Measuring User Confidence in Smartphone Security and Privacy

Erika Chin

Electrical Engineering and Computer Sciences
University of California at Berkeley

Technical Report No. UCB/EECS-2012-231
http://www.eecs.berkeley.edu/Pubs/TechRpts/2012/EECS-2012-231.html

December 10, 2012

Measuring User Confidence in Smartphone Security and Privacy

by Erika Chin

Research Project

Submitted to the Department of Electrical Engineering and Computer Sciences, University of California at Berkeley, in partial satisfaction of the requirements for the degree of **Master of Science, Plan II**.

Approval for the Report and Comprehensive Examination:

Committee:

Professor David Wagner
Research Advisor

(Date)

* * * * * * *

Professor Dawn Song
Second Reader

(Date)

Measuring User Confidence in Smartphone Security and Privacy

Erika Chin
University of California, Berkeley
emc@cs.berkeley.edu

Abstract

In order to direct and build an effective, secure mobile ecosystem, we must first understand user attitudes toward security and privacy for smartphones and how they may differ from attitudes toward more traditional computing systems. What are users' comfort levels in performing different tasks? How do users select applications? What are their overall perceptions of the platform? This understanding will help inform the design of more secure smartphones that will enable users to safely and confidently benefit from the potential and convenience offered by mobile platforms.

To gain insight into user perceptions of smartphone security and installation habits, we conduct a user study involving 60 smartphone users. First, we interview users about their willingness to perform certain tasks on their smartphones to test the hypothesis that people currently avoid using their phones due to privacy and security concerns. Second, we analyze why and how they select applications, which provides information about how users decide to trust applications. Based on our findings, we present recommendations and opportunities for services that will help users safely and confidently use mobile applications and platforms.

1 Introduction

Smartphones have dramatically changed the computing landscape. They complement and, in some cases, supplant traditional computing devices such as laptops and desktops [8]. We have seen a tremendous growth in the number and diversity of smartphone applications in marketplaces such as the Apple App Store, Android Market, and Amazon AppStore.

Despite the popularity of smartphones, there are reasons to believe that privacy and security concerns might be inhibiting users from realizing the full potential of their mobile devices. Although half of U.S. adults own smartphones [5], mobile online shopping is only 3% of overall shopping revenues [7], suggesting that users are hesitant to perform these tasks on their smartphones. A recent commercial study also found that 60% of smartphone users are concerned that using mobile payments could put their financial and personal security at risk [4].

Our goal is to help smartphone users confidently and securely harness the power of mobile platforms. In order to improve the security of mobile systems, we must understand the challenges and concerns that users currently have with performing sensitive operations on their smartphones and identify opportunities to improve the security of the device. We interviewed 60 smartphone users about their willingness to perform certain actions on their phones. We found that participants are significantly less willing to make shopping purchases, provide their Social Security numbers, access health data, or check their bank accounts on their smartphones than on their laptops. Our data also sheds some light on why users might be more reluctant to perform these tasks on their phones (see Section 4). We expect these results may be helpful in identifying opportunities to improve the security of these devices.

Applications play a critical role in users' experiences with their smartphones. To help protect users while selecting applications, it is important to understand each step in the mobile application installation process: how users discover applications, the factors they consider before installation (e.g., price, brand name), and where they download applications from. We survey the 60 study participants about how and why they install mobile applications.

This paper presents the results of structured interviews and surveys of 60 participants. The participants span four popular platforms: Windows and Mac for laptops, and Android and iPhone for smartphones. We compare and contrast

laptop and smartphone behaviors and perceptions, using laptops as a reference point for understanding smartphone-specific concerns. The structured interviews were a tool to (1) test our hypothesis that people are less willing to perform sensitive operations on their smartphones, and (2) collect qualitative data about users' mobile security concerns. We also survey participants about the applications that they installed on their smartphones to guide the design of new security indicators.

Contributions: This paper makes the following contributions:

- We find that users are (1) more concerned about privacy on their smartphones than their laptops and (2) more apprehensive about performing privacy-sensitive and financial tasks on their smartphones than their laptops.
- We report the threats that participants worry about on their smartphones: physical theft and data loss, malicious applications, and wireless network attackers. We also find that participants' fears of wireless network attackers stem from misconceptions about how wireless network communication works.
- We make several recommendations that could increase security and/or user confidence in their smartphones: (1) improved data backup, lock, and remote wipe services; (2) new security indicators in smartphone application markets to increase user trust in their selection of applications; and (3) user education and improved user interfaces to address common misconceptions about wireless network communication.

2 Background and Related Work

2.1 Application and Security Models

Windows: The Windows platform has encouraged a relatively ad hoc application ecosystem, with third-party application software being commonly acquired from diverse sources (e.g., online, physical retailers) without any centralized application market place. Given this decentralized nature, there is little by way of *curation* of the applications, and users have to install anti-virus software (again from third-party sources) to protect themselves against malware, which is a well-documented problem for Windows.

Mac: In contrast, the Mac platform is generally perceived to be more immune to malware, as there have been relatively fewer documented cases of malware attacks. Macs also have anti-virus options, but they are less widely adopted [17]. Similar to Windows, the traditional application ecosystem has also been largely decentralized. Motivated by the success of the mobile App Store, Apple launched the Mac App Store as a centralized market for desktop applications. It appears to be reasonably successful [1].

Android: There are several "marketplaces" for Android users to download applications, with the Android Market being the most popular. The Android Market is not curated, although recent reports suggest that it is scanned for malware by Google [2]. (Google also removes software that is found to violate their TOS.) There are several demonstrated malware attacks on the Android platform. Anti-virus applications are available for Android, although their effectiveness has been publicly questioned [33, 29].

iOS: The App Store is a centralized, curated marketplace for downloading iPhone applications. While the exact details of the curation process is unknown,[1] there is evidence to suggest that Apple does check for security violations. Although there have been few samples of iPhone malware, there is plenty of grayware and jailbreaking applications [23]. Users are prompted when applications want to access location or other information via pop-up notifications.

2.2 Related Work

Application Selection: Past research suggests that privacy and security play roles in users' installation decisions. Wash interviewed people about computer security threats, and several interviewees indicated that they were cautious when installing new software because of malware concerns [39]. In an experiment performed by Good et al., people preferred applications with better privacy policies unless the privacy came at the cost of application functionality [25]. We further explore users' concerns about application trustworthiness (and how they prioritize those concerns) by asking people to recall the factors that led them to install applications. We also ask people about how they discover

[1] Most visible media reports of applications being denied have to do with the content served rather than specific security reasons.

applications, which may provide insight into how trust in software is established. Matthews et al. found that word-of-mouth and browsing the App Store are important discovery methods for iOS applications [30]; we further expand the scope of this study to Android as well.

Researchers have investigated whether placing privacy indicators in search results influences users' online shopping decisions. They found that privacy indicators can cause users to pay a premium to purchase items from online vendors with better privacy scores [24, 38]. However, the timing and placement of the indicators affects whether users heed them [21]. We hypothesize that privacy and security indicators could play a similar role in application selection, so we investigate users' installation workflows to identify potential places for security and privacy indicators.

Smartphones vs. Computers: We explore whether users have different security and privacy concerns for their smartphones and computers. Past studies have found that people often begin tasks on smartphones but complete them on computers [12, 28, 30]. Many platform switches can be attributed to screen size, network performance, or typing difficulties. However, we suspect that privacy and security concerns may also play a role. Matthews et al. observed that some users shop for items on their phones but defer payment until they are at a computer [30]. We investigate whether security concerns about smartphones may be responsible for users' preferences for computers in certain situations.

Smartphone Privacy and Security: Smartphones are ideally suited for location-aware services. Consequently, prior research has focused on users' attitudes towards location privacy. A large body of work addresses how users share location information with social contacts [14, 26, 18, 11, 40, 13] and companies [20, 19]. However, smartphones can also be used to handle other types of confidential data, and there are threats beyond social contacts and advertising companies (e.g., muggers and man-in-the-middle network attackers). Ben-Asher et al. surveyed smartphone users and found that people consider other information on their phones sensitive (e.g., photos and contacts) and worry about physical attacks on their phones [15]. As such, the scope of our inquiry goes beyond location and social contacts. We ask people about their willingness to access several types of information on their phones, and our survey design allowed study participants to describe their own threats.

Smartphone Application Usage: Prior work has studied how smartphones are used. Falaki et al. examined Android and Windows Phone application usage from the perspective of reducing energy consumption [22]. They found that smartphone users primarily spend their time interacting with a small subset of their installed applications; relative application popularity can be modeled as an exponential distribution. Others have similarly studied the time that people spend using certain applications [28, 30]. Our inquiry focuses on application discovery and installation rather than usage, as our end goal is to help users avoid installing malicious or otherwise-undesirable applications.

3 Methodology

We performed structured interviews and surveys of 60 users to obtain both a quantitative and qualitative understanding of how people use their smartphones. As a point of comparison, we also asked them about similar behaviors on their laptops. Our questions focused on application discovery, application selection, and users' willingness to perform different application activities on each platform. Each participant owned a laptop (Windows or Mac) and a smartphone (Android or iPhone). Our choice of platforms was motivated by their dominant market share in the respective categories.

Prior to beginning the study, we obtained IRB approval as an exempt protocol. We coded all personally identifiable information so that only the lead researcher could connect data to participants and deleted audio recordings following the transcription process.

3.1 Recruitment

We recruited participants in December 2011 and January 2012. We placed an advertisement in the "Et cetera jobs" section of the San Francisco Bay Area Craigslist and offered $60 for participation in our study. The advertisement stated that the study was about smartphones but did not mention privacy or security. To be eligible, users had to be age 18 or older, own a personal smartphone, own a personal laptop, and be willing to bring both devices to the interview. Respondents were asked to specify their age, operating system of their laptop, the operating system of their mobile phone, and their availability over the following weeks. If they had multiple laptops or phones, they were asked to list all of the devices and specify whether they were used equally or whether one was a primary device. We did not state

the operating systems that we were recruiting for in order to avoid respondents from giving us false data about their device (e.g., borrowing a friend's device for the study or using an old or secondary device).

