System do you use for your primary smartphone?
    - ○ iOS
    - ○ Android
    - ○ Windows
    - ○ Other or Not Applicable [Free text]
    - ○ I don't know

    End survey if not iOS or Android
7. Which of the following smart device(s) do you currently own?
    - ○ Smart Speaker
    - ○ Smart Doorbell
    - ○ Smart Thermostat
    - ○ Smart TV
    - ○ Smart Fridge
    - ○ None of the above
    - ○ Other: [Free text]
8. Which smart speaker (voice assistant) do you use? Select all that apply. *[Displayed if "Which of the following smart device(s) do you currently own?" Smart Speaker Is Selected]*
    - ○ Echo Device
    - ○ Google Home
    - ○ Apple HomePod
    - ○ Other: [Free text]
9. How frequently do you use your smart speaker(s)? (i.e. an Echo Device, Google Home, etc.) *[Displayed if "Which of the following smart device(s) do you currently own?" Smart Speaker Is Selected]*
    - ○ Multiple times a day
    - ○ Almost once a day
    - ○ A few times a week
    - ○ A few times a month
    - ○ Almost never

10. How much time do you spend on your primary smartphone on average?
    - Please estimate your daily average in hours. [Slider]

Page Break

11. Do you currently have access to your primary smartphone device? We may ask you to refer to your smartphone during this survey.
    - Yes
    - No

Part 2A: iOS Background Questions

[Displayed if "Which Operating System do you use for your primary smartphone?" iOS Is Selected]

1. What is the iPhone model of your primary smartphone?
    - SE (1st or 2nd generation)
    - 12, 12 Pro, 12 Mini
    - 11, 11 Pro, or 11 Pro Max
    - X, XS, XS Max, or XR
    - 8 or 8 Plus
    - 7 or 7 Plus
    - 6, 6 Plus, 6S, or 6S Plus
    - 5, 5S, or 5C
    - Other: [Free text]
    - I don't know
2. Is your primary smartphone device jailbroken?
    - Yes
    - No
    - I don't know
3. Please navigate through the following steps on your smartphone to answer the following question accurately:
   Settings App > General > About > Software Version
   Which version of iOS does your primary smartphone have? *[Displayed if "Do you currently have access to your primary smartphone device? We may ask you to refer to your smartphone during this survey." Yes Is Selected]*
    - iOS 14
    - iOS 13
    - iOS 12
    - iOS 11
    - iOS 10
    - iOS 9
    - Other: [Free text]

Page Break

4. Please navigate through the following steps on your smartphone to answer the following question accurately:
   Settings > Screen Time
   Can you see your daily average in screen time for the past week? Note that some phones show daily numbers but don't show an average, please select no if that's the case. *[Displayed if "Do you currently have access to your primary smartphone device? We may ask you to refer to your smartphone during this survey." Yes Is Selected]*
    - Yes
    - No

Page Break

5. How much time on average do you spend on your primary smartphone? Please report your daily average. *[Displayed if "Please navigate through the following steps on your smartphone to answer the following question accurately:*
   Settings > Screen Time
   Can you see your daily average in screen time for the past week? Note that some phones show daily numbers but don't show an average, please select no if that's the case" Yes Is Selected]
    - hour(s) [Free text]
    - minute(s) [Free text]

Part 2B: Android Background Questions

[Displayed if "Which Operating System do you use for your primary smartphone?" Android Is Selected]

1. What is the Android model of your primary smartphone?
    - Blackberry
    - HTC
    - Lenovo
    - LG
    - Motorola
    - Nexus
    - Nokia
    - Google Pixel

- Samsung Galaxy
- Sony Xperia
- Other: [Free text]

