Replication: Measuring User Perceptions in Smartphone Security and Privacy in Germany

Maxim Schessler
maxim.schessler@uni-bonn.de
University of Bonn
Germany

Eva Gerlitz
gerlitz@cs.uni-bonn.de
Fraunhofer FKIE
Germany

Maximilian Häring
haering@cs.uni-bonn.de
University of Bonn
Germany

Matthew Smith
smith@cs.uni-bonn.de
University of Bonn, Fraunhofer FKIE
Germany

ABSTRACT

In 2021, smartphones are ubiquitous and offer numerous possibilities. Previous work found that the interaction of people with smartphones is influenced by the perception of the devices' security and privacy. Therefore, it is important to learn about the relations of behavior and perception, to better understand challenges and design systems accordingly. In 2012, a study conducted in the US found differences in how participants perceive their devices' (laptop vs. smartphone) security and privacy. At the time, smartphones were still relatively new, and the participants had significantly less trust in their smartphones compared to laptops. Since then, smartphones and computers have improved a lot in soft- and hardware, and people are now much more familiar with smartphones in general. To understand the current state and the development of device perception, we repeated the original study in Germany, with minor adaptions, as online interviews with 30 participants. While the US study suggested security concerns limit smartphone usage, we did not find significant differences that would restrict the use of smartphones today. However, there are still comparatively great concerns about privacy on smartphones.

CCS CONCEPTS

• **Security and privacy** → *Human and societal aspects of security and privacy*; • **Human-centered computing** → *Human computer interaction (HCI).*

KEYWORDS

smartphone, smartphone usage, laptop usage

ACM Reference Format:
Maxim Schessler, Eva Gerlitz, Maximilian Häring, and Matthew Smith. 2021. Replication: Measuring User Perceptions in Smartphone Security and Privacy in Germany. In *European Symposium on Usable Security 2021 (EuroUSEC '21), October 11–12, 2021, Karlsruhe, Germany*. ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3481357.3481511

EuroUSEC '21, October 11–12, 2021, Karlsruhe, Germany

ACM ISBN 978-1-4503-8423-0/21/10…$15.00
https://doi.org/10.1145/3481357.3481511

1 INTRODUCTION

With the first iPhone release in 2007, the smartphone market was relatively young when in 2012, Chin et al. [16] conducted a study to examine users' security and privacy perceptions on smartphones and laptops. In the following years until today, the use of smartphones has increased massively. In the United States of America, 39% of the adult population owned a smartphone in 2012, compared to 81% in 2019 [24]. Furthermore, in 2019 time spent on mobile devices passed watching TV for the first time in the U.S.A., with an average of over three and a half hours per day. Most of it, namely 70% or around three hours, is spent on smartphones [18]. This means that far more people own a smartphone and use it more frequently. With this growth, new technological possibilities arise. Online banking, 2Fa, using map applications or messengers is ubiquitous. Currently, there are many discussions about bringing more sensitive data to devices like smartphones, i.e., medical files. We were therefore interested in whether and how the situation of trust in those devices changed in the last 9 years. For this, we ran a study close to the one by Chin et al. [16] in 2012. We conducted 30 online[1] interviews with persons residing in Germany. The structure and content were based heavily on a study by Chin et al. [16], with us testing the willingness to perform certain tasks, security and privacy perception, asking for worries and fears, and installation behavior of the participants.

We can report no statistically significant differences in the willingness to perform security and privacy-related tasks on laptops versus smartphones, and while there are still slightly more concerns on smartphones, it should not be enough to impede general smartphone usage in contrast to laptop usage. Although our results indicate a positive development in smartphone perception, some circumstances make it hard to compare the studies directly. The presented study was carried out in a different country, with a smaller, and in particular, younger group of participants compared to the original. Therefore, the results should only be taken as indicative of the situation.

[1] This was not initially planned but necessary due to the global COVID-19 pandemic.

The rest of the paper is structured as follows: First, we shortly discuss the related work and literature relevant to this study. Then we explain our methodology, including the differences to the original study. Afterward, we present our results in two parts, focusing first on privacy and security perception and then application installation. At last, we discuss our results, their legitimacy, and their importance.

2 RELATED WORK

In the following, we give an overview of the findings of the study we used as a template by Chin et al. [16], related literature done since then, and an overview of the relevant technological improvements since 2012.

2.1 Security and Privacy Perceptions

In 2012, Chin et al. [16] interviewed 60 participants about their laptop and smartphone habits regarding security and privacy. The aim was to (1) uncover if participants use their smartphones less because of security concerns and (2) gain information about their installation habits, especially about the trustworthiness of an application. The authors found that users are less likely to do security and privacy-critical tasks on their smartphones than on laptops for many reasons. This includes fear of theft and loss of data, a false understanding of network communication, problems with the user interface (UI), and no trust in new and unknown smartphone applications. Therefore the authors propose several ways to remedy this problem: user education, new security indicators, UI usability improvements, better backup options, and better remote lock services.

The following paragraphs compare their findings concerning security and privacy perceptions to research done since then.

Security Perceptions. Chin et al. [16] found many participants who switched from their smartphone to a computer while performing a task they deem privacy or security important, indicating security concerns on smartphones. Newer research confirms this finding. Analyzing a large European online retailer in 2018, Haan et al. [17] found a positive correlation of users switching devices from smartphone to computer, when products cost more and costumers have less experience with the platform. In 2019, Liu et al. [22] observed a lower perceived financial risk and higher spending, if customers use an application instead of the mobile website on their smartphone and a case study with data from 629 users by McGill et al. in 2017 [23] identified that users believe it to be harder to secure their smartphone to the same safety level a computer has. As a result, they make even less effort to secure them. The authors additionally examined user behavior on smartphones and computers, resulting in a similar finding as Chin et al. in 2012 [16]: online banking and shopping are performed more often on a computer. However, they did not differentiate between security and usability reasons, as participants merely reported the devices they perform these actions on.

The original study by Chin et al. [16] shows, that there are differences in perception users show in regards to the Operating System (OS). This was confirmed by other research. For example, in 2014, Reinfelder et al. [26] dealt with the differences in security and privacy awareness of Android and iOS users, finding Android users to mention more risks. Research by Ünal et al. in 2015 [31] investigated mobile commerce on Android and iOS and saw a more positive attitude towards it by iOS users.

There are several factors users consider when installing an application. Chin et al. [16] found that user reviews, recommendations from friends, and popularity are some of the strongest by which users decide. In contrast, the app developer and the related brand loyalty were not reported as important by the participants. Research published in 2017 [20] has similar findings but also gives permissions, a concept that changed over the years, before installation more weight and importance. Furthermore, there seems to be strong enough trust in the popular app markets, to mostly disregard security concerns in 2018 [15].

Privacy Issues. Privacy was something participants were significantly more concerned about on smartphones than laptops in 2012 [16]. Research by Gu et al. from 2017 [20] found Android users have privacy concerns if apps need permissions they consider sensitive. However, this is alleviated by the app's popularity or a good justification for why the permissions are needed. An analysis of installed apps by Furuni et al. in 2020 [19] shows the concerns participants have are justified, with many of the applications misusing permissions and data they do not need for their primary task. Furthermore, research by Balapour et al. from 2020 [11] found privacy perception of apps influences their security perception. While much of this could indicate people would more carefully consider which app to use or install, the actual behaviour often contradicts users' privacy concerns, as was observed by Barth et al. in 2019 [12]. The authors found that other aspects, such as cost or functionality of the apps, are often weighted higher than privacy concerns.

2.2 Technological Development

Many of the recommendations by Chin et al., such as better backup- or remote lock options, usability improvements to interfaces, and user education, have been worked on over the years. There have been major changes in the design and usability of backups (Google Drive in 2012, Apple iCloud in 2011) [4, 5] and unlocking (e.g., introduction of TouchID in 2013 and FaceID in 2017) [6, 7, 13]. User Education is something that takes time and social penetration of the respective technologies is seen as desirable by many countries and institutions, leading to initiatives for improving technological literacy and digital competence. An example is the in 2017 published European Digital Competence Framework [14], setting standards for education and skill assessment in Europe. We expect that users today are better educated about technological and digital aspects than in 2012. The fear of missing important information or clicking the wrong button is something mentioned by participants in the original study [16]. There is much research and improvement in user interfaces (UI) and usability made in the last decade [8, 25, 28]. Today's bigger screen size are better for usability in regards to response rate and Fitts' Law values [30]. Besides, the permission systems for installed apps on iOS and Android got reworked over time, and now both are viewed more positively compared to the old system [27].