To be eligible for our study, respondents needed to own Android phones or iPhones in addition to Mac OS 10.*, Windows XP, Windows Vista, or Windows 7 laptops. We eliminated respondents who listed anything other than the four operating systems we were looking for (e.g., Blackberry or Linux) or did not list both a laptop and a smartphone. After this filtering, we obtained 282 eligible responses (33 Android/Mac, 82 iPhone/Mac, 104 Android/Windows, 63 iPhone/Windows). In order to demographically balance our sample across ages and genders, we sorted the list of eligible participants by age and gender and randomly selected 15 Windows/iPhone users, 15 Windows/Android users, 15 Mac/iPhone users, and 15 Mac/iPhone users from the groups. We offered interview slots on both weekdays and weekends to accommodate work constraints (37 on weekdays, 23 on weekends).

Demographics: In total, we interviewed 30 men and 30 women. By design, 19 participants were between ages 18-27, 14 between ages 28-37, 14 between 38-47, and 13 were age 48 and older. As mentioned earlier, we balanced age and gender distributions within each laptop and mobile device category. One caveat, however, is that we were unable to obtain a balanced demographic for the Mac/Android category due to a limited pool of respondents. As a result, 5 of the 7 men in the Mac/Android category were in the youngest age group. Although this could bias the data towards younger users' preferences, we believe it is a realistic representation of the Mac/Android population.

As such, we believe that the opinions expressed by participants are representative of opinions across age groups, genders, and races. We do, however, point out one potential source of bias—our participants could be more price conscious than the overall population of smartphone users because we recruited participants from Craigslist.

3.2 Procedure Overview

We conducted study sessions in campus classrooms, with one participant and one interviewer per session. Each session consisted of computerized surveys, two card-sorting activities, and a structured interview. The surveys were completed on laptops provided by the interviewers. The interviewer was able to view each survey shortly after completion and ask for clarification if participants' responses were unclear. (To avoid priming participants, we did not explicitly mention privacy or security until the last question of the interview.) For completeness, we provide a detailed description in Appendices A–G. Each session took around 50-90 minutes:

1. The interviewer defined the term "application" and explained the difference between websites and applications.
2. The participant filled out a survey about laptop usage, where we asked questions to determine how participants use their devices. These questions included the amount of time that the participant has owned the device, whether the device is the participant's primary computer or phone, whether the device is shared, and how many applications are installed on the device.[2]
3. The participant completed a sorting activity to rank the factors that s/he considers when selecting laptop applications. We gave participants notecards that featured descriptions and (platform-appropriate) screenshots of factors. Participants sorted factors into three categories ("always consider," "sometimes consider," and "never or rarely consider") and then ordered the factors within the groups by relative importance. The factors were: price, popularity of app, search ranking/sponsored listing, user reviews and ratings, expert reviews online (blogs, magazines, etc.), salesperson suggestions in a store (like BestBuy), friends' recommendations, familiarity with brand, ease of installation, screenshots, End User License Agreements and Terms of Services, the application's privacy policy, and "Other" for additional factors (Appendix G). All participants received the same set of notecards for the laptop sorting activity. (To avoid ordering biases, we shuffled the notecards before each activity.)
4. The participant filled out a survey about the applications installed on his or her laptop. We asked each participant to go down their list of applications, sorted by the installation date. Participants were given 10 minutes to describe their installed applications, and we instructed them to skip pre-installed applications. For each application, the participant recorded the type of application, how s/he heard about it, what prompted him or her to install it, what factors s/he considered before installing it, etc. On average, participants were able to describe seven applications in the allotted time.
5. The participant filled out a survey on smartphone usage similar to the laptop usage survey.

[2]We guided participants to the list of installed applications.

6. The participant completed an analogous sorting activity to rank factors s/he considers when installing smartphone applications. (Since Permissions are only relevant to Android users, we also gave a permissions notecard to those with Android phones.)
7. The participant filled out a survey about the applications installed on his or her smartphone. We asked each participant to go down their list of applications in a certain order; Android participants sorted applications alphabetically, and iPhone participants followed the list of icons as they appeared on their home screens. Again, participants were given 10 minutes to describe their installed applications, and we instructed them to skip pre-installed applications.
8. We conducted a structured interview about the participant's willingness to perform specific tasks on his or her smartphone and laptop. Specifically, we discussed nine tasks: using location-aware services (e.g., Maps, Twitter (optional), Foursquare, Yelp, etc.), using apps or websites that can charge them money (e.g., Skype will charge their credit cards for used minutes), logging into bank accounts, managing finances (e.g., Mint, Quicken), making purchases while shopping, checking work-related e-mail, using [their] Social Security Number (e.g., taxes), managing health documents, and sharing photos.

   For each task, we asked whether the user had previously performed the task using a laptop application, laptop website, smartphone application, or smartphone website. If a participant answered "no" to any of the four questions, we asked if he or she would be willing to do so if the situation arose. If a participant answered "sometimes," we asked him or her to elaborate on the conditions that would influence his or her decision.
9. Last, we asked participants (1) whether they worry about security on their smartphones more or less than security on their laptops, (2) whether they worry about privacy on their smartphones more or less than privacy on their laptops, and (3) what their primary concerns about their smartphones are. We asked participants to verbally explain their choices in each case.

4 Security and Privacy Perceptions

In order to help users securely achieve full device functionality, we must first identify how users perceive the security and privacy of these devices: Are they comfortable performing sensitive tasks on phone? How does their security model of the phone compare to the security model of the laptop? What do they particularly worry about with regard to their device?

Knowing how users consider their phones has implications for how our security efforts should be focused. In this section, we analyze how our survey participants typically use their devices and how they think about the security and privacy of their devices.

4.1 Task Willingness

Users' willingness to perform different types of potentially sensitive activities (e.g., giving credit card numbers, banking, location) on their devices naturally expose them to different levels of risk in revealing private information. To understand this, we asked participants free-form questions inquiring if they had performed specific types of tasks (e.g., shopping, reading work email) on their laptop and phone and their willingness to do so if they have not already performed such tasks.[3] We also inquired why they might not perform the task on their devices.

For each type of activity, we hypothesized that participants were less likely to perform the activity on their phones; we suspected that users may perceive their phones as less secure and also be apprehensive given the relative recency of smartphone adoption.

In Figure 1, we show the percentage of participants that either have or would be willing to perform each task on their device. In general, most participants (over 80%) have or are willing to perform each type of task on their laptop. However, they may be less likely to do some types of tasks on their smartphone.

We find that there is a significant difference in the users' willingness to use their SSN, make purchases, access health/medical records, and access their bank account on their smartphone as compared to their laptop. We find no statistical difference in the users' willingness to use finance management tools, share photos, access work-related email, and use location on either device.

[3] Only about half of the participants were asked about finance management and photo sharing, due to a delay in an IRB amendment.

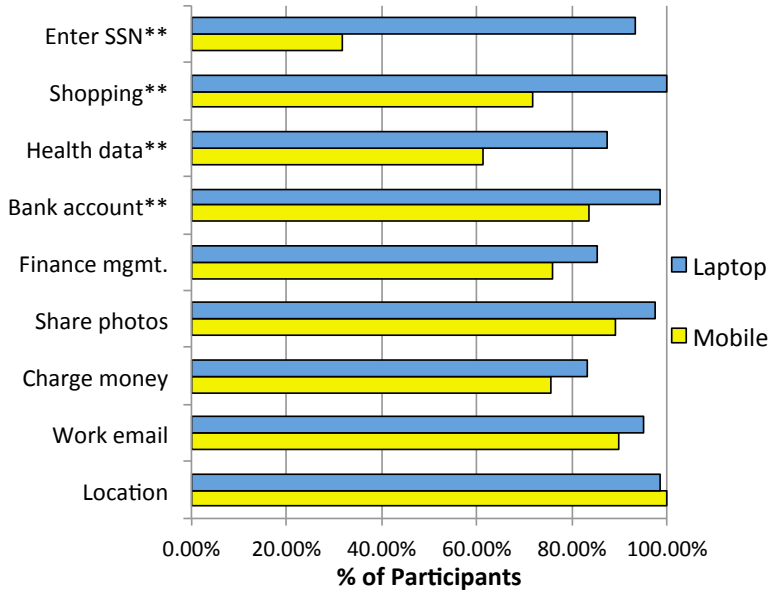


Figure 1: Percentage of participants that either have done it or would do it on their device. Asterisks mark tasks with statistically significant differences between devices.

When asked why they would not perform some specific activity, participants gave a whole spectrum of reasons such as "There's no need," "The laptop is easier to read," and "It's too insecure." We count the number of participants who cited security as a reason for their unwillingness in Table 1.[4] Overall, 62.5% (75 of 120) of smartphone responses were security-related. (19.2% of smartphone responses were usability related.) Security concerns played a major role in users' reluctance to enter their SSN, make purchases, access health data, and access their bank account on their phone. We discuss their reasons in greater depth for each type of task next.

	Laptop		*Mobile*	
Data Type	Security	Other	Security	Other
Enter SSN	4 (7%)	0 (0%)	36 (60%)	5 (8%)
Shopping	0 (0%)	0 (0%)	11 (18%)	6 (10%)
Health data	2 (4%)	6 (12%)	9 (18%)	10 (20%)
Bank account	1 (2%)	0 (0%)	8 (13%)	2 (3%)
Finance mgmt.	0 (0%)	5 (15%)	4 (12%)	4 (12%)
Share photos	0 (0%)	1 (3%)	1 (3%)	3 (8%)
Charge money	2 (3%)	8 (14%)	6 (10%)	9 (15%)
Work email	0 (0%)	3 (5%)	0 (0%)	6 (10%)
Location	1 (2%)	0 (0%)	0 (0%)	0 (0%)

Table 1: The number of people who would not perform certain actions on their devices because of security or other concerns.

4.1.1 Statistically Significant Results

SSN: Significantly more users were willing to enter their SSN on laptops than on their phone (exact McNemar, $p < 0.0001$). Four people would not give their SSN out even through their laptops citing security reasons. Of these, two people prefer to use their desktop computer and one person prefers to fax the information. Of the people who were willing to enter their SSN on their laptop, a number of people said they would do it only for tax purposes or only if it seemed secure.

[4]Participants were able to specify multiple reasons for their unwillingness.