2. Is your primary smartphone device rooted?
   - My device is rooted
   - My device is non-rooted
   - I don't know
3. Please navigate through the following steps on your smartphone to answer the following question accurately:
   Settings App > About Phone > Android Version Settings App > About Phone > Software Information > Android Version
   Which version of Android does your primary smartphone have?
   - Android 11
   - Android 10
   - Pie 9.0
   - Oreo 8.0-8.1
   - Nougat 7.0-7.1.2
   - Marshmallow 6.0-6.0.1
   - Lollipop 5.0-5.1.1
   - KitKat 4.4-4.4.4
   - Other: [Free text]

Page Break

4. Please navigate through the following steps on your smartphone to answer the following question accurately:
   Settings > Digital Wellbeing
   Can you see your daily average in screen time for the past week? Note that some phones show daily numbers but don't show an average, please select no if that's the case. *[Displayed if "Do you currently have access to your primary smartphone device? We may ask you to refer to your smartphone during this survey." Yes Is Selected]*
   - Yes
   - No

Page Break

5. How much time do you spend on your primary smartphone on average? Please report your daily average. *[Displayed if "Please navigate through the following steps on your smartphone to answer the following question accurately:*
   Settings > Digital Wellbeing
   Can you see your daily average in screen time for the past week? Note that some phones show daily numbers but don't show an average, please select no if that's the case." Yes Is Selected]
   - hour(s) [Free text]
   - minute(s) [Free text]

Part 3: Pew Knowledge Questions

1. What does it mean when a website has "https://" at the beginning of its URL, as opposed to "http://" without the "s"?
   - Information entered into the site is encrypted
   - The content on the site is safe for children
   - The site is only accessible to people in certain countries
   - The site has been verified as trustworthy
   - Not sure
2. Many web browsers offer a feature known as "private browsing" or "incognito mode." If someone opens a webpage on their computer at work using incognito mode, which of the following groups will NOT be able to see their online activities?
   - The group that runs their company's internal computer network
   - Their company's internet service provider
   - A coworker who uses the same computer
   - The websites they visit while in private browsing mode
   - Not sure
3. When a website has a privacy policy, it means that the site…
   - Has created a contract between itself and its users about how it will use their data
   - Will not share its users' personal information with third parties
   - Adheres to federal guidelines about deceptive advertising practices
   - Does not retain any personally identifying information about its users
   - Not sure

4. If a website uses cookies, it means that the site ...
    - Can see the content of all the files on the device you are using
    - Is not a risk to infect your device with a computer virus
    - Will automatically prompt you to update your web browser software if it is out of date
    - Can track your visits and activity on the site
    - Not sure
5. Which of the following is the largest source of revenue for most major social media platforms?
    - Exclusive licensing deals with internet service providers and cellphone manufacturers
    - Allowing companies to purchase advertisements on their platforms
    - Hosting conferences for social media influencers
    - Providing consulting services to corporate clients
    - Not sure
6. Where might someone encounter a phishing scam?
    - In an email
    - On social media
    - In a text message
    - On a website
    - All of the above
    - None of the above
    - Not sure
7. The term "net neutrality" describes the principle that ...
    - Internet service providers should treat all traffic on their networks equally
    - Social media platforms must give equal visibility to conservative and liberal points of view
    - Online advertisers cannot post ads for housing or jobs that are only visible to people of a certain race
    - The government cannot censor online speech
    - Not sure

Part 4: SA-6

1. Please rate your agreement or disagreement with the following statements. *Options: {Strongly agree, Agree, Neutral, Disagree, Strongly disagree}*
    - I seek out opportunities to learn about security measures that are relevant to me.
    - I am extremely motivated to take all the steps needed to keep my online data and accounts safe.
    - Generally, I diligently follow a routine about security practices.
    - I often am interested in articles about security threats.
    - I always pay attention to experts' advice about the steps I need to take to keep my online data and accounts safe.
    - I am extremely knowledgeable about all the steps needed to keep my online data and accounts safe.