3 METHODOLOGY

To be as close as possible to Chin et al. [16], we contacted the authors. Thankfully they shared the study material with us, i.e., their complete interview guide. Sharing the original data set was not possible. We used the study design and adapted them to our specific situation. For example, we conducted the study in Germany, while the original study was run in the US. Initially, we planned on recruiting within the US, but due to high transaction fees and limited resources, this would have halved our sample size. We translated the questions to German as close as possible to the original meaning. Instead of inviting participants to our lab, we interviewed them online to comply with COVID-19 regulations. Contents-wise, some changes to the interviews were needed to be up-to-date (e.g., application examples) and to accommodate the online interviews. Section 3.1 explains the different parts of the study and shows our adoptions to the original study in detail. An overview of all changes can be seen in Appendix C in Table 3.

3.1 Surveys and Interview

Chin et al. [16] conducted structured interviews consisting of activities like filling out surveys and sorting note cards for which participants had to bring their laptop and smartphone. To carry out all activities comparable to the study from 2012, the interview itself was held and recorded over Zoom (duration of 45-90min), and all activities had to be solved using an online survey. Like in 2012, it was ensured that the participants had the laptop and smartphone available they specified at the time of recruitment.

The survey was divided into several parts in accordance with the paper surveys handed out by Chin et al. [16]. The interview (with intermediary surveys) can be found in Appendix B. In the following, we will give details about the different parts and the changes we made, all of which can be seen summarized in Table 3.

Demographic and Definition: We asked participants for their age, gender, their education, household income, and technological savviness. Furthermore, we defined what an "application" is and gave several examples about the difference of the meaning in contrast to a website.

Laptop - Usage. The first survey concerned the participants' general laptop usage. We asked to verify the OS the participants use to ensure it is the same they mentioned in the recruitment. Several more questions followed concerning for example, the time-frame of ownership, other devices, and their uses cases, sharing habits regarding their laptops or types of installed applications.

Laptop - Installation Factors. In the next part, the participants were asked to do a card sorting activity about the importance of several factors in the choosing process of a laptop application. The order of the factors was randomized by the survey software. Using a drag and drop system, they were supposed to sort several installation factors (e.g., price, popularity, user reviews, and ratings, etc.). The original study added the "permission" card only to the Android part of the card sorting activity. This made sense as in 2012, the other OS did not support a user permission system. Today, all OS encountered in this study have some sort of permission system in place. We, therefore, included the "permission" card in each sorting activity.

The goal for the participant was to sort them into three categories: what they always consider, sometimes consider, and never or rarely consider. Factors in the first two were to be sorted by importance in their own category.
In contrast to the original study, no pictures were included on the cards anymore. This was decided because the original cards had no overall design structure as some cards had pictures and some only words. We found that including pictures in the online card sorting would make the activity clunky and confusing.

Laptop - Installed Applications. We helped and explained how to navigate to a list of installed applications on the participants' laptops. We asked them to count all applications the interviewees installed themselves, skipping any pre-installed ones. Then we asked them to sort the list by installation date and requested them to take the first seven applications on their list and answer several questions for each of them (about the cost, where they heard about the app, etc.). This was a timed section (10min) in the original, resulting in an average of 7 applications. Considering this and removing variance, we chose to ask for a fixed number of 7 apps.

Asking the participants to count all their installed applications was moved from the original study's *Laptop Usage* to this part to improve the interview flow.

Smartphone Parts. The previous three laptop parts were repeated with questions about the participants' smartphones. We only changed the order used in the *Installed Applications* part when sorting installed apps. In the original study, the sorting was alphabetically for Android and in the order on the home screen for iOS users. Since there is still no possibility to sort the applications equally for all operating systems, we decided to use the same approach.

Structured Interview. The last part was a structured interview we held to determine which tasks users had or would perform on which device. There were four questions for each task:

- If they ever did the task on a laptop website?
- If they ever did the task on a laptop app?
- If they ever did the task on a smartphone website?
- If they ever did the task on a smartphone app?

If the participant denied doing so, we asked if they would and why (not). In contrast to the original study, if participants had never performed a task (neither over a website or an app), we asked if they, in general, would. In contrast, the original study asked if they would install an application for it. The tasks were entering their SSN, shopping, managing health documents, online banking, finance management, sharing photos, using something that can charge money, work email and using location-aware services.

Additional changes. Additional to the previously mentioned changes, we had to make some general and minor changes to improve the online interview experience and adapt it to today. For example, we added additional questions to validate the gender, age, and device information we got told in the recruitment and then modernized the study. The examples used in the original study were sometimes changed to newer and better-known alternatives. Additionally, we added pre-made selection options to some of the questions to improve the online surveys' usability. An example is a question about types of installed applications, where we offered a list that covered

possible app categories ([1]) instead of leaving this as a free text answer.

We also added additional questions that covered the demographic of the participant (education, income, technological savviness), asked about tablet usage, and aimed for a better differentiation on how long the participant has had their devices.

3.2 Recruitment

We recruited participants in Germany in August 2020. Like the original study, we used a service similar to Craigslist called eBay Kleinanzeigen [2]. There we published the advert in the "Mini jobs" section. Due to the online nature of the study, participants from all over Germany could and did take part. Similar to the original study, it was framed as a smartphone study, without hints to security and privacy. We offered 30 Euro as remuneration, and the only requirements were to own a personal laptop and smartphone and be 18 years or older. The translated call for participants can be found in Appendix A.

Findings by Chin et al. [16] indicate that the mobility of a laptop is linked to its security perception as it makes situations like bringing the device to a cafe possible. To achieve useful data for comparison, it was decided to only allow laptops, even though the online interview would have made it possible to include stationary computers. If interested to participate in the study we asked people to send us their age, gender, and a list of their devices, including operating systems and an indication of which they use primarily.

Chin et al. [16] recruited participants with four different combinations of operating systems (Windows/Android, Windows/iOS, macOS/Android, macOS/iOS) for the study. As these are still systems with a major market share, we chose to do the same. To not tempt participants to cheat with suitable devices, we did not mention OS requirements during recruiting. However, as we had too few applicants with Apple devices, we changed the advert halfway through the recruitment time frame and mentioned that we prefer participants with at least one Apple device.

3.3 Data analysis

Since a large part of the structural interviews were surveys and similar activities, we analyzed much of the data statistically. In all but three cases, we used the same statistical test as the original study. For statistical testing of the task willingness in Section 4.1.1, we performed exact McNemar tests. As in the original study for the differences in perception of security and privacy (Section 4.1.2), we used the chi-square goodness of fit test, but in contrast to Chin et al. [16] we reduced the degrees of freedom from 4 to 2 combining the categories "a lot more" and "a lot less" with "more" and "less", since we had only one participant answering "a lot less" and none "a lot more". The original study used a one-tailed t-test when comparing the willingness to try out apps from unknown brands (Section 4.2.3). This test requires normally distributed data, which is why we decided to replace it with the Wilcoxon signed rank test. For statistical tests, we always report the p-values. For chi-square tests, we also note the χ^2 and degrees of freedom, and for the Wilcoxon signed rank test and Mann-Whitney test, the z value. We use the significance level (alpha) of 0.05 for every statistical test.

To calculate the number of participants needed to show the same effect as seen for the statistically significant results of the original study, we re-performed the statistical tests from Chin et al. [16] to get the effect sizes, and performed power analyses. However, since the original study's raw data could not be shared, this was not possible for all mentioned tests. In Section 4, we compare our results to data extracted from the published paper, considering the needed number of participants.

Free text answers were coded by one researcher, using the themes from the original study as a basis for the codebook. All mentioned quotes were discussed by two researchers.

3.4 Demographics

Forty-six people applied for the study, of which we invited 30, prioritizing older participants and apple users for balancing reasons. Three participants did not show up for the study and were replaced. Out of the 30 participants 15 used the combination of Windows and Android. The other half used at least one Apple device. Table 1 shows the demographics of our participants.

Because of our limited recruitment period and lack of participants we had not as much leeway in balancing our participant pool. We had more men inquiring to participate, which leads to us interviewing 17 men and 13 women. Like in the original study, most participants belong to the youngest age group, and we had trouble finding 48 years old and up. We had a younger participant base than the original study.