In contrast only a minority (31.67%) of participants were willing to enter their SSN on their mobile phone. Of the 41 people who do not and would not give their SSN on their phone, 36 cited security reasons such as not trusting the relatively "new phone technology," fearing that the SSN will be stored by the application and then they will lose the phone, and generally distrusting the phone due to bugginess (thinking it may be infected).

Health Data: Similarly, participants were less willing to access health data on their phone (exact McNemar, $p = .0002$). Of the eight participants who would not use health document services on their laptop, most said they did not need such a service. Two participants said their willingness might depend on the reviews and security. Of the 19 participants who were unwilling to use health document services on their mobile phone, 9 participants gave security reasons; one participant's comment was particularly interesting: "The more health problems you have, the more potentially private they become, and the more private they become, the less likely I am to do it on a cell phone."

Bank Account: Participants are more willing to access their bank account on their laptops than on their phones ($\chi^2(1) = 9.00$, $p = 0.0027$). The one person who does not and would not access his/her bank account on his/her laptop cited security reasons and would only use the desktop computer for bank access. Of the 10 participants who do not and would not access their bank account on their phone, 8 cite security reasons, mentioning the fear of someone hacking into it as well as the fear of simply losing it. At least three people mentioned worrying about losing their phones. We also saw 2 people who were inclined to do banking from their phones but were prevented from doing so for some reason (e.g., their bank did not support it).

Shopping: For shopping purchases, we found a statistically significant difference between behavior on phones and laptops (exact McNemar, $p = 0.0002$). All participants have or would make purchases through their laptop. Of the 17 that have not and would not shop online on their smartphones, 11 cited security reasons. Some mentioned not being able to trust the applications: "1) I don't feel secure with the apps. 2) I almost always have my laptop with me and for some reason I just feel more secure. Or I'll wait 'til I get home...when I'm on a secure network." Some do not feel comfortable shopping on a WiFi network: "If I'm on my phone, I'm probably out and I'm a little wary of using my credit card cuz there are plenty of hackers hanging out in cafes in SF." Others fear physical phone loss: "No, because I lose my phones pretty often and normally they store the information, like your credit cards." We also note that 7 participants mentioned usability issues (e.g., hitting the wrong button during checkout or missing detailed information) as potential apprehensions with using shopping. One person said, "I just feel more clumsy with my phone [interface]. It seems like a pain...I'll just close applications on myself when I don't mean to. It's not tabbed so I don't know when I've quit something or just pushed it to the background. And I don't want that to happen in the middle of a payment or purchase and not know what's going on."

4.1.2 Other Comments

While we did not observe a statistically significant difference between phones vs. laptops for the other activities, the qualitative reasons that our participants cited in not running some of the tasks on their phones were nevertheless illuminating. We highlight some of these comments.

Location: We did not observe a statistically significant difference between mobile and laptop usage with respect to location-sensitive activities (exact McNemar, $p = 1.0000$). However, a few participants voiced concerns about tasks involving location information. Four people prefer not to give out location on their laptop for safety reasons and to avoid getting burglarized, as they use their laptop primarily in their home. Incidentally, all four participants concerned about robberies were female. Two participants were willing to use location-tracking applications except for social networking. These participants and two others mentioned they would be OK with social network-related location-tracking if they could turn it off at will and two more people mentioned that they would like to be able to turn off location tracking. Despite these privacy concerns, all participants barring one were willing to use location services on both devices, indicating that the utility that location-aware applications offer seem to override privacy concerns. Contrary to prior studies that suggested that location privacy is a critical issue for mobile phone users [36, 35, 32], our survey found no evidence that users are more concerned about location privacy on their phone. Users appear to be comfortable with location-based services on their phones and laptops, which suggests researchers' heavy emphasis on location privacy may be misplaced.

Financial Management: Similarly, we found no statistically significant difference with regard to financial management behavior (exact McNemar, $p = 0.3750$).[5] Of the five people who do not and would not use financial management software on their laptops, all specified that there was just no need for it at present. Of the eight people who do not or would not use financial management software on their mobile device, half give security reasons and the other half have no need or would prefer to use their laptop. Three people also cite user interface issues (e.g., accidentally making mistakes on the touchscreen).

Charge Money: Similarly, we found no statistically significant difference with regard to using applications that could potentially charge them money (exact McNemar, $p = 0.2668$). Of the ten participants who would not use an application that could charge them money on their laptop, only two of them had security concerns. The rest were primarily concerned with having additional charges or preferred finding versions that did not cost money. (This is likely a bias of our price-sensitive participant demographic.) Of the 15 participants who would not use an application that could charge them money on their phone, 6 people mentioned security concerns: For example, one person said, "I try not to use my credit card over the phone most of the time. I'm not very comfortable. On the phone especially." Others were concerned about blindly accepting charges or accidentally hitting a button that would charge them: For example, one participant said, "It just feels less secure. I just feel more clumsy with my phone [interface]...I'll just close applications on myself when I don't mean to...And I don't want that to happen in the middle of a payment or purchase and not know what's going on."

Work-Related E-mail: Similarly, we found no statistically significant difference with regard to checking work-related email (exact McNemar, $p = 0.2500$). The few participants who said they would not check email cited a lack of need, work-life balance, and readability issues.

Photo-sharing: Again, we found no statistically significant difference regarding willingness to share photos from their laptop vs. phone (exact McNemar, $p = 0.2500$). The only participant who would not share photos on their laptop simply said there was "no need to." Of the four people who do not do this on their phone, most were "not big photo taker(s)." The fourth is particularly security-sensitive about sharing photos due to a traumatic, recurring problem with her Facebook and Gmail accounts being hacked.

4.1.3 Discussion

Overall, participants are generally less willing to perform some tasks on their phones, especially when it comes to money-related tasks and personally sensitive data, such as SSN and health records. However, at least some of these problems could plausibly be addressed by better user interfaces; e.g., making users feel more comfortable about their online shopping experience on phones by assuring them that the credit card information is not stored or giving them additional visual cues before confirming purchases.

One potential concern is that the framing of the question "Would you be willing to do activity X?" might create a *pleasing bias*, where participants may say "Yes" to please the interviewer. However, since our hypothesis is that participants will be less willing to do this activity on their phones, this strengthens our observations. On the other hand, although we did not mention security and privacy during recruitment (nor were our questions overtly security-related at this point in the interview), some participants may alternatively assume the pleasing answer to be "No, I don't reveal this information" creating bias in the other direction. Similarly, another source of bias may be potential unwillingness to admit to "risky" behavior. Whichever way the bias goes, we expect it to apply similarly to both platforms. As our focus is on relative willingness (the comparison between willingness on the laptop and willingness on the smartphone), our comparison is valid even with such biases.

4.2 Perceptual Differences

Next, we analyze how security- and privacy-conscious our participants are and how these attitudes vary across the different platforms. We hypothesized that people are more concerned about both security and privacy on their phone. Figure 2 summarizes our findings. While we find no significant difference with regard to security, we see more participants are more concerned about privacy on their phones (51% compared to laptops' 13%) ($\chi^2(4) = 24.16$, $p = 0.0001$).

[5]We differentiate financial management from accessing bank accounts by defining it as a process that involves the aggregation of financial information by a third party (e.g., Quicken, Mint).

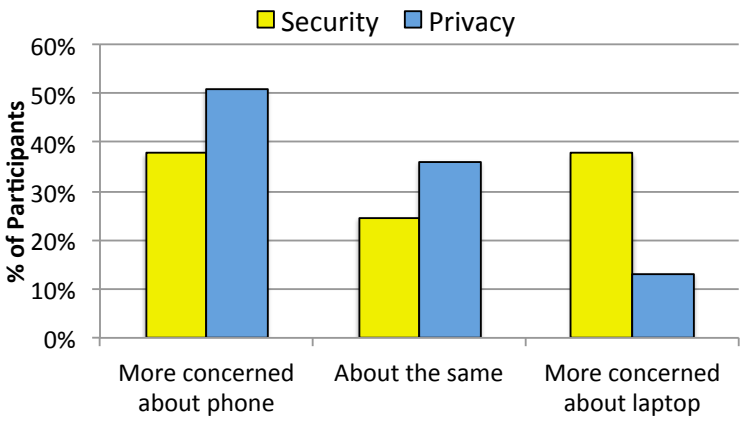


Figure 2: People's relative level of concern about security and privacy on their phone vs. their laptop.

We also asked participants to verbally explain the rationale behind their perception. Participants who were more concerned about security on their laptop gave a range of reasons, such as: they do not perform sensitive tasks on their phones, they have experienced first-hand or heard about friends getting attacked on laptops but not phones, and they rely on user reviews in mobile application markets as a security factor while these are generally not available for laptop applications. On the other hand, participants who were more concerned about security on their phone said they do not feel safe on Wi-Fi or 3G networks, they do not have anti-virus on phones, Apple products (i.e., iPhone) are safer, phones are easier to lose, and because phone technology and software is newer than laptops, they have less experience and knowledge about phones.

Participants who were more concerned about privacy on their phone mentioned that their phones carry more personal information (e.g., pictures, text messages), their phones reveal their location, and phone numbers are tied to their identity. Participants who were more concerned about privacy on their laptops simply said they do fewer personal things on their phone, do not use it as much, or they trust the iPhone brand more than the Windows brand.

This interview question also revealed that some participants' perceptions of security are influenced by incorrect beliefs about technology. Seven participants attributed their reluctance to use mobile phones to doubts about the security of mobile phones' wireless network connections (WiFi and 3G). For example, one participant said, "Any idiot with...$20 with malicious intent can pick up anything [over the air] from anyone with a cell phone." Another participant who expressed concerns about mobile phones' wireless network connections explicitly stated that she did not have the same worries about laptops:

> *Participant:* ...I tend to use my phone in environments where hackers hang out. Just going to a techie cafe and giving away your credit card on your iPhone seems like asking for it.
> *Interviewer:* So you don't bring your laptop to cafes?
> *Participant:* I do.

When asked to explain their perceived difference between laptop security and mobile phone security, another participant stated that using 3G on a mobile phone is less secure than using WiFi on a laptop because 3G does not require a password. The absence of a password made the participant believe that all data transmitted from a mobile phone is public to others who are physically nearby.

