Android Permissions: User Attention, Comprehension, and Behavior

Adrienne Porter Felt
Elizabeth Ha
Serge Egelman
Ariel Haney
Erika Chin
David Wagner

Electrical Engineering and Computer Sciences
University of California at Berkeley

Technical Report No. UCB/EECS-2012-26
http://www.eecs.berkeley.edu/Pubs/TechRpts/2012/EECS-2012-26.html

February 17, 2012

Acknowledgement

We thank Angie Abbatecola for her help with survey and study logistics, and Jennifer King for her insightful comments and discussion. This material is based upon work supported by Facebook and National Science Foundation Graduate Research Fellowships. Any opinions, findings, conclusions, or recommendations expressed here are those of the authors and do not necessarily reflect the views of Facebook or the National Science Foundation. This work is also partially supported by National Science Foundation grant CCF-0424422, a gift from Google, and the Intel Science and Technology Center for Secure Computing.

Android Permissions: User Attention, Comprehension, and Behavior

Adrienne Porter Felt*, Elizabeth Ha†, Serge Egelman*,
Ariel Haney†, Erika Chin*, David Wagner*
*Computer Science Department †School of Information
University of California, Berkeley
{apf,egelman,emc,daw}@cs.berkeley.edu, {lizzy,arielhaney}@ischool.berkeley.edu

ABSTRACT

Android's permission system is intended to inform users about the risks of installing applications. When a user installs an application, he or she has the opportunity to review the application's permission requests and cancel the installation if the permissions are excessive or objectionable. We examine whether the Android permission system is effective at warning users. In particular, we evaluate whether Android users pay attention to, understand, and act on permission information during installation. We performed two usability studies: an Internet survey of 308 Android users, and a laboratory study where we interviewed and observed 25 Android users. Study participants displayed low attention and comprehension rates: both the Internet survey and laboratory study found that 17% of people paid attention to permissions during installation, and only 3% of Internet survey respondents could correctly answer all three permission comprehension questions. This indicates that current Android permission warnings do not help most users make correct security decisions. However, a notable minority of users demonstrated both awareness of permission warnings and reasonable rates of comprehension. We present recommendations for improving user attention and comprehension, as well as identify open challenges.

1. INTRODUCTION

Android supports a booming third-party application market. As of July 2011, the Android Market included more than 250,000 applications, which have been downloaded more than six billion times [33]. Unfortunately, the growth in the Android platform has triggered the interest of unscrupulous application developers. Android grayware collects excessive amounts of personal information (e.g., for aggressive marketing campaigns), and malware harvests data or sends premium SMS messages for profit. Grayware and malware have both been found in the Android Market, and the rate of new malware is increasing over time [16, 45].

Google does not review or restrict Android applications. Instead, Android uses *permissions* to alert users to privacy- or security-invasive applications. When a user initiates the process of installing an application, he or she is shown the list of permissions that the application requests. This list identifies all of the phone resources that the application will have access to if it is installed. For example, an application with the SEND_SMS permission can send text messages, but an application without that permission cannot. If the user is not comfortable with the application's permission requests, then he or she can cancel the installation. Users are not shown permissions at any time other than installation.

Technical Report. University of California, Berkeley.

In this paper, we explore whether Android permissions are usable security indicators that fulfill their stated purpose: "inform the user of the capabilities [their] applications have" [4]. We base our inquiry on Wogalter's Communication-Human Information Processing (C-HIP) model, which provides a framework for structuring warning research [43]. The C-HIP model identifies a set of steps between the delivery of a warning and the user's final behavior. We connect each step with a research question:

1. *Attention switch and maintenance*. Do users notice permissions before installing an application? A user needs to switch focus from the primary task (i.e., installation) to the permission warnings, and she needs to focus on the permission warnings for long enough to read and evaluate them.
2. *Comprehension and memory*. Do users understand how permissions correspond to the risks of applications? Users need to understand the scope and implications of permissions.
3. *Attitudes and belief.* Do users believe that permissions accurately convey risk? Do users trust the permission system to limit applications' abilities?
4. *Motivation.* Are users motivated to consider permissions? Do users care about their phones' privacy and security and view applications as threats?
5. *Behavior.* Do permissions influence users' installation decisions? Do users ever cancel installation because of permissions? Users should not install applications whose permissions exceed their comfort thresholds.

Each step is critical: a failure of usability at any step will render all subsequent steps irrelevant. We focus on the first two steps but also study the end behavior, for an end-to-end assessment of how Android permissions affect user actions.

We performed two usability studies to address the attention, comprehension, and behavior questions. First, we surveyed 308 Android users with an Internet questionnaire to collect data about their understanding and use of permissions. Next, we observed and interviewed 25 Android users in a laboratory study to gather nuanced data. The two studies serve to confirm and validate each other.

Our primary findings are:

- *Attention.* In both the Internet survey and observational laboratory study, 17% of participants paid attention to permissions during a given installation. 42% of laboratory study participants were completely unaware of permissions.
- *Comprehension.* Overall, people demonstrated very low rates of comprehension. Only 3% of Internet survey respondents could correctly answer three comprehension questions. However, 24% of laboratory study participants demonstrated a competent (albeit imperfect) understanding of permissions.