Table 1: Participants' demographics ($N = 30$)

Demographic	Number	Percent
Gender		
Female	13	43%
Male	17	57%
Age		
18 - 27	18	60%
28 - 37	7	23%
38 - 47	3	10%
48+	2	7%
Laptop OS		
Windows	21	70%
macOS	9	30%
Smartphone OS		
Android	17	57%
iOS	13	43%

3.5 Ethics

The Research Ethics Board of our university reviewed and approved the study. In the interviews, we followed the standard routine to ensure no involved person would take any harm. The interview could be paused or stopped entirely without mentioning any reason at any time, and any question could be skipped. No person made use of this option. In the transcription of the interviews, any identifying information was removed.

4 RESULTS

In this section, we present the data from the interviews, focusing first on security and privacy perceptions and later on how/why applications are installed. We also compare the results to findings from Chin et al. [16]. All participants got an ID assigned consisting of two letters for the OS combinations (WA, WI, MA, MI) and a number. We will note the ID with every quotation.

4.1 Security and Privacy Perception

The original study examined the security and privacy perception of users and the difference between devices. We first examine the same three aspects as the original study: The willingness to perform a specific task on their devices, the difference users see in their devices' security and privacy, and the biggest worries and fears they have regarding their smartphones. We put the results in comparison to the original ones and look at the influence the OS has (e.g., iOS vs. Android).

4.1.1 Willingness to perform tasks. In 2012, Chin et al. [16] found that the willingness to perform a task on a device was influenced by its perceived security as well as its usability. The authors asked the participants if they did or would perform some tasks (Entering their SSN, online shopping, sharing photos, etc.) on their devices. If they denied, they were asked for the reasons. Back then, the authors found significant less participants willing to enter their Social Security number (exact McNemar, $p < 0.0001$), manage health data (exact McNemar, $p = 0.0002$), do online banking ($\chi^2(1)= 9.0, p = 0.0027$) and online shopping (exact McNemar, $p = 0.0002$) on their smartphone in comparison to their laptop.

Since then, many improvements regarding security and usability in smartphones have been implemented, as summarized in subsection 2.2. Additionally, people now had more time to get used to smartphones and integrate them into their daily lives. We thus believed that both areas (security perception and usability) improved enough since the original study to find a difference in today's willingness to perform certain tasks. To test this, we asked the participants the same question as in the original study.

For this part, we did not have enough data, i.e., the effect sizes or group sizes, of the original study to calculate the number of needed participants for this study. To have some estimation, we thus assumed that most participants who did not want to perform a specific task on their laptops were also unwilling to perform it on their smartphones and set the probability that this was the case to 1%. To show the same effect following this assumption, we would have needed 8 (SSN), 28 (Shopping), 57 (Health Data), and 69 (Bank Account) participants. Since we interviewed 30 participants, the difference for SSN and Shopping should have been visible, if existing. Yet, non of the tests were statistically significant for the German sample.

The results in comparison to those from 2012 can be seen in Table 2. Reasons for not performing tasks in this study included security concerns, such as low trust in device security, and non-security reasons, such as preferring longer tasks on laptops due to larger screens or better work environments and rather working on their smartphones on shorter tasks due to the easy and fast access. We also saw participants who would, in general, perform a task on both devices but favored one of them.

There is still a slight trend, that more participants rejected a task on their smartphone because of security reasons, with the biggest gap in using the bank account (Laptop $_{2020}$: 0, Smartphone $_{2020}$: 3 | exact McNemar, $p = 0.25$). Additionally, in 2012, 18% cited security as the cause to not use online shopping on their smartphones, while participants in 2020 rejected online shopping on their phones solely due to the smaller screen size.
Interestingly, four participants mentioned security as the reason not to perform a task on their smartphone, while at the end of the interview, they told us that they worry more about security on the laptop. The amount of data on the device and the higher chance of device theft were mentioned as reasons. After a reminder of the answers before, one was surprised and told us: "I had a virus on a computer and believe it is easier to get them there. I have strange habits, maybe something I got from my parents."(ID: WA15). There seem to be some subconscious habitual biases against smartphones.

In the following, we will give details on the results for the four areas for which Chin et al. [16] found statistically significant differences between laptops and smartphones.

Task: Enter SSN. Entering the Social Security Number was the task with the biggest difference between laptop and smartphone in the original study. Back then, 60% [16] would not enter the SSN on their smartphone (laptop $_{2012}$: 7%) because of security reasons. While there are probably some cultural differences, with people in the USA attributing more importance to their SSN, we can only report 4 (13%) participants not willing to enter it on their phone. Two participants would never enter the SSN online. The other two had security concerns on their phone but mostly thought about usability and found it easier on their laptop.

Task: Shopping. Shopping is an action where the original study found a significant difference between smartphones and laptops. No one had any concerns on their laptops, but 18% would not shop on their smartphone because of security reasons. We did not have a single participant mentioning security reasons in regards to online shopping. There were some participants favoring online shopping on their laptops or tablets because of the bigger screen and some using their smartphone more because of the faster and easier access, with two therefore not willing to shop on their smartphone, but no security concerns came up.

Task: Health Data. There was a statistically significant difference in the original study (laptop $_{2012}$: 4%, smartphone $_{2012}$: 18%), with more participants not wanting to manage their health documents on their smartphone. We had a higher percentage of users citing security as a reason on laptops than in 2012 (laptop $_{2020}$: 10%, smartphone $_{2020}$: 13%), but in absolutes, it was only three overlapping participants that would not input health data on either device and one more on his smartphone. Even on the contrary, participants mentioned how much easier and time-efficient it is to send and manage documents to or from the health insurance on their "new" phone applications.

Task: Bank Account. Chin et al. found a statistically significant difference, and while not statistically significant (we would have needed to interview at least 69 participants to show the same effect if present), we had our biggest difference between devices in this aspect. There were only 3 participants having strong enough

Table 2: The number of participants who would not perform a specific task in the 2020 study (30 participants) and in the 2012 study (60 participants) [16]. Significant differences between the devices are bold.

Task	Laptop 2020		Smartphone 2020		Laptop 2012		Smartphone 2012	
	Security	Other	Security	Other	Security	Other	Security	Other
Enter SSN	7%	0%	13%	7%	**7%**	**0%**	**60%**	**8%**
Shopping	0%	0%	0%	7%	**0%**	**0%**	**18%**	**10%**
Health data	10%	3%	13%	0%	**4%**	**12%**	**18%**	**20%**
Bank account	0%	0%	10%	0%	**2%**	**0%**	**13%**	**3%**
Finance mgmt.	0%	10%	3%	10%	0%	15%	12%	12%
Share photos	0%	13%	0%	3%	0%	3%	3%	8%
Charge money	0%	0%	0%	0%	3%	14%	10%	15%
Work email	0%	7%	0%	10%	0%	5%	0%	10%
Location	7%	0%	0%	0%	2%	0%	0%	0%

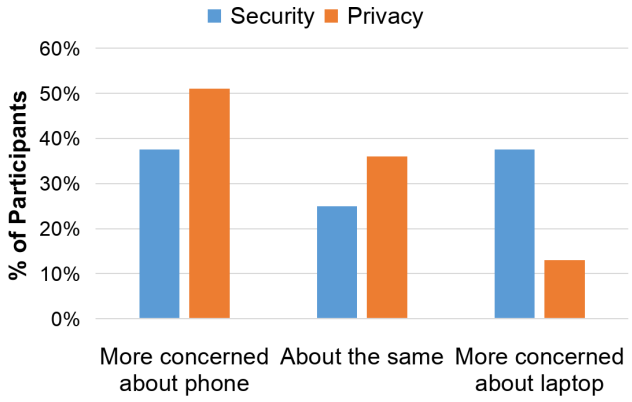
security concerns to reject online banking, all of them only on their smartphones. That is a pretty similar margin to the one in the original study. Maybe it is culturally influenced (e.g., popularity of cash in Germany [10, 21]), but one mentioned wanting to try online banking and just not being informed right now how safe it is (default trust higher in laptop). Another one (ID: WA06) uses an iPad for online banking and would use it on an iPhone but does not trust their Android device. So it is not only about laptop vs. smartphone but also OS differences. We will further look into this in Section 4.1.4.

4.1.2 Differences in Perception. In this part, we tried to understand which device our participants are more concerned regarding security and privacy. Chin et al. [16] did not observe a difference in security perception but saw statistically significant lower trust in smartphone privacy (more concern on laptop $_{2012}$: 13%, smartphone $_{2012}$: 51%), as seen in Figure 1a.