These participants' statements indicate that some users have misinterpreted security advice about public wireless networks. The intended purpose of network security warnings is to encourage users to use HTTPS websites when they are connected to untrusted networks. Instead, it appears that some users have become afraid of all wireless networks without understanding the threat. This has the unintended effect of deterring mobile phone usage in public.

4.3 Worries and Fears

We also asked each participant an open-ended question on their primary concerns about their phone. Due to the nature of the question and responses, we do not present quantitative data in this case. One potential bias is that we asked this

question after the previous discussion of activities. The discussion of their concerns may have primed them to be more security-conscious. Thus, we explicitly asked participants to think of broad concerns including and beyond security and privacy.

Among the top factors that participants mentioned were (in no specific order):

- physical phone loss (misplacement and theft)
- physical damage
- data loss and (lack of) backup
- reception/signal strength
- battery life
- trusting applications

Many people expressed worry about phone loss (17 people), damage (11 people), and data loss (5 people). Furthermore, these were often motivated by security and privacy concerns and not just about the inconvenience or monetary loss of the phone. Among the people that mentioned losing their phone, one participant said, "Losing it. Haha. There's a lot of data in there. Both: SSN, credit card info. I mean I store it there as well–stuff that I've accessed and of course personal stuff, photographs, whatever." Another person said, "Physically dropping it and walking downtown Oakland and somebody taking it from my hands and running from me. And then, you know, losing everything on there cuz I have pictures of friends and family."

Others expressed doubt in the trustworthiness of the applications: "..I haven't downloaded any of them because they don't agree with me: The permissions–they have access to this and that, and I don't want that." Another person said, "...they are always wanting me to commit to, you know, tracking you, or —and that I'm just weird about. And I never agree to it...I haven't followed through with it because I just didn't like it, I wasn't comfortable with what they wanted me to do."

Some worry about trying to preserve their privacy and security due to distrust of applications and have established creative, albeit roundabout, approaches: "Let's say if I ever were to create an account for an app, I actually put down an email address that I don't–uh, it's like a spam address. So I tried as often as possible to put in *not* actual information or I would never put in my credit card information."

These concerns show both worry about the security of the device itself (to protect their data) as well as the security and trustworthiness the applications installed on the device. Android and iPhone participants seem equally concerned about physical phone loss and damage. While Apple does provide a free iCloud service with an option to locate and remotely lock the phone (via the Find My iPhone app), it is likely that our participants were not aware of the service. (This service was released in Oct 2011, just two months before our study. Prior to this, iPhone had a for-pay service.) While Android also provides a remote backup service, our experience is that it is not very user friendly.

4.4 Main Observations and Implications

Our key takeaways are:

- Users are less willing to perform tasks that involve money (banking, shopping) and sensitive data (e.g, SSN, health records) on their phones than on their laptops.
- In addition to the security concerns they reveal by avoiding tasks on their phone, we find that users are more concerned with privacy on their phone than they are on their laptop. This is likely due to their increased inclination to perform privacy-sensitive tasks on their phone (location, photo sharing, text messaging, etc).
- These apprehensions stem from four main factors: worries about physical damage and physical phone loss, user interface concerns (e.g., click on purchase by mistake), their perception of the security and privacy properties of the phones, and some prevalent misconceptions about the security of their network connections on their phones.

We believe that these sources of apprehensions can be alleviated through the design of easy-to-use backup and remote phone lock/recovery services, better user interface design and visual cues for sensitive tasks, and steps toward educating users regarding when to trust or not trust their wireless connections.

One remaining concern is that even if we implement the above measures, users may still constrain their activities simply because they cannot trust the actual applications they run on their phones. In the next section, we address the issue of helping users trust their mobile applications and helping them gauge the security and privacy properties of their applications.

5 Installation Decisions

This section presents the factors that influenced participants' installation decisions. Our goal is to understand how and why users decide to install applications so that we can identify key points in the decision process where the application system may be improved. To this end, we examine the role of referral sources, user reviews, brands, and other security-relevant factors in participants' application installation decisions. We find that study participants often install free and unfamiliar mobile phone applications that they find via advertisements or browsing. However, a majority of participants downloaded their applications from centralized mobile phone application markets.

5.1 Application Discovery

We explore how survey participants heard about the applications installed on their device to identify how they discover applications.

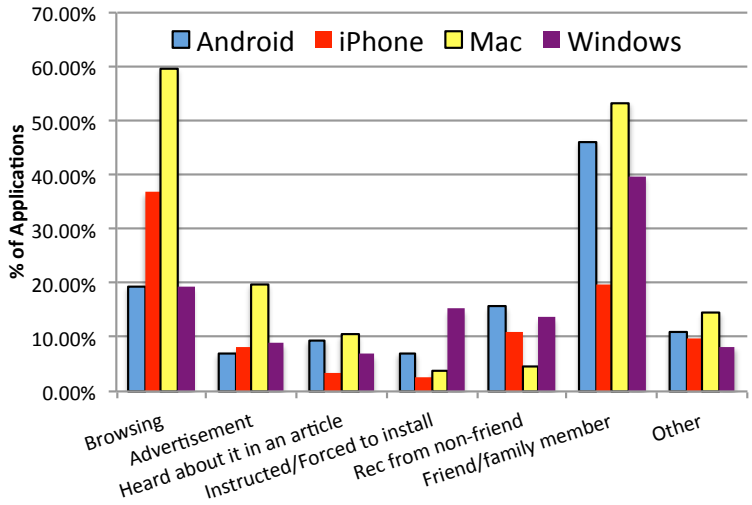


Figure 3: *How participants first heard about applications. The graph shows all of the applications recorded by all participants.*

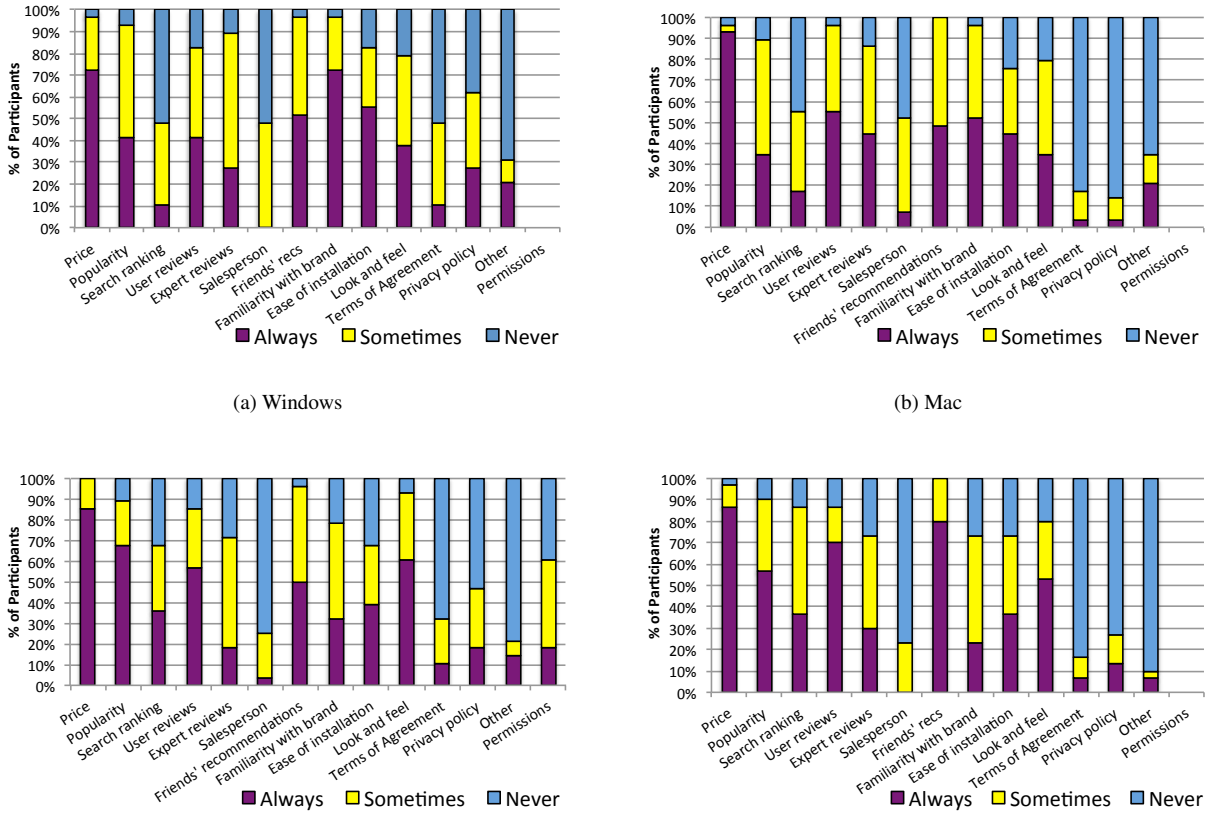
Figure 3 shows the referral sources of participants' applications. (Participants could record multiple referral sources per application.) It is interesting to note, despite the ease and availability of application markets for smartphones, there are not large differences in application discovery mechanisms between the devices. Two forms of referrals predominate: recommendations from friends and family members, and browsing. Installing an application from a trusted brand or recommended by a friend/family member likely represents a lower degree of risk than installing a relatively unknown application from an unknown developer discovered through an ad or casual browsing of the web/application markets. We find that 44.8% of iPhone applications and 15.7% of Android applications were discovered exclusively via browsing or advertisements without any additional referrals from other people.

5.2 Installation Factors

Once a user has discovered an application, he or she needs to decide whether to install it. We analyze the self-reported factors that influence participants' installation decisions.

Figure 4 reports data from the sorting exercises in which participants classified a set of installation factors (e.g., price, brand, screenshots) as factors they *Always consider*, *Sometimes consider*, or *Never/Rarely consider* during installation. We also asked participants to rank the factors within each group from most to least important. Price, popularity, and recommendations from friends and family are the three factors with the highest number of participants who "Always" and "Sometimes" consider them. Overall, participants are more likely to try free applications from unknown developers on their mobile phones, suggesting a larger security risk than on traditional laptop devices.