Page Break

2. You answered you [participant's selected answer] with the following statement: I often am interested in articles about security threats. Why did you feel this way? Please explain why you chose this answer. [Free text] *(Used as an attention check)*

Part 5: IUIPC

Please rate your agreement or disagreement with the following statements. *Options: {Strongly agree, Agree, Somewhat agree, Neutral, Somewhat disagree, Disagree, Strongly disagree}*

1. **Control**
    - Consumer online privacy is really a matter of consumers' right to exercise control and autonomy over decisions about how their information is collected, used, and shared.
    - Consumer control of personal information lies at the heart of consumer privacy.
    - I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction.
2. **Awareness**
    - Companies seeking information online should disclose the way the data are collected, processed, and used.
    - A good consumer online privacy policy should have a clear and conspicuous disclosure.
    - It is very important to me that I am aware and knowledgeable about how my personal information will be used.
3. **Collection**
    - It usually bothers me when online companies ask me for personal information.

- When online companies ask me for personal information, I sometimes think twice before providing it.
- It bothers me to give personal information to so many online companies.
- I'm concerned that online companies are collecting too much personal information about me.

Part 6: Pew Company Questions

1. How confident are you, if at all, that companies will do the following things? *Options: {Very confident, Somewhat confident, Not too confident, Not confident at all}*
   - Follow what their privacy policies say they will do with your personal information
   - Promptly notify you if your personal data has been misused or compromised
   - Publicly admit mistakes and take responsibility when they misuse or compromise their users' personal data
   - Use your personal information in ways you will feel comfortable with
   - Be held accountable by the government if they misuse or compromise your data

Page Break

2. You answered you are [participant's selected response] that companies will: Publicly admit mistakes and take responsibility when they misuse or compromise their users' personal data. Why did you feel this way? Please explain why you chose this answer. [Free text] *(Used as an attention check)*

Part 7: How Well Do My Results Generalize? (as it appears in [46])

1. Do you feel as you already know enough about . . . *Options: {Already know enough, Would like to learn more, Does not apply, Do not know}*
   - Choosing strong passwords to protect your online accounts
   - Managing the privacy settings for the information you share online
   - Understanding the privacy policies of the websites and applications you use
   - Protecting the security of your devices when using public Wifi networks
   - Protecting your computer or mobile devices from viruses and malware
   - Avoiding online scams and fraudulent requests for your personal information

Part 8: Demographics

1. Please indicate your age. If you'd prefer not to answer, you can skip this question.
   - Use the slider to indicate your age. [Slider]
2. What gender do you best identify with?
   - Man
   - Woman
   - Non-binary
   - Prefer to self-describe [Free text]
   - Prefer not to answer
3. Which of the following best describes your race? Select all that apply.
   - White
   - Black or African American
   - American Indian or Alaska Native
   - Hispanic or Latino
   - Asian
   - Native Hawaiian or Pacific Islander
   - Other [Free text]
   - Prefer not to answer
4. Please specify the highest degree of level of school you have completed or currently attending.
   - No high school degree
   - High school graduate, diploma or the equivalent (for example, GED)
   - Some college credit, no degree
   - Trade, technical, vocational training
   - Associate's degree
   - Bachelor's degree
   - Master's degree
   - Professional degree
   - Doctorate degree
   - Other [Free text]
   - Prefer not to answer
5. What is your current employment status?
   - Employed Full-Time
   - Employed Part-Time
   - Self-employed

- ○ Unemployed
- ○ Student
- ○ Home-maker
- ○ Retired
- ○ Disabled
- ○ Prefer not to answer

6. What is your annual household income?
   - ○ Up to $25,000
   - ○ $25,000 to $49,999
   - ○ $50,000 to $74,999
   - ○ $75,000 to $99,999
   - ○ $100,000 or more
   - ○ Prefer not to answer
7. How frequently do you give computer or technology advice (e.g., to friends, family, or colleagues)?
   - ○ Almost always
   - ○ Often
   - ○ Sometimes
   - ○ Rarely
   - ○ Never

end of survey