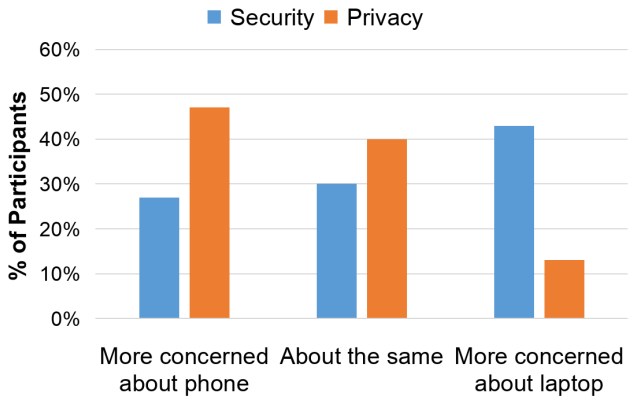
When calculating the number of needed participants, we re-performed a χ^2-Test to identify the effect size but using a degree of freedom of 2 instead of 4, since we did not have complete data of the original study. We would have needed 89 participants.

An overview of the results of this study can be seen in Figure 1b. We saw more participants concerned about security on their laptop (laptop $_{2020}$: 43%, smartphone $_{2020}$: 27%), but more privacy concerns on smartphones (laptop $_{2020}$: 13%, smartphone $_{2020}$: 47%). These directions of perception are similar to the original study results, where the authors found a statistically significant difference in privacy concern between devices. While we have a similar distribution of percentages they are not statistically significant, possibly due to a too small sample size (security: $\chi^2(2)= 1.400, p = 0.4966$ | privacy: $\chi^2(2)= 5.6, p = 0.0608$).

Explaining why they had differences in concern between devices, some participants did remember having heard or even suffered laptop viruses themselves. However, no such thing occurred on smartphones. Smartphones often had the mobility aspect and ease of loss against them. We did not observe any networking misconceptions as mentioned in the original study, e.g., the internet connection on a smartphone not being as secure as on the laptop. There was only one participant explicitly mentioning the internet connection in a discussion, refusing to use unknown public WiFi for security-sensitive tasks.



(a) 2012 [16]



(b) 2020

Figure 1: Participants security and privacy concerns on their devices

When talking about their smartphones, many participants (privacy: 10 out of 14, security: 6 out of 8) decided about which device they have more concerns, by mostly concentrating on the amount of data and the device's frequency of use. A similar observation was made on laptops (privacy: 3 out of 4, security: 3 out of 13). This indicates the data on the device is the main reason for any concerns, more than the device type or other reasons.
Another interesting statement we heard was: "I think there are more demands from apps to access things."(ID: MI05) When talking about why there is more privacy concern on the smartphone. This might indicate that a visible permission system can negatively impact a person's privacy perception of the device.

Some participants' trust in their devices depended on if they use an application or a browser. Someone stated: "I would rather not do it on the smartphone in the browser, the laptop browser feels safer."(ID: WA06) This person, however, had no concerns regarding apps on the smartphone. Another participant expressed the belief that "It is easier to fake a web page on an iPhone."(ID: WI02) We also asked participants about the differences between smartphones and tablets. Participants saw no difference in using the devices other than a more frequent usage of the phone and using tablets more for entertainment like watching videos and gaming.

4.1.3 Worries and Fears. We asked the same question about smartphone concerns as in the original study. Similarly, we mainly heard security and privacy reasons. It was positioned at the end of the interview, after many other questions concerning security. We thus assume the answers are influenced by this. More than a third of the participants worried about unauthorized data access, including photos, videos, messages, and passwords. Some told us they do not worry at all (4 participants). Some reasons were no trust in apps (3 participants), device loss (4 participants), and the lack of privacy (4 participants). So there was still some worry about device and data loss but not nearly as much as in the original study (phone loss $_{2020}$: 13% | phone loss $_{2012}$: 28%). After asking if they do not have backups, the answer was they do, but still worry because: "I had problems recovering data before. Since you don't know whether everything is really there, you have to check it regularly."(ID: WA08).
Looking at the main worries found in the original study, we observed only one participant who was concerned about the battery of his smartphone, but none who worried about signal strength.

4.1.4 OS Influence. As mentioned before, three participants were remarking they trust their Apple device more than alternatives. While we do not have a big enough sample size and differences in OS perception was not an explicit question, only one participant explicitly mentioned trusting his Apple device less. The reason was some recent news about vulnerabilities in iPhones, ignoring that similar circumstances also happen on Windows and Android. Most were confident in the security and privacy of their Apple devices, some even citing this as reasons to buy them. One participant who would not use online banking on an Android smartphone told us: "No, only on my iPad". After we asked him about his iPad he answered: "Yes, I trust it more than my laptop(Windows) or Android. I had only good experiences with it, no problems and everything is really easy. I trust the brand Apple very much."(ID: WA06). Therefore we believe any studies trying to understand differences in computer and smartphone perception and usage should strongly take into account the potential influence the device OS/brand has.

4.2 Application Installation

Downloaded and installed applications are one of the reasons for security breaches on smartphones [9]. Therefore, in this section, we examine possible reasons for unsafe installation decisions and compare the observations to the original study.

4.2.1 (De-)installation Frequency. Every performed installation is a possible added risk for device security. We found significantly more participants removing applications regularly on their phone compared to their laptops (laptop $_{2020}$: 10, smartphone $_{2020}$: 21 | exact McNemar: $p = 0.0034$). However, there was only one participant mentioning security-related concerns in this context who stated removing apps because of permissions like location. The most mentioned reason for removing apps was no further need for it (n= 23) or storage concerns (n= 10).

Nine participants mentioned variations of "I prefer to use websites on my laptop and apps on my phone." or perceived installing applications on their laptop as too much effort but had no problem with it on their phone.
We assume a combination of easier and safer installation on smartphones, usability problems of smartphone browsers and lower app prices as suspected in the original study [16] are responsible for the higher install frequency on smartphones.

4.2.2 Application Discovery. Chin et al. [16] hypothesized that installing an application recommended by someone trusted is probably not as risky as one from an advertisement or found by browsing. As can be seen in Figure 2, a recommendation from trusted people like family and friends is the most important way of discovering apps, with 42% of apps discovered this way. Recommendations by non-friends are relevant (20%). Browsing (24%) also plays a big role. Advertisements (19%) seems to be more relevant on smartphones (laptop $_{2020}$: 10%, smartphone $_{2020}$: 28%), which was not observed in the original study.
One interesting part of the app installations closer looked upon in the original study was applications discovered by only advertisement and browsing. In contrast to the original study with 44.8% of applications found this way on iOS and 15.7% on Android, we observed 22% on iOS and 33% on Android.

4.2.3 Installation Factors. There are several aspects that influence users in their decision on whether to install an app or not. Some of them might lead to a lower risk of installing malware, e.g., known brands, expert reviews, user rating, and the privacy policy [16]. We gathered data in a similar sorting activity to the original study about how important some individual factors are in the installation decision. This data can be found in Appendix C. The most considered factor was the price, followed by user reviews and familiarity with the brand. Interestingly, on Android, 80% always consider the ease of installing an app, which is more than double the percentage on other OSs. In the following, we present our results to the aspects that were closer looked upon in the original study.