Certain factors might make participants more or less susceptible to malware. For example, a user who reads privacy policies, reads user reviews, and installs applications from trusted brands may be less likely to encounter malware or



(a) Windows

(b) Mac

(c) Android

(d) iPhone

Figure 4: *The relative importance of different factors considered while installing applications.*

grayware. Our installation factor analysis also provides insight into whether users consider existing security indicators (i.e., terms of agreement, privacy policies, and Android permissions).

Reviews: User reviews are a way of establishing trust in an application's safety and quality, even though individual user reviews themselves are not always trustworthy. More than 80% of participants reported that user reviews "Always" or "Sometimes" influence their installation decisions, regardless of platform. Due to the inclusion of user reviews in official mobile marketplaces, we hypothesized that user reviews would be more important in mobile application decisions than laptop installation decisions. However, our results do not support this hypothesis. We compared participants' rankings of reviews for their laptop installations and mobile phone installations using the Wilcoxon signed-rank test (which is appropriate for paired, non-parametric interval data) and found no significant difference ($z = 0.39$, $p = 0.69$). Instead, participants' laptop responses suggest that they are interested enough in reviews to seek them out even when they are not centrally available.

Brand: An application's brand name (e.g., the company that developed the software) can act as a security signal; familiar brands are less likely to be malware or grayware. We hypothesized that participants would be more likely to consider brands when installing laptop applications than when installing mobile phone applications because laptop brands tend to be established and well-known. To test this hypothesis, we asked participants how willing they would be to try an application from an unfamiliar brand or company. We asked this question twice: once for mobile phones, and once for laptops. Figure 5 shows participants' responses, which are on a scale of 1 (least likely to try an unfamiliar brand) to 5 (most likely to try an unfamiliar brand). We find that participants are more willing to try applications from unfamiliar brands on mobile devices than on laptops (paired one-tailed t-test, $p < 0.01$; responses were approximately normally distributed). This result is consistent with the factor rankings in Figure 4, where brand familiarity was mostly in the "Sometimes" category for mobile platforms.

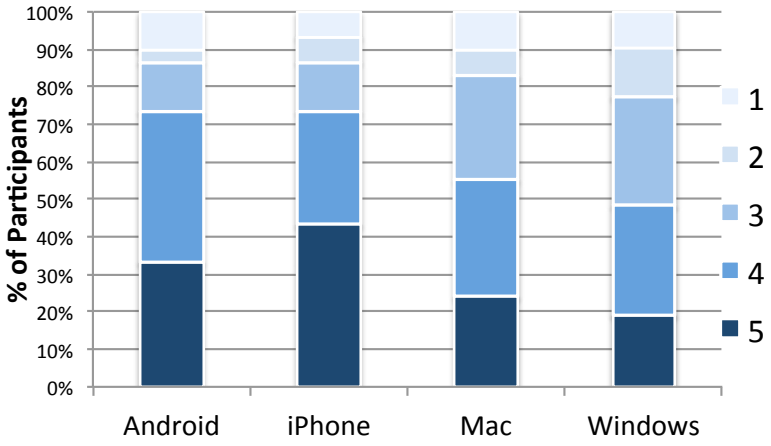


Figure 5: *The willingness of participants to try applications from unfamiliar brands, on a scale of 1 (least likely)–5 (most likely).*

Price: We hypothesized that users would be less likely to pay for mobile phone applications than laptop applications. To test this hypothesis, we asked participants whether each of their applications was free or paid. Figure 6 shows the results; the "Other" entries for Windows and Mac are primarily applications that came bundled with peripherals or were supplied by employers. We find that participants have significantly more free applications on their phones than on their laptops (Wilcoxon signed-rank test for matched, non-parametric data; $z = -4.54, p < 0.0001$). We also observe that participants with Android phones have a higher percentage of free applications than participants with iPhones (post-hoc Mann-Whitney test for independent, non-parametric data, adjusted for multiple testing with the Bonferroni correction; $z = 2.36, p < 0.025$), which is consistent with industry reports [10, 3].

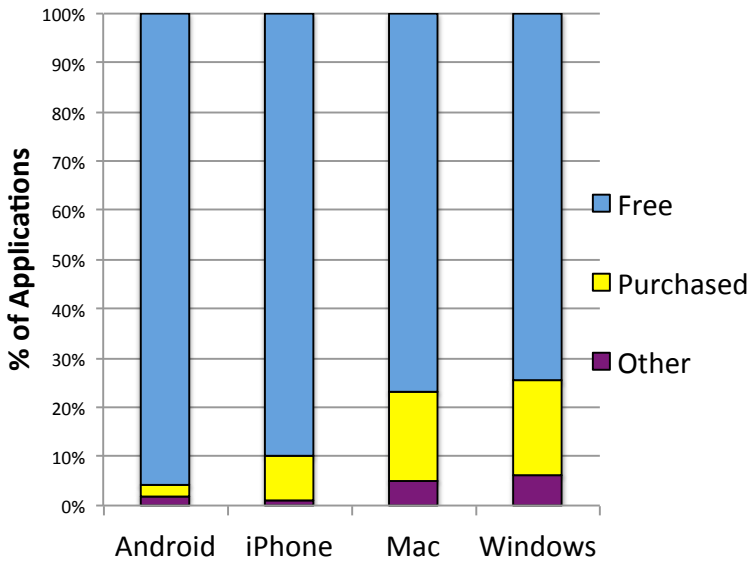


Figure 6: *The percentage of applications that were free or paid.*

Privacy: End user agreements, privacy policies, and terms of agreement are explicit security and privacy indicators. Few participants consider them before installing mobile phone applications, which is consistent with past literature [16, 6]. Surprisingly, 60% of participants with Android phones report "Sometimes" or "Always" considering permissions, although it is one of the lowest-ranked factors. These results indicate that participants rely on other indicators of trust (e.g., recommendations and reviews) instead of these explicit but hard-to-understand security and privacy indicators.

5.3 Application Download Sources

Users can install applications from online stores, physical stores, company websites, or "official" application marketplaces like the Apple App Store. The type of application download source influences the availability of security-relevant information prior to installation. For example, official application marketplaces list user reviews, salespeople work at physical stores, and company websites only provide favorable information about their applications. We are particularly interested in official marketplaces and large online stores because they have the potential to be augmented with additional information about privacy and security.

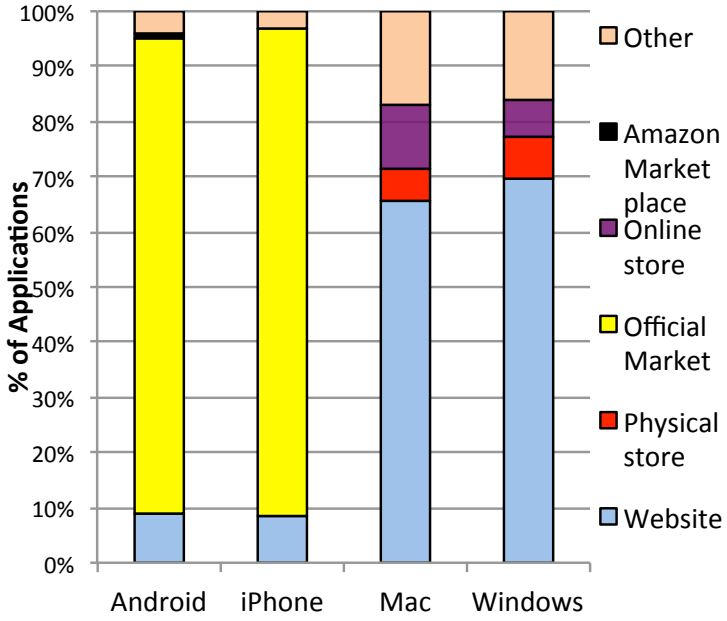


Figure 7: *Breakdown of application download sources*

We hypothesized that official application marketplaces are the dominant source for downloading mobile applications. To test this hypothesis, we collected data on where participants downloaded their applications from. Figure 7 shows the download sources for participants' applications, normalized by the total number of applications recorded for each device type. The results confirm our hypothesis: nearly 85% of mobile applications came from official marketplaces. This is promising as it suggests that adding new security features to official marketplaces would provide security information to most users during most installations. Prior work has shown that malware is much less common on official marketplaces than on alternative sources [41]. Our data suggests that users' exposure to malware from alternative sources may be modest.

5.4 Number and Types of Applications

We consider the number and types of applications that users install on their devices. The number and types of applications on a device can provide insight into the likelihood that a user encounters malware or grayware. In particular, users who install a large number of disposable applications on their devices have a higher risk profile than users who install a small number of applications. To explore this area, we asked study participants to count and categorize their applications; we checked and re-categorized applications as necessary for consistency.

We hypothesized that participants would have more applications on their mobile phones than on their laptops because mobile applications are less expensive. The mean and median numbers of applications installed on laptops were 21 and 12, respectively. In comparison, the mean and median numbers of applications installed on mobile phones were 36 and 24.5, respectively. Using the Wilcoxon signed-rank test for non-parametric matched data, the results support our hypothesis: participants installed more applications on their mobile phones ($z = -3.54, p < 0.001$).

Figure 8 depicts the types of applications that participants installed on their devices. The largest differences are between laptops and mobile phones rather than between platforms of the same device type. Participants appear to primarily use their laptops for productivity (e.g., MS Word), entertainment, browsing, and playing media. In the case of mobile phones, the top application types are entertainment, games, social networking, productivity, and shopping. Notably, transportation and shopping applications only appear on participants' mobile phones.

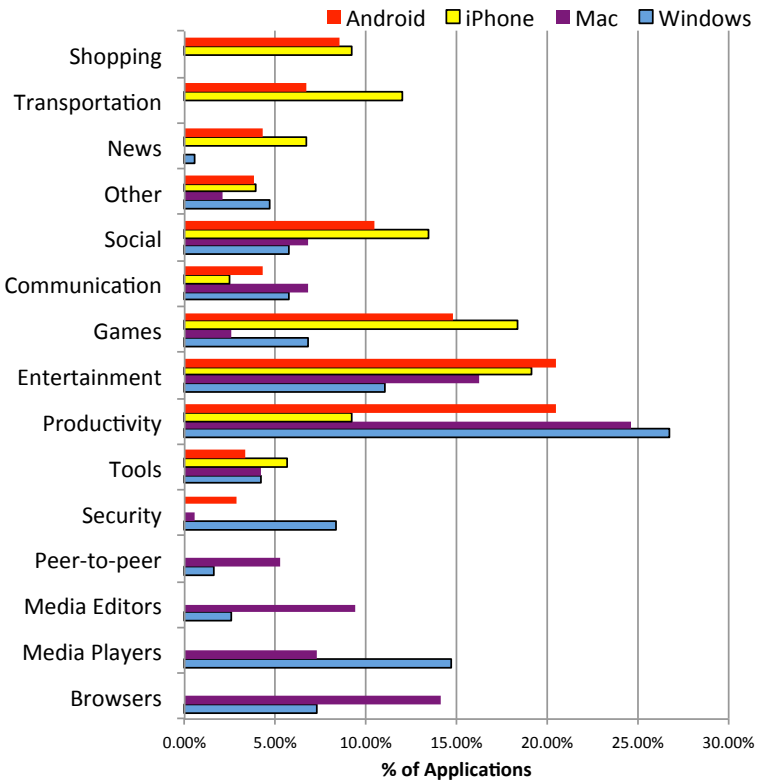


Figure 8: Types of Applications: Sorted by Percentage

5.5 Main Observations and Implications

Study participants reported that they are more willing to experiment with applications on their mobile phones. They are more likely to install free, non-brand-name applications on their mobile phones, and they often discover them via browsing or advertisements. Participants also do not greatly consider existing security indicators like privacy policies and EULAs. Instead, they rely on user reviews and popularity to signal the quality and safety of applications. Overall, participants' installation habits for mobile phones are potentially higher-risk than their laptop installation habits.

Given that participants are not interested in existing security indicators, we recommend the addition of new, user-friendly security indicators to official application marketplaces to help users. Study participants downloaded most of their applications from official marketplaces, which means that application market designers have an opportunity to influence nearly all application installations. Based on participants' habits and preferences, we believe that the most effective new security indicators would be:

- *Browsing.* Participants often find applications while browsing application markets. Markets could augment search results, lists of popular applications, and lists of recently-uploaded applications with security and privacy information.
- *Brands.* Mobile platforms are still relatively new. A program that identifies, establishes, and promotes "trusted" mobile brands could help users find trustworthy applications.
- *Reviews.* Most participants report that they read and consider user reviews. Reviews can alert users to undesirable applications, but they are not always reliable. Markets could support trusted reviewing programs that highlight reliable reviews.

6 Demographic Factors

In this section, we investigate whether the observations from the previous sections are influenced by specific participant attributes such as age, gender, and how long they have owned the device. This inquiry is preliminary: its purpose is to generate hypotheses that can serve as a basis for additional future research.

6.1 Information Gain

We want to understand if a specific participant attribute such as age or gender influences users' behaviors or perceptions. We use the metric of *information gain* [31] from machine learning and data mining literature to automatically identify "interesting" relationships between observations and participant attributes.

Background: Information gain is based on the notion of entropy. The entropy of a (discrete) random variable Y, denoted by $H(Y)$, is a measure of the "degree of randomness" or "uncertainty" in knowing Y. The entropy is highest when the distribution of Y is a uniform random distribution; it is lowest when Y is deterministic and takes exactly one value. Now, given a second variable X (e.g., age or gender), the information gain, denoted by $IG(Y, X)$, quantifies how much knowing the value of X reduces this uncertainty in Y. The relative information gain is simply the ratio $\frac{IG(Y,X)}{H(Y)}$. Intuitively, a high value of this metric means that X gives more information about Y and implies a stronger hidden relationship. Thus, computing the values of the relative information gain between the observation Y and many factors $X_1, X_2, \ldots$ helps us automatically identify the X variables that give us more information to identify relationships between variables.

Application: In our setting, the variable Y is some observation of user behavior (e.g., number or type of applications installed) and the variable X is a participant's attribute (e.g., age, or gender). A high value of the relative information gain tells us that the attributes gives us interesting information about the observation (e.g., do people of a certain age behave differently compared to the overall distribution?). Thus, we use the information gain as a way to systematically identify latent relationships between user behaviors and user attributes. Notably, the relationships are indicative; we do not and cannot claim high information gain as conclusive evidence of a causal relationship between the observation and attributes.

6.2 Results

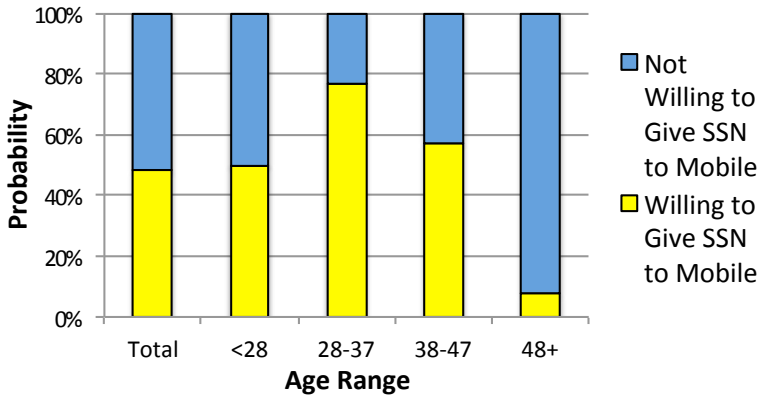


Figure 9: Willingness to use SSN on mobile applications, separated by age group.

We find a high relative information gain (0.19 or higher) between four factors and observations. For each of these, we performed post-hoc Fisher's exact tests and report the p-values. The four relationships with high information gain are:

- The age of the participant and the likelihood of them using their SSN on mobile phones. From Figure 9, we see that participants who are aged 48 or older are much less likely to be willing to disclose their SSNs on their phones ($p = 0.001$).
- The age of the participant and their concerns about privacy on mobile phones vs. laptops. Figure 10 shows that participants who are aged 48 or older tended to worry about privacy on their mobile phone more than on their laptops ($p = 0.011$).
- How long they have owned the phone and the most common factor they considered when installing applications. Participants who have owned the phone for less than half a year considered price more than others ($p = 0.437$).

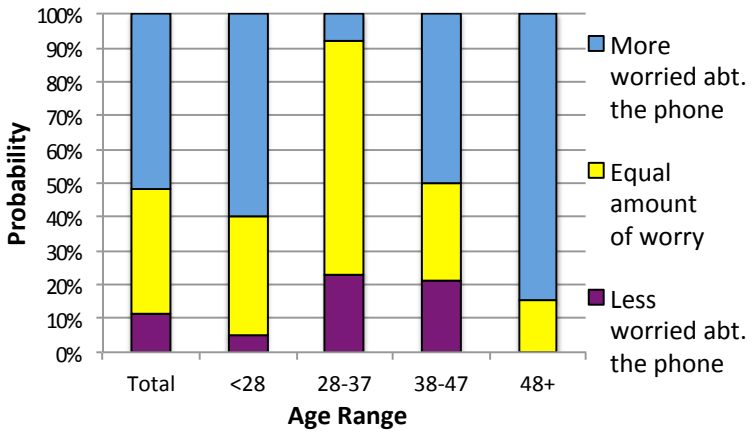


Figure 10: Comparison of whether they worry about privacy more on their phone or laptop, separated by age group.

- How long they have owned the phone and the amount they worry about security on mobile phones vs. laptops. Participants who have had the phone more than two years were less worried about phone security than laptop security ($p = 0.305$).

In order to determine whether the relationships between factors and observations are statistically significant, we compare the p-values to a significance level of 2.39×10^{-5}. We applied the Bonferroni correction to the significance level, using 2088 as the number of comparisons because the information gain analysis considered the relationships between 24 factors and 87 observations. Following this correction, we find that none of the trends are statistically significant. Despite this, they may be worth examining as a priori hypotheses in future research.

7 Discussion

In this section, we discuss the scope of our study and reflect on our results, summarizing the key findings on behaviors and misperceptions that are constraining users from exploiting the full potential of smartphones. Based on these findings, we provide general recommendations and opportunities for services that will help users safely and confidently use mobile applications and platforms. We conclude this section with some open questions.

7.1 Limitations

During our study, many people mentioned concerns about losing their phone or having it stolen. It is possible that higher levels of concern about theft or loss of phones (compared to laptops) may make people more reluctant to store sensitive data on their phones or more reluctant to enter sensitive data into smartphone applications. It is possible that this factor might contribute to differences in perception and behavior between smartphone and laptop use. Additionally, their concern may also be related to whether they lock their phone with a PIN or key pattern. We did not investigate these possibilities, but they would be good questions for future research.

It is also possible that differences in user authentication may affect users' perception of security on their laptops and phones. For instance, it is possible that users might associate entering a password with a feeling of security. If laptop users are used to typing a password to log into a website before entering sensitive information on that website, they may assume that their data is protected, whereas if they do not need to enter a password when using smartphone applications, they may feel less confident that the data they enter into the application will be stored securely. We did not study this possibility, but it too would be a good question for future studies to investigate.

Similarly, we did not examine whether users perceive the security of browsers differently from the security of applications (e.g. local vs. remote data storage) and whether they alter their behavior based on those perceptions. We would like to further examine this.

Although the participants referred to the applications on their phone to aid their memory (we prompted them to review their list of installed applications), our study is based on self-reported data. Self-reported data may be

susceptible to pleasing bias or under-reporting. While our interviews allow participants to elaborate on their response, which may reveal insights into their behavior, it would also be interesting to conduct a follow-on observational study to test our findings by observing actual user behavior.

7.2 Findings

Security and Privacy Perceptions: Study participants were more concerned with privacy on their phones than on their laptops. They were also less likely to make purchases and perform sensitive tasks (e.g., accessing health data) on their phones due to apprehensions regarding (1) the user interface and (2) the perceived security of their phones. On the other hand, while there has been a lot of focus on helping users feel comfortable with location-aware services, a majority of our participants use and are comfortable with using location services because of their perceived utility.

Misconceptions: We also observe that some of the users' apprehensions likely stem from misconceptions about the security of the applications and gaps in their understanding between the security of their wireless connections vs. end-to-end security.