Reviews. User reviews are a sort of soft safety net. While not as reliable as expert opinions and tests, they warn of the most

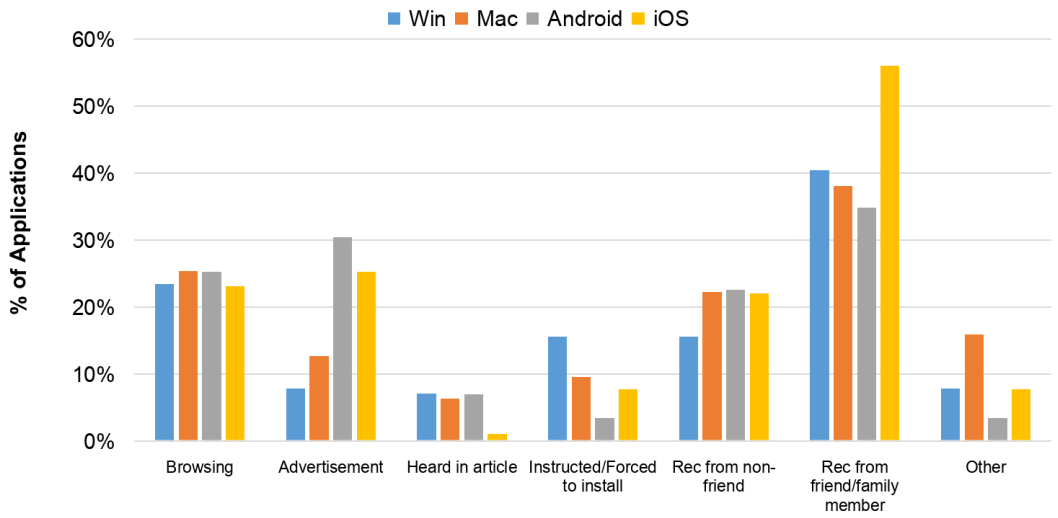


Figure 2: Where participants first heard about their installed applications (recorded 7 per person).

conspicuous hazards. Chin et al. expected greater importance of user reviews on smartphones because of the in-build review system in the most used mobile app markets but found no significant difference. We can confirm this observation (Wilcoxon signed rank test: $z = -0.69, p = 0.49$) with a nearly identical distribution of importance between laptops and smartphones. For the three choices always|sometimes|never, we had 63%|23%|13% in laptops and 60%|27%|13% in phones.

Permissions. In the original study, permission was only a given card if the participant had an Android smartphone since the other operating systems had no permission system. This is not the case anymore, so we added it to every OS. Permissions are a useful tool an attentive user can use to see if an app wants access to more data than it needs, making it easier to spot malicious applications. We expected permissions to have more weight on the smartphone install decision because they are more relevant there but found similar results on both devices (laptop $_{2020}$: 27%|47%|27%, smartphone $_{2020}$: 23%|53%|23%).

Brand. Chin et al. argued that a known brand having malicious software is less likely. Therefore, the brand itself is a good security indicator [16]. The original study observed statistically significantly more participants who were likely to try out unknown brands on smartphones than on laptops. The authors hypothesized this effect is caused by the more known and older brands on laptops and more unknown and new smartphone apps [16].

Unfortunately, we could not perform a power analysis for this section since we neither had the effect size nor the necessary data from the original study to calculate it.

We did not observe a statistically significant difference for the importance of the brand of an application for different devices. Neither in the factor sorting task (laptop $_{2020}$: 54%|23%|23%, smartphone $_{2020}$: 40%|40%|20%) nor in a specially geared question (Figure 3). There we asked about the willingness to try out apps from unknown brands and did not find a significant difference between the devices (Wilcoxon signed rank test: $z = -0.7338, p = 0.4654$). This can maybe be attributed to a more mature smartphone market with well-established brands.

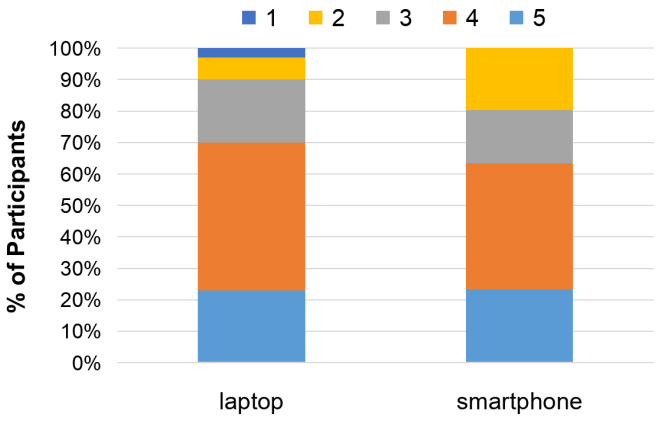


Figure 3: Participants willingness to try out apps of unknown brands from 1 least likely to 5 most likely

Price. Chin et al. [16] found statistically significant more participants who had paid applications on their laptops than on their smartphones. This corresponded with the authors' assumption that users are likely to have fewer paid apps on their phones. We performed a power analysis and needed 23 participants. Since we conducted the study with 30 participants, we should have seen an effect, if present. Indeed, we observed fewer paid apps on smartphones but not statistically significantly so (Wilcoxon signed rank test: $z = -1.7891, p = 0.0735$), as can be seen in Figure 4. Similar there were more participants always paying attention to price on smartphones (laptop $_{2020}$: 70%, smartphone $_{2020}$: 90%). While the original study found statistically significantly more paid apps on iOS than Android, we had findings in the other direction, with

around two times more on Android. However, this is not a significant difference (Mann-Whitney: $z = 0.3139, p = 0.7566$). We would have needed 310 participants for the expected effect size, so the absence of statistical significance should not be over interpreted.

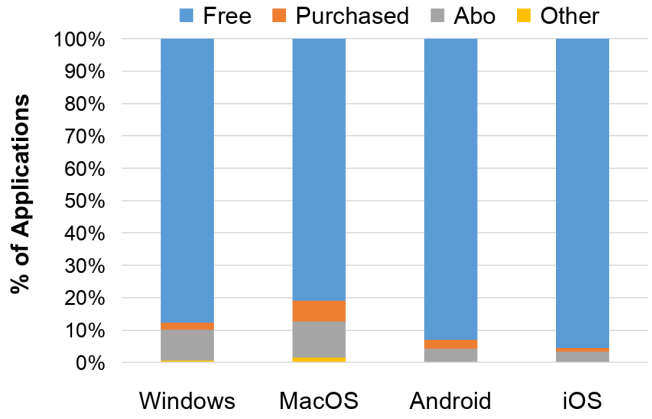


Figure 4: How many applications were free or paid (7 per participant)

End User Agreement and Privacy Policy. End user agreements and privacy policies show what corporations do with processed data, but users often ignore them, as observed in the original study. Almost half of the participants in our study said they rarely or never pay attention to them (laptop $_{2020}$: 48% smartphone $_{2020}$: 43%).

4.2.4 Application Download Sources. There are different sources to download applications. Official marketplaces like the Google Play Store, Apple App Store, or Microsoft Store should have lower risk associated than third-party ones. Alternative app markets maintained by large tech corporations, for example, have more malicious apps than the Google Play Store [32]. The original study observed that most mobile applications are from official stores (around 85%), with no such installs on laptops. On laptops, around 65% of the applications were sourced from websites, and official app markets did not exist [16].
We found similar results for official smartphone store installations (86%), and with the release of official markets on macOS and Windows we had 21% of laptop applications from there. This certainly is a change, and we believe this will result in a lower risk of malicious installs. These are the lower bounds of our measured values because we counted every unspecific mentioned App store as a third-party one. Some participants choose "website" as a source, but downloaded the app from the linked app market. We noticed this oversight too late. Therefore, some downloads from official sources might be not counted as such.

4.2.5 Number of Applications. Simply put, more installed applications increase the chances of having malware installed. Therefore a lower application count should be better for device security if the install source is the same. We already observed a higher frequency in app installations and removing on smartphones than on laptops, so we expected more installed apps on phones. This was also the case for Chin et al., as they found more applications on smartphones $_{2012}$ (mean: 36, median: 24.5) than laptops $_{2012}$ (mean: 21, median: 12) [16]. We have an even bigger difference with significant (Wilcoxon signed-rank test: $z = -4.06, p < 0.00001$) more apps on smartphones $_{2020}$ (mean: 51.2, median: 51) than laptops $_{2020}$ (mean: 22, median: 19).
We omitted analyzing the types (e.g., shopping, news, games) of applications participants had installed. The small share of apps we inquired about per person (seven apps) and the fact that the different sorting methods per OS distort the statistics do not provide useful results. For example, Amazon as a shopping app has a much higher chance to get recorded on Android due to the alphabetical sorting method.

5 DISCUSSION

In this section, we discuss the changes, improvements and still existing problems that smartphones have and look into possible biases and limitations of this study.

5.1 Changes Between 2012 and Today

We measured the willingness to perform a specific task on the smartphone vs. a laptop. We find no statistically significant differences between these device types. Especially everyday actions like shopping and apps charging money are carried out without being obstructed by security reasons. Just two participants had usability reasons not to shop on their phones. Comparing this to the findings by Chin et al. [16] this indicates a change.
Comparing security concerns on devices between the years, we see a shift towards more worries on laptops. We also did not find nearly as many participants worrying about phone and data loss, which may be attributed to better backup and encryption services and fewer problems with these.

We could not find serious misconceptions (e.g., network security) as the authors of the previous study. This could be a possible consequence of user education or more time to get used to smartphones. Participants did not mention technical worries (e.g., battery or signal strength) as they did in 2012. Only one mentioned the battery but was half-joking. One more thing that stood out positively was participants praising the ease of use of apps, for example, health insurance management apps, and how satisfied they are with them.

However, we observed irrational habits concerning smartphones, which the participants could not explain. We thus encourage further researchers to investigate the influences and reasons.

5.2 Open Problems

While many results indicate improvements in the situation, there are still open problems. We observed participants not trusting the reliability of backups or remembering having problems with them. This indicates a field for further research and engineering.

One recommendation by Chin et al. [16], which did not get implemented over time, was per-app security indicators in popular app markets. With us observing advertisement to be more pronounced as a source of app installations on smartphones and the general frequency users install apps, smartphone security seems to strongly depend on the safety of apps from official app markets.

We found no improvement in users' privacy perception on smartphones. But with research like Balapour et al. [11] indicating privacy perception negatively influencing security perception, it is even more important to design solutions. We also saw indications that a visible permission system could negatively impact privacy perception.

When asked about considered elements before installing an app, end user agreements and privacy policies are still not considered often compared to other properties. Further research should find ways of making these more attractive to users or identify alternatives that can inform the user properly before an installation.

5.3 Feeling vs. Knowledge

One of the more interesting discoveries was that some participants did not want to do sensitive tasks on smartphones but later told us they worry less about it. When this was pointed out, we heard explanations that could indicate a sort of learned behavior (e.g., from parents) that they do not think about much, but when concretely asked, they think a smartphone is safer. Yet another possible explanation was that privacy perceptions often had more to do with the amount of important data and frequency of use than the device itself. Therefore, if someone uses their laptop for important tasks, because they trust it more, their worries about security might increase. This difference between unconscious and conscious perception should be kept in mind when designing studies.

5.4 OS Influence

While not specifically asked, four out of the 30 participants mentioned differences in device perception depending on the OS, three of whom had an Apple device; indicating that the OS can possibly influence security perception, also suggested by other research [16, 26, 31]. Any study investigating privacy or security perception regarding smartphones needs to account for this.

5.5 Limitations and Bias

Several aspects impact our results. As mentioned in section 3, we had to carry out our study in Germany, which certainly has cultural and linguistic implications. We recruited from eBay Kleinanzeigen with many of our participants being students or low wage earners. Choosing to pay our participants 30 Euro should influence our demographic range a bit since the 60$ (with inflation worth 68$ in 2020 [3]) paid in the first study is around double our remuneration. However, the lower average salary and living costs of this study's location probably counter this aspect at least partially. Some security and privacy conscious people could have been deterred by the need to give their bank details to receive the payment (some, in fact, lost their interest, after knowing we do not support PayPal). We had 30 participants, exactly half of the original study. As mentioned throughout the paper, we performed a power analysis, calculating the required number of participants needed to find the same effect as reported in the original study. For Section 4.1.2, we would, for example, have needed 89 participants. Due to how time intensive the interview format is, we were not able to achieve this high number. Therefore, statistical significance, or its lack, has to be interpreted with caution.

Only half of the participants have an Apple device, while this was true for 75% in the original study. However, we believe this to be a more accurate representation of the German population [29]. Additionally, there is a slight bias towards male and younger participants. With the before mentioned aspects and online nature of the study, the results have to be understood as insights into the current state with the need for further research.

The chosen methodology of the original study that we followed for asking participants about their installed apps on their devices introduced a bias through the different sorting orders and the low cross-section of tested apps. Although it is suitable for a rough overview, a, e.g., automated analysis of all installed applications probably would have delivered more accurate results.

6 CONCLUSION

When a study found more privacy and security concerns on smartphones in 2012 [16] the smartphone market was just emerging. They found trust problems and concerns. Now, nine years later, many of the original problems improved. We conducted a similar study, using online interviews (n=30) to understand how much has changed since 2012. Our observations suggest that the smartphone ecosystem matured and has none of the large general problems found in the original study. We found that many of the original recommendations are now at least partially the reality. While there are still more participants worried about the privacy of smartphones than on laptops, and concerns exist, some of which the participants themselves call "irrational", there are many that trust their smartphone more than their laptop. Overall we see no significant perception problems hampering smartphone usage today anymore, but still, see room to improve privacy concerns and backups.

REFERENCES

[1] [n.d.]. Categories and Discoverability - App Store - Apple Developer. URL https://developer.apple.com/app-store/categories/. Accessed: August 05, 2021.

[2] [n.d.]. Ebay Kleinanzeigen. URL www.ebay-kleinanzeigen.de. Accessed: July 29, 2021.

[3] [n.d.]. U.S. Bureau of Labor Statistics. URL https://data.bls.gov/cgi-bin/cpicalc.pl. Accessed: February 22, 2021.

[4] 2011. Apple Introduces iCloud. URL https://www.apple.com/newsroom/2011/06/06Apple-Introduces-iCloud/. Accessed: July 29, 2021.

[5] 2012. Google Drive officially launches with 5GB free storage, Google Docs integration. URL https://www.theverge.com/2012/4/24/2971025/google-drive-official-launch-features. Accessed: July 29, 2021.

[6] 2013. iPhone 5s Review: A New Touch for iPhone. URL https://www.wsj.com/articles/SB10001424127887323527004579081192462456798. Accessed: July 26, 2021.

[7] 2017. iPhone X announced with edge-to-edge screen, Face ID, and no home button. URL https://www.theverge.com/2017/9/12/16288806/apple-iphone-x-price-release-date-features-announced. Accessed: July 26, 2021.

[8] Naveed Ahmad, Aimal Rextin, and Um E Kulsoom. 2018. Perspectives on usability guidelines for smartphone applications: An empirical investigation and systematic literature review. *Information and Software Technology* 94 (2018), 130–149. https://doi.org/10.1016/j.infsof.2017.10.005

[9] Milad Taleby Ahvanooey, Qianmu Li, Mahdi Rabbani, and A. Rajput. 2020. A Survey on Smartphones Security: Software Vulnerabilities, Malware, and Attacks. *ArXiv* abs/2001.09406 (2020).

[10] Carlos A. Arango-Arango, Yassine Bouhdaoui, David Bounie, Martina Eschelbach, and Lola Hernandez. 2018. Cash remains top-of-wallet! International evidence from payment diaries. *Economic Modelling* 69 (2018), 38 – 48. https://doi.org/10.1016/j.econmod.2017.09.002

[11] Ali Balapour, Hamid Reza Nikkhah, and Rajiv Sabherwal. 2020. Mobile application security: Role of perceived privacy as the predictor of security perceptions. *International Journal of Information Management* 52 (2020), 102063. https://doi.org/10.1016/j.ijinfomgt.2019.102063