Applications: We see that users are likely to install more applications on their mobile devices and that these are more likely to be Games or Entertainment applications compared to applications on their laptops. We find that users are likely to discover many applications via browsing, advertisements, and friends' recommendations. They are likely to be less brand-conscious and more price-conscious while installing applications on their mobile devices. They are also likely to ignore the applications' terms of service and policy agreements.

7.3 Recommendations

Based on our findings, we summarize opportunities for new services and mechanisms that might improve overall smartphone security and help users' confidently harness the full potential of mobile applications.

User education: As we saw earlier, several misconceptions about the security of platforms and the network connections may be preventing users from fully realizing the utility of smartphones. Educating users about the security properties of the different media and particularly emphasizing the benefits of end-to-end encryption can go a long way in helping clear such misconceptions. Previous lab studies have shown that such user awareness and training programs have been effective in other security contexts (e.g., [34]).

New security indicators: Several participants expressed mistrust in their applications, and many participants installed applications from unknown developers without considering the existing security indicators. Thus, we make a case for the creation of new security indicators in centralized smartphone application marketplaces. Participants often arrive at applications via browsing, so security indicators could be added to the browsing UI. We also find that participants do not consider smartphone brands, likely because smartphone platforms are too new for there to be established brands; new security indicators could help smartphone users identify "trustworthy" brands. Participants report that they often consider user reviews, but user reviews are not always reliable. An application market could institute a trusted reviewer program to flag and promote trustworthy user reviews.

User interfaces for sensitive applications: More usability efforts could be directed in increasing the participants' comfort-level with sensitive applications. For example, we could look into ways to make it more visually apparent to the user that they are on a secure network or interacting with a secure website. Participants also expressed that it is easy to accidentally press something that could cost them money or miss informative text. The user interface of such applications can be improved to encourage users to feel comfortable making such transactions using their phones. For example, one could think of better ways of using touch inputs that are specifically targeted towards purchase confirmations.

Better backup options: Users are concerned with data loss and physical loss of phone. Recent efforts such as iCloud show that industry leaders are beginning to take note of this problem. The adoption of such services, however, remains to be seen. In particular, today's backup software is difficult for the average user to easily configure. For example, there is no centralized mechanism for users to specify the type of data being backed up on the current Android platform. Making user interfaces and designing better default configurations to handle the common case (e.g., music, video, messages, email) would likely spur the adoption of such services.

Better remote lock services: To further address users' concerns with loss and theft of the phone, wireless carriers and platform vendors could provide value-added remote locking and remote wiping services. While there are AV vendors who do offer such services bundled with the security software [9], our participants seemed to be unaware of their availability. This will help ease users' fears about losing their phones, which appears to constrain their activity. Other alternatives to secure phones from loss or theft could be the design of better continuous authentication mechanisms (e.g., based on facial recognition) [37, 27].

7.4 Open questions

Mobile proficiency tests: One thing we would have liked to analyze is if user behavior, perception, and apprehensions are somehow related to proficiency. However, our initial efforts and pilot experiments at developing such a proficiency test revealed serious shortcomings in terms of the knowledge and activities we should ideally test. Furthermore, based on our observations of popular misconceptions even among participants that we considered computer proficient, we speculate that traditional metrics for computer proficiency developed for traditional desktop computing are likely to be insufficient predictors of mobile proficiency. Thus, it would be useful to create standardized testing procedures for measuring mobile user proficiency to complement the user education steps described earlier.

Moreover, we would like to measure whether application/task familiarity affects proficiency. Are users more comfortable on laptops due to their experience performing tasks on them and the relative time they have had with the laptop over the smartphone? Is smartphone task apprehension due to a temporary adjustment period or is it due to the current device environment?

Fine-grained demographic variations: Our preliminary investigation in Section 6 revealed some interesting differences between behaviors and perceptions across age groups. Our sample size prevents us from doing more fine-grained analysis of such demographic variations. For example, it would be interesting to look at combinations of two or more demographic factors: age and gender or age and proficiency taken together.

Would mobile findings extend to tablets? In addition to smartphones, we also see greater adoption of tablets, again with iOS and Android being the two dominant platforms. An open question is if users' behavior and perception differ between phones and tablets, and whether our observations regarding apprehensions with phone security also extend to tablets. For example, it is possible that theft and loss may be less of a concern with tablets given the form factor.

Other platforms: We chose Windows/Mac and Android/iPhone as the representative platforms for laptops and smartphones because they have a dominant market share today. It will also be interesting to understand similarities and differences between other platforms including Linux for laptops, and Blackberry and Windows Mobile for smartphones. Specifically, it will also be interesting to understand if user experience or comfort-level with a platform on the laptop also extend to their phones.

8 Conclusion

The smartphone ecosystem—application vendors, application markets, and usage patterns—is relatively new and quite different from traditional desktop computing. Consequently, we need to understand the security and privacy implications of user behaviors and perceptions at every step of the ecosystem before we can begin to improve the security of the device. This understanding can guide the design of solutions that will help users safely benefit from the potential and convenience offered by mobile platforms.

As a step toward this, we conducted a broad user study across 60 participants. We find that participants are apprehensive about running privacy- and financially-sensitive tasks on their phones as a consequence of four main factors: fear of theft and data loss, misconceptions about the security of their network communications, worries about accidentally touching/clicking, and mistrust of smartphone applications. Thus, we recommend that devices come pre-bundled with easy to use data backup, remote lock, and remote wipe services, and we make a case for better user education and user interfaces to address common misconceptions and apprehensions. To address users' mistrust of smartphone applications, we also propose the addition of new security indicators into centralized application markets. We find that participants often install a large number of applications from unfamiliar brands without reading the applications' privacy policies, which likely contributes to their mistrust of applications. We believe that this mistrust could be addressed by augmenting centralized markets with information about trusted brands and trusted application reviewers.

Acknowledgments

Many thanks to my collaborators: Adrienne Felt for her help interviewing participants, Vyas Sekar for his help interviewing participants and his expertise on information gain analysis, and David Wagner for his constant advice. Thank you also to Angie Abbatecola for her help with ensuring that laboratory study participants were paid in a timely fashion.

This material is based upon work supported by the Intel Science and Technology Center for Secure Computing and National Science Foundation Graduate Research Fellowship. Any opinions, findings, conclusions, or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of the National Science Foundation.

References

[1] Apple's Mac App Store downloads top 100 million. http://www.apple.com/pr/library/2011/12/12Apples-Mac-App-Store-Downloads-Top-100-Million.html.

[2] Google announces Bouncer service. http://googlemobile.blogspot.com/2012/02/android-and-security.html.

[3] Mobile application stores state of play. http://www.distimo.com/blog/2010_02_our-presentation-from-mobile-world-congres-2010-mobile-application-stores-state-of-play/.

[4] Most smartphone users browse, shop online with their phones. http://www.marketstrategies.com/news/2068/1/Most-Smartphone-Users-Browse-Shop-Online-With-Their-Phones.aspx.

[5] Pew: Smartphones overtake feature phones among adults in the U.S. http://www.bgr.com/2012/03/02/pew-smartphones-overtake-feature-phones-among-adults-in-the-u-s/.

[6] Privacy policy infographic. http://selectout.org/blog/privacy-policy-infographic/.

[7] Shopping behavior on phones. http://www.richrelevance.com/blog/2011/12/richrelevance-holiday-shopping-study-mobile-matters/.

[8] Smartphone, tablet sales outpace PC growth. http://graphics.thomsonreuters.com/12/02/GLB_TECHMKTB0212_SC.html.

[9] Top-5 Antivirus for Android. http://www.techclap.com/9486/top-5-free-antivirus-android-phone/.

[10] Why Eric Schmidt's prediction about Android vs. iOS development is dead wrong. http://www.networkworld.com/community/blog/why-eric-schmidts-prediction-about-android-vs-ios-development-dead-wrong.

[11] D. Anthony, D. Kotz, and T. Henderson. Privacy in location-aware computing environments. *IEEE Pervasive Computing*, 6(4):64–72, 2007.

[12] P. Bao, J. Pierce, S. Whittaker, and S. Zhai. Smart phone use by non-mobile business users. In *Proc. of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services (MobileHCI)*, 2011.

[13] L. Barkhuus. Privacy in location-based services, concern vs. coolness. In *Proc. of the Workshop on Location System Privacy and Control*, 2004.

[14] L. Barkhuus and A. Dey. Location-based services for mobile telephony: a study of users' privacy concerns. In *Proc. of INTERACT*, 2003.

[15] N. Ben-Asher, N. Kirschnick, H. Sieger, J. Meyer, A. Ben-Oved, and S. Möller. On the need for different security methods on mobile phones. In *Proc. of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services (MobileHCI)*, 2011.

[16] R. Boehme and S. Kopsell. Trained to accept?: A field experiment on consent dialogs. In *Proc. of ACM SIGCHI Conference on Human Factors in Computing Systems (CHI)*, 2010.

[17] C. Breen. Do you need antivirus software? `http://www.macworld.com/article/137397/2008/12/doyouneedantivirus.html`.

[18] S. Consolvo, I. E. Smith, T. Matthews, A. LaMarca, J. Tabert, and P. Powledge. Location disclosure to social relations: Why, when, & what people want to share. In *Proc. of the ACM SIGCHI conference on Human Factors in Computing Systems (CHI)*, 2005.

[19] D. Cvrcek, M. Kumpost, V. Matyas, and G. Danezis. A study on the value of location privacy. In *Proc. of the 2006 Workshop on Privacy in an Electronic Society (WPES)*, 2006.

[20] G. Danezis, S. Lewis, and R. Anderson. How much is location privacy worth? In *Proceedings of the Workshop on the Economics of Information Security Series (WEIS)*, 2005.

[21] S. Egelman, J. Tsai, L. F. Cranor, and R. Acquisti. Timing is everything?: The effects of timing and placement of online privacy indicators. In *Proc. of the 27th International Conference on Human Factors in Computing Systems (CHI)*, 2009.

[22] H. Falaki, R. Mahajan, S. Kandula, D. Lymberopoulos, R. Govindan, and D. Estrin. Diversity in smartphone usage. In *Proc. of the International Conference on Mobile Systems, Applications, and Services (MobiSys)*, 2010.