[12] Susanne Barth, Menno D.T. de Jong, Marianne Junger, Pieter H. Hartel, and Janina C. Roppelt. 2019. Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and Informatics* 41 (2019), 55–69. https://doi.org/10.1016/j.tele.2019.03.003
[13] 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).
[14] Stephanie Carretero, Riina Vuorikari, and Yves Punie. 2017. The digital competence framework for citizens. *Publications Office of the European Union* (2017).
[15] Amita Goyal Chin, Mark A. Harris, and Robert Brookshire. 2018. A bidirectional perspective of trust and risk in determining factors that influence mobile app installation. *International Journal of Information Management* 39 (2018), 49 – 59. https://doi.org/10.1016/j.ijinfomgt.2017.11.010
[16] Erika Chin, Adrienne Porter Felt, Vyas Sekar, and David Wagner. 2012. Measuring User Confidence in Smartphone Security and Privacy. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (Washington, D.C.) *(SOUPS 12)*. Association for Computing Machinery, New York, NY, USA, Article 1, 16 pages. https://doi.org/10.1145/2335356.2335358
[17] Evert de Haan, P.K. Kannan, Peter C. Verhoef, and Thorsten Wiesel. 2018. Device Switching in Online Purchasing: Examining the Strategic Contingencies. *Journal of Marketing* 82, 5 (2018), 1–19. https://doi.org/10.1509/jm.17.0113 arXiv:https://doi.org/10.1509/jm.17.0113
[18] eMarketer. 2019. US Time Spent with Mobile 2019. URL https://www.emarketer.com/content/us-time-spent-with-mobile-2019. Accessed: July 29, 2021.
[19] Marco Furini, Silvia Mirri, Manuela Montangero, and Catia Prandi. 2020. Privacy perception when using smartphone applications. *Mobile Networks and Applications* (2020), 1–7.
[20] Jie Gu, Yunjie (Calvin) Xu, Heng Xu, Cheng Zhang, and Hong Ling. 2017. Privacy concerns for mobile app download: An elaboration likelihood model perspective. *Decision Support Systems* 94 (2017), 19 – 28. https://doi.org/10.1016/j.dss.2016.10.002
[21] Handelsblatt. 2020. Why Germany is so slow on the global road toward a cashless society. URL https://www.handelsblatt.com/english/finance/payments-why-germany-is-so-slow-on-the-global-road-toward-a-cashless-society/23712232.html. Accessed: July 29, 2021.
[22] Huan Liu, Lara Lobschat, Peter C. Verhoef, and Hong Zhao. 2019. App Adoption: The Effect on Purchasing of Customers Who Have Used a Mobile Website Previously. *Journal of Interactive Marketing* 47 (2019), 16 – 34. https://doi.org/10.1016/j.intmar.2018.12.001
[23] Tanya McGill and Nik Thompson. 2017. Old risks, new challenges: exploring differences in security between home computer and mobile device use. *Behaviour & Information Technology* 36, 11 (2017), 1111–1124. https://doi.org/10.1080/0144929X.2017.1352028 arXiv:https://doi.org/10.1080/0144929X.2017.1352028
[24] Pew Research Center. 2019. Mobile Fact Sheet. URL https://www.pewresearch.org/internet/fact-sheet/mobile/. Accessed: July 29, 2021.
[25] Lumpapun Punchoojit and Nuttanont Hongwarittorrn. 2017. Usability studies on mobile user interface design patterns: a systematic literature review. *Advances in Human-Computer Interaction* 2017 (2017).
[26] Lena Reinfelder, Zinaida Benenson, and Freya Gassmann. 2014. Differences between Android and iPhone Users in Their Security and Privacy Awareness. In *Trust, Privacy, and Security in Digital Business*, Claudia Eckert, Sokratis K. Katsikas, and Günther Pernul (Eds.). Springer International Publishing, Cham, 156–167.
[27] Lena Reinfelder, Andrea Schankin, Sophie Russ, and Zinaida Benenson. 2018. An Inquiry into Perception and Usage of Smartphone Permission Models. In *Trust, Privacy and Security in Digital Business*, Steven Furnell, Haralambos Mouratidis, and Günther Pernul (Eds.). Springer International Publishing, Cham, 9–22.
[28] H. M. Salman, W. F. Wan Ahmad, and S. Sulaiman. 2018. Usability Evaluation of the Smartphone User Interface in Supporting Elderly Users From Experts' Perspective. *IEEE Access* 6 (2018), 22578–22591. https://doi.org/10.1109/ACCESS.2018.2827358
[29] Statcounter. 2020. Operating System Market Share Germany. URL https://gs.statcounter.com/os-market-share/all/germany. Accessed: July 29, 2021.
[30] Tsai-Hsuan Tsai, Kevin C Tseng, and Yung-Sheng Chang. 2017. Testing the usability of smartphone surface gestures on different sizes of smartphones by different age groups of users. *Computers in Human Behavior* 75 (2017), 103–116.
[31] Perin Ünal, Tuğba Taşkaya Temizel, and P. Erhan Eren. 2015. A Study on User Perception of Mobile Commerce for Android and iOS Device Users. In *Mobile Web and Intelligent Information Systems*, Muhammad Younas, Irfan Awan, and Massimo Mecella (Eds.). Springer International Publishing, Cham, 63–73.
[32] Haoyu Wang, Zhe Liu, Jingyue Liang, Narseo Vallina-Rodriguez, Yao Guo, Li Li, Juan Tapiador, Jingcun Cao, and Guoai Xu. 2018. Beyond Google Play: A Large-Scale Comparative Study of Chinese Android App Markets. In *Proceedings of the Internet Measurement Conference 2018* (Boston, MA, USA) *(IMC '18)*. Association for Computing Machinery, New York, NY, USA, 293–307. https://doi.org/10.1145/3278532.3278558

A CALL FOR PARTICIPANTS

Online study about smartphones | Online Interview 50-90min | 30€ compensation

We are searching for online interview participants. The duration is 50-90min and the information obtained will be processed anonymously. There will be a recording, which will be deleted after transcription (probably on the same day). The interview is not a test, we just want your opinions and experiences. Questions can be skipped at any time.

Prerequisites: own a personal smartphone, own a personal laptop and be at least 18 years old

What you will do: A zoom conversation with us, cameras or video is not necessary. You will answer questions and fill out a survey online.

Compensation: 30€

If you want to participate or if you have questions, please contact me. To participate we would need a list with age, gender and your devices (laptops/smartphones), please mark which operating systems they are using and which of the devices you primarily use.

Example:

Age: 20

Gender: male

Devices: Laptop(Windows 10), Laptop(Windows 7), Smartphone(Android)

Main laptop: Windows 10

Main smartphone: Android

B INTERVIEW / SURVEY

B.1 Demographic Questions

- What is your age?
- What is your gender?
- What is the highest degree or level of school you have completed?
- What is your household income?
- How often do you ask for help facing technical problems? [Never(1)-Every time(5)]
- How often are you asked for help when somebody is facing technical problems? [Never(1)-Every time(5)]

B.2 Computer usage questions

- Which operating system is installed on your laptop? (If you have installed more than one operating system, please choose the one you are mainly using)
- Which [Windows | macOS] version do you use?
- How long have you owned this computer?
- How many years have you owned a computer in general?
- Is this your only computer? If not, how many computers do you use? If you have multiple computers, do you use them for different purposes? Please explain. Which laptop did you bring?
- How many people regularly (weekly) use this laptop? (e.g., Do any family members/co-workers use it)?
- Does anyone occasionally use this laptop? (excluding people using it regularly) What circumstances?
- I am likely to try computer applications made by companies or brands that I am not familiar with. [Likert 1-5]

- What types of applications do you tend to install on your computer? [Books, Business, Developer Tools, Education, Entertainment, Finance, Food & Drink, Games, Graphics & Design, Health & Fitness, Lifestyle, Magazines & Newspapers, Medical, Music, Navigation, News, Photo & Video, Productivity, Reference, Shopping, Social Networking, Sports, Travel, Utilities, Weather, Other]
- Where do you usually look for applications? [App Stores, Web search (e.g., Google, Ecosia, DuckDuckGo), Retail Stores, Ask Friends & Family, Other]
- Do you have anti-virus software installed on your laptop? If so, what brand? Did it come pre-installed? Is it a free or paid version?
- If there is an "update" available for your Windows/Mac (not individual applications), do you: [Apply it immediately, Do it weekly/monthly, Ignore until prompted again or critical, Always enable auto update, Ignore until later if it requires you to restart your computer, Other]

B.3 Mobile usage questions

- Which operating system is installed on your smartphone?
- How long have you owned this Android or iPhone?
- How many years have you owned a Android or iPhone in general?
- Is this your only mobile phone? If not, how many mobile phones do you use? If you have multiple mobile phones, do you use them for different purposes? Please explain. Which phone did you bring?
- How many people regularly (weekly) use this phone? (e.g., Do any family members/co-workers use it)?
- Does anyone occasionally use this phone? (excluding people using it regularly) What circumstances?
- I am likely to try mobile applications made by companies or brands that I am not familiar with. [Likert 1-5]
- What types of applications do you tend to install on your computer? [Books, Business, Developer Tools, Education, Entertainment, Finance, Food & Drink, Games, Graphics & Design, Health & Fitness, Lifestyle, Magazines & Newspapers, Medical, Music, Navigation, News, Photo & Video, Productivity, Reference, Shopping, Social Networking, Sports, Travel, Utilities, Weather, Other]
- Where do you usually look for applications? [App Stores, Web search (e.g., Google, Ecosia, DuckDuckGo), Retail Stores, Ask Friends & Family, Other]
- Do you have anti-virus software installed on your phone? If so, what brand? Did it come pre-installed? Is it a free or paid version?
- If there is an "update" available for your Android/iPhone(not individual applications), do you: [Apply it immediately, Do it weekly/monthly, Ignore until prompted again or critical, Always enable auto update, Ignore until later if it requires you to restart your phone, Other]

B.4 Installed application questions

Participants were first asked to count the number of applications they themself installed and then take the first 7 (sorting depending on OS) and answer the following questions for each:

- Name of the application
- The application was: [Free, Purchased, free to download but needs a paid user account, Other]
- Where did you get the application from? [Physical Store, Online store (e.g., Amazon, AppStore), Company website, Other]
- If you answered digital/online store, which one?
- What prompted you to install this application?
- How did you first hear about this application? [Choose all that apply: Friend or family member, Recommendation from someone other than a friend, Advertisement, Instructed/Forced to install it (e.g., by other software), Browsing, Heard about it in an article, Other]
- What factors did you consider before installing it? [Choose all that apply: Price, Popularity of the application, Search ranking/sponsored listing, User reviews, Expert reviews online (blogs, magazines, etc.), Salesperson suggestions in a store (like Saturn, Mediamarkt etc.), Friends' recommendations, Familiarity with the brand, Ease of installation, Screenshots, End User License Agreements and Terms of Services, The application's privacy policy, Permissions, Other]
- How often do you use it? [Daily, Weekly, Monthly, A few times a year, Other]

B.5 Factors considered

Participants were asked to drag and drop the following elements into one of the three buckets: Always consider, sometimes consider, and never or rarely consider. Then put the "Always consider" and "sometimes consider" piles into rank order, from most to least considered.

- Price (Free vs. $$$)
- Popularity of app
- Search ranking/sponsored listing
- User reviews + ratings
- Expert reviews online (blogs, magazines, etc.)
- Salesperson suggestions in a store (ex. Saturn, Mediamarkt, etc.)
- Friends' recommendations
- Familiarity with brand
- Ease of installation (e.g., drag-and-drop install, having to register before use, etc.)
- Screenshots / look + feel
- End User License Agreements and Terms of Services
- Application's privacy policy
- Permissions
- Other

B.6 Interview Questions

At the end of the laptop and smartphone survey parts, we verbally asked:

- Do you regularly uninstall applications on your [laptop | smartphone]? If so, why? Have you recently uninstalled applications for any reason? If so, why?

For each of the devices (laptop/smartphone) we asked the questions:

- Have you used a website that is location-aware on your laptop? (e.g., Maps, Twitter (optional), Facebook (optional))?
- Have you used an application on your laptop that is location-aware? (e.g., TweetDeck, weather apps)
- If they answered no, they were asked: Would you install an application or use a website that that can learn your location? Why/Why not? If you answered "sometimes," under what conditions?

They were asked for all of the following topics:

- Have you used an application on your laptop that is location-aware? (e.g., TweetDeck, weather apps)
- Have you used an application on your laptop that can charge you money? (For example, Skype will charge your credit card if you use up your minutes. Some games. Renewal of the anti-virus.)
- Have you logged into your bank account on your laptop?
- Have you used a finance management website on your laptop? (Ex. Mint, Buxfer, BillShare, Venmo)
- Have you made a purchase on a shopping site (e.g., amazon.com) on your laptop? (via website)
- Have you accessed work-related email on your laptop via browser?
- Have you given your Social Security Number to a website on your laptop? (Ex. job apps, credit card apps, online tax software)
- Have you used a website to manage your health documents on your laptop? (Ex. GoogleHealth)
- Have you used a website to share photos on your laptop?

At last, we asked:

- Do you worry about security (e.g., malicious programs) on the phone [a lot more than | more than | about the same | less than | a lot less than] security on the laptop? Please explain.
- Do you worry about privacy (e.g., leaking sensitive data) on the phone [a lot more than | more than | about the same | less than | a lot less than] privacy on the laptop? Please explain.
- In general, what are your primary concerns about your phone?
- Do you own a tablet? How does your usage of your tablet differ from the usage of your phone? (e.g., apps you tend to install, update behavior, etc.)

C EXTRA

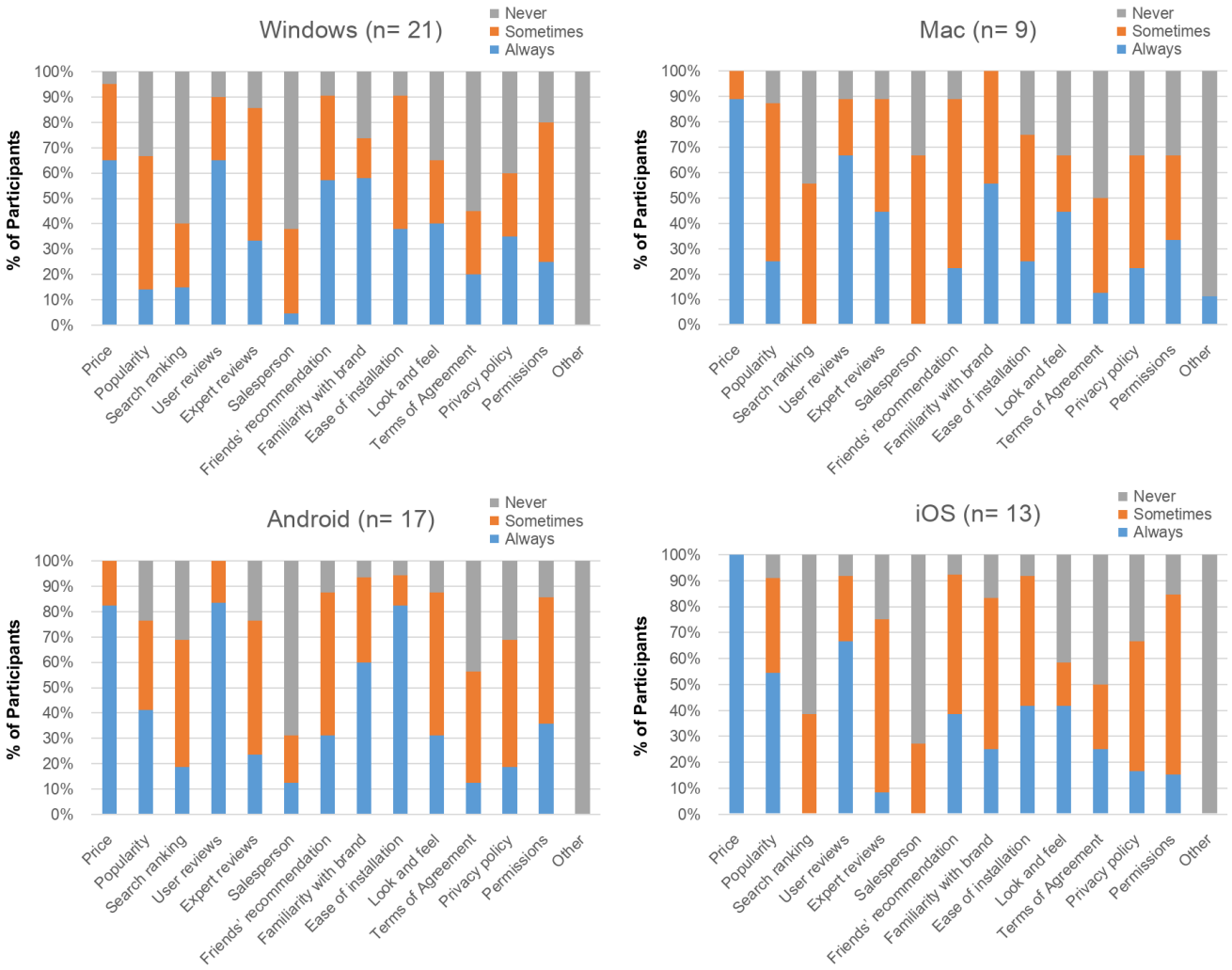


Figure 5: Relative Importance of factors considered before installing an application.

Table 3: Overview of the changes between the original and this study. The questions were adjusted with more up-to-date examples and usability enhancements. Some extra questions were added.

	Original (2012) [16]	New Study (2020)
Interview type	Personal	Online (Zoom)
Survey type	paper	online
Residency of participants	USA	Germany
Language	English	German
Recruitment	Craigslist	Ebay Kleinanzeigen (a german classified ads website)
Number of Participants	60	30
Gender M / F / Other	50% / 50% / 0%	57% / 43% / 0%
Windows / Android	25%	50%
Windows / iOS	25%	20%
macOS / Android	25%	7%
macOS / iOS	25%	23%
Card Sorting	some cards had pictures	only text
Installed Applications	maximum in 10 min (avg. 7 apps)	a fixed number of 7 apps
Task Willingness...	to install an application	to install an application or use a website