[23] A. Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner. A survey of mobile malware in the wild. In *Proc. of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM)*, 2011.

[24] J. Gideon, S. Egelman, L. Cranor, and A. Acquisti. Power Strips, Prophylactics, and Privacy, Oh My! In *Proc. of the 2006 Symposium on Usable Privacy and Security*, pages 133–144, July 2006.

[25] N. Good, R. Dhamija, J. Grossklags, S. Aronovitz, D. Thaw, D. Mulligan, and J. Konstan. Stopping spyware at the gate: A user study of privacy, notice and spyware. In *Proc. of the Symposium On Usable Privacy and Security (SOUPS)*, 2005.

[26] G. Iachello, I. Smith, S. Consolvo, M. Chen, and G. D. Abowd. Developing privacy guidelines for social location disclosure applications and services. In *Proc. of the Symposium on Usable Privacy and Security (SOUPS)*, 2005.

[27] K. Niinuma, U. Park, and A. Jain. Soft biometric traits for continuous user authentication. *IEEE Transactions on Information Forensics and Security*, 2010.

[28] A. K. Karlson, B. R. Meyers, A. Jacobs, P. Johns, and S. K. Kane. Working overtime: Patterns of smartphone and pc usage in the day of an information worker. *Pervasive Computing*, 5538:398–405, 2009.

[29] M. Kassner. Android security apps playing catch-up to malcode. `http://www.techrepublic.com/blog/security/android-security-apps-playing-catch-up-to-malcode/6534`.

[30] T. Matthews, J. Pierce, and J. Tang. No smart phone is an island: The impact of places, situations, and other devices on smart phone use. *Research Report RJ10452 IBM*, 2009.

[31] T. Mitchell. *Machine Learning*. McGraw-Hill.

[32] M. Ongtang, S. McLaughlin, W. Enck, and P. McDaniel. Semantically rich application-centric security in Android. In *Proc. of the 25th Annual Computer Security Applications Conference (ACSAC)*, December 2009.

[33] H. Pilz and S. Schindler. Are free Android virus scanners any good? `http://www.av-test.org/fileadmin/pdf/avtest_2011-11_free_android_virus_scanner_english.pdf`.

[34] S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L. Cranor, J. Hong, and E. Nunge. Anti-phishing Phil: The design and evaluation of a game that teaches people not to fall for phish. In *Proc. of the Symposium On Usable Privacy and Security (SOUPS)*, 2007.

[35] N. Sadeh, J. Hong, L. Cranor, I. Fette, P. Kelley, M. Prabaker, and J. Rao. Understanding and capturing people's privacy policies in a mobile social networking application. *Personal and Ubiquitous Computing*, 13(6):401–412, 2009.

[36] E. Toch, J. Cranshaw, P. Hankes-Drielsma, J. Springfield, P. Kelley, L. Cranor, J. Hong, and N. Sadeh. Locaccino: A privacy-centric location sharing application. In *Proc. of the 12th ACM International Conference Adjunct Papers on Ubiquitous Computing*, 2010.

[37] I. Traore and A. Ahmed. Continuous authentication using biometrics: Data, models, and metrics. `http://my.safaribooksonline.com/book/-/9781613501290`.

[38] J. Tsai, S. Egelman, L. Cranor, and A. Acquisti. The effect of online privacy information on purchasing behavior: An experimental study. In *Proc. of the Workshop on the Economics of Information Security*, 2007.

[39] R. Wash. Folk models of home computer security. In *Proc. of the Symposium on Usable Privacy and Security (SOUPS)*, 2010.

[40] J. Wiese, P. G. Kelley, L. F. Cranor, L. Dabbish, J. I. Hong, and J. Zimmerman. Are you close with me? Are you nearby?: Investigating social groups, closeness, and willingness to share. In *Proc. of the 13th International Conference on Ubiquitous Computing*, 2011.

[41] Y. Zhou, Z. Wang, W. Zhou, and X. Jiang. Hey, you, get off of my market: Detecting malicious apps in official and alternative Android markets. In *Proc. of the 19th Annual Network and Distributed System Security Symposium (NDSS)*, 2012.

APPENDIX

A Computer Usage Questions

- How long have you owned this computer?
- 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? 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? E.g., games, productivity, social, etc.
- Where do you usually look for applications? E.g., app stores, retail stores, Google search, etc.
- 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 autoupdate, Ignore until later if it requires you to restart your computer, Other]
- How many applications have *you* installed yourself on your computer?

B Computer Applications Questions

- Name of application
- What type of application is it? [Entertainment, Games, News, Security, Social Networking, Sports, Productivity, Other]
- Was this application: [Free, Purchased, Other]
- Where did you get this 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 BestBuy), Friends' recommendations, Familiarity with brand, Ease of installation, Screenshots, End User License Agreements and Terms of Services, The application's privacy policy, Other]
- How often do you use it? [Daily, Weekly, Monthly, A few times a year, Other]

C Mobile Usage Questions

- How long have you owned an [Android phone—iPhone]?
- 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? 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? E.g., games, productivity, social, etc.
- Where do you usually look for applications? E.g., app stores, retail stores, Google search, etc.
- 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 autoupdate, Ignore until later if it requires you to restart your phone, Other]
- How many applications have *you* installed yourself on your phone?

D Mobile Applications Questions

- Name of application
- What type of application is it? [Entertainment, Games, News, Security, Social Networking, Sports, Productivity, Other]
- Was this application: [Free, Purchased, Other]
- Where did you get this from? [Apple App Store, Android Market, Amazon Marketplace, Website, Other]
- 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 BestBuy), Friends' recommendations, Familiarity with brand, Ease of installation, Screenshots, End User License Agreements and Terms of Services, The application's privacy policy, Permissions (For Android phones only), Other]
- How often do you use it? [Daily, Weekly, Monthly, A few times a year, Other]

E Factors Considered

Participants were asked to put the following factors into 3 buckets: Always consider, sometimes consider, and never or rarely consider. They then sorted the top two buckets in rank order.

- Price
- Popularity of the application
- Search ranking/sponsored listing
- User reviews
- Expert reviews online (blogs, magazines, etc.)
- Salesperson suggestions in a store (like BestBuy)
- Friends' recommendations
- Familiarity with brand
- Ease of installation
- Screenshots
- End User License Agreements and Terms of Services
- The application's privacy policy
- Permissions[6]
- Other

[6]Only provided to those with Android phones

F Discussion Questions

Participants were asked:

- Have you used a website that is location-aware on your laptop? (E.g., Maps, Twitter (optional), Facebook (optional), Foursquare, Yelp)?
- Have you used an application on your laptop that is location-aware? (E.g., TweetDeck)
- If they answered no, they were asked: Would you install an application on your laptop that that can learn your location? Why/Why not? If you answered "sometimes," under what conditions?
- The previous questions were repeated but in the context of their mobile phones.

This series of questions was asked for the following topics:

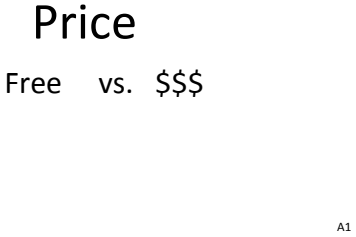
- Have you used an application on your laptop that is location-aware? (E.g., TweetDeck)
- Have you used an application on your laptop that can charge you money? (For example, Skype will charge your credit card if you use up your minutes. Some massive player games. Renewal of anti-virus.)
- Have you logged into your bank account on your laptop (via app)?
- Have you used a finance management application on your laptop? (E.g., Quicken)
- Have you made a purchase on a shopping site on your laptop (via app)?
- Have you accessed work-related email on your laptop via app?
- Have you given your Social Security Number to an application on your laptop? (E.g., Tax software)
- Have you used an application to manage your health documents on your laptop?
- Have you used an application to share photos on your laptop? (E.g., Picasa App, iPhoto)

Finally,

- 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?

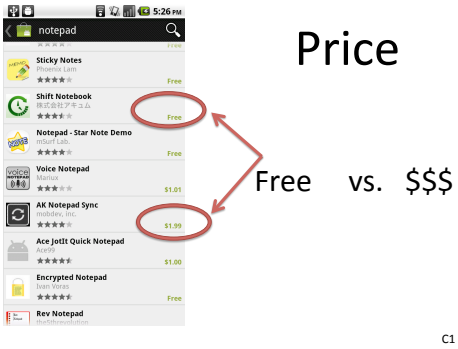
G Notecard Images

We include a few examples of the notecards we provided for the sorting activity. The first three sub-figures in Figure 11 show the differences in the laptop, Android, and iPhone sets. The remaining sub-figures are examples of some of the other cards.

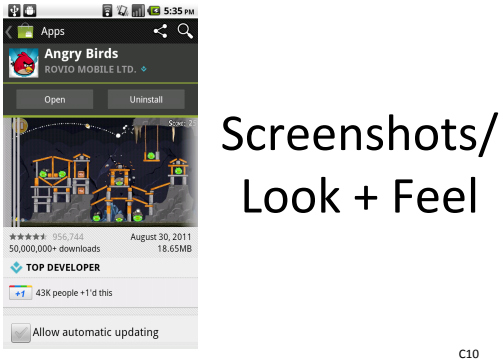


(a) “Price” notecard (laptop users)

(b) “Price” notecard (iPhone users)

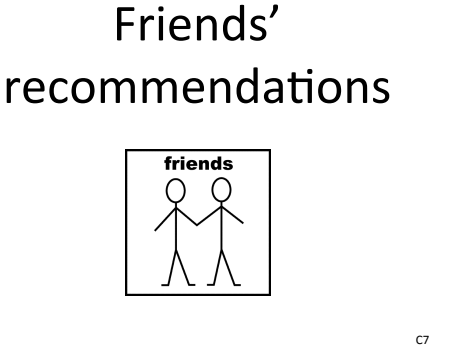


(c) “Price” notecard (Android users)



(d) “Screenshots/Look-and-feel” notecard (Android users)

(e) “Expert reviews” notecard (laptop, Android, and iPhone users)



(f) “Friends’ recommendations” notecard (laptop, Android, and iPhone users)

Figure 11: *Sorting Activity notecard examples*