- *Behavior.* A majority of Internet survey respondents claimed to have decided not to install an application because of its permissions at least once. 20% of our laboratory study participants were able to provide concrete details about times that permissions caused them to cancel installation.

Our findings indicate that the Android permission system is neither a total success nor a complete failure. Due to low attention and comprehension rates, permissions alone do not protect most users from undesirable applications (i.e., malware or grayware). However, a minority of laboratory study users demonstrated awareness of permissions and reasonable rates of comprehension. This minority could be sufficient to protect others if their opinions about application permissions could be successfully communicated via user reviews. We also found that some people have altered their behavior based on permissions, which demonstrates that users can be receptive to security and privacy warnings during installation.

Contributions. We contribute the following:

- Android permissions are intended to inform users about the risks of installing applications [4]. We evaluate whether Android permissions are effective security indicators.
- Researchers have speculated that Android permission warnings are ignored by users [17, 14]. We perform two studies to investigate how people use permissions in practice; to our knowledge, we are the first to provide substantive data.
- We explore the reasons why users do not pay attention to or understand Android permissions, and we identify specific problems with the way permissions are presented.
- We provide a set of recommendations for improvement to Android permission warnings and discuss open problems.

2. BACKGROUND AND RELATED WORK

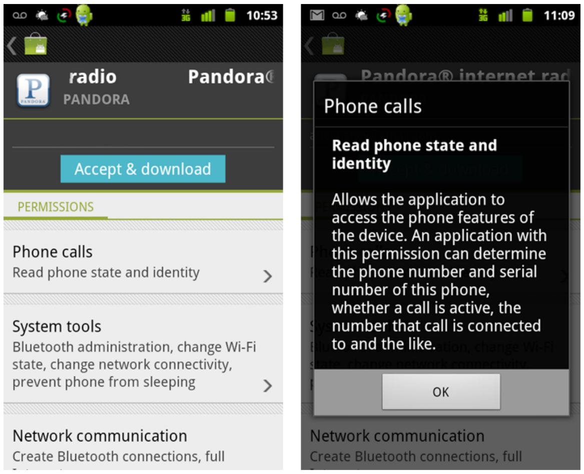
In this section, we provide an overview of Android permissions and the installation process. We then present some of the relevant literature on smartphone privacy and the effectiveness of warnings.

2.1 Android Permissions

In order to protect Android users, applications' access to phone resources is restricted with *permissions*. An application must obtain permissions in order to use sensitive resources like the camera, microphone, or call log. For example, an application must have the `READ_CONTACTS` permission in order to read entries in a user's phonebook. Android 2.2 defines 134 permissions.

Obtaining permissions is a two-step process. First, an application developer declares that his or her application requires certain permissions in a file that is packaged with the application. Second, the user must approve the permissions requested before installation. Each application has its own set of permissions that reflects its functionality and requirements. Users can weigh the permissions against their trust of the application and personal privacy concerns.

The official Android Market provides every application with two installation pages. The first installation page includes a description, user reviews, screenshots, and a "Download" button. After pressing "Download," the user arrives at a final installation page that includes the application's requested permissions (Figure 1). Permissions are displayed as a three-layer warning: a large heading that states each permission's general category, a small label that describes the specific permission, and a hidden details dialog. If an application requests multiple permissions in the same category, their labels will be grouped together under that category heading. If a user clicks on a permission, the details dialog opens. The details dialog may include examples of how malicious applications can abuse the permission (e.g., "Malicious applications can use this to send your data to other people"). The permission system gives users a binary choice: the user can cancel installation, or the user can accept all of the permissions and proceed with installation.


10:53
radio
Pandora
PANDORA
Accept & download
PERMISSIONS
Phone calls
Read phone state and identity
System tools
Bluetooth administration, change Wi-Fi state, change network connectivity, prevent phone from sleeping
Network communication
Create Bluetooth connections, full
11:09
Pandora® internet rad
Phone calls
Read phone state and identity
OK
Network communication
Create Bluetooth connections, full

Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and the like.

Figure 1: On the left, a screenshot of the Android Market's final installation page, displaying the application's permission requests. On the right, the permission dialog that appears if a user clicks on a permission warning.

On most phones, Android users can also download applications from non-Google stores like the Amazon Appstore. When a user selects an application through an unofficial store, that store might not present permission information. However, Android's installation system will always present the user with a permission page before the application is installed on the phone. Like the final installation page in the Android Market, the installer displays permissions as a multi-layer warning. This paper focuses on the Android Market's installation process because the official Android Market is the primary distributor of Android applications.

2.2 Smartphone Privacy

Past studies on smartphone users' privacy concerns have primarily focused on location tracking and sharing [5, 9, 28, 23, 35]. Although location sharing is an important aspect of smartphone privacy, only 2 of 134 Android permissions pertain to location. Concurrently, Roesner et al. [34] studied user expectations for location, copy-and-paste, camera, and SMS security. Our study encompasses all permissions and focuses on how users perceive the existing permission warnings.

In concurrent and independent work, Kelley et al. [24] performed twenty semi-structured interviews to explore Android users' feelings about and understanding of permissions. However, the scope of our study is much broader: we collected large-scale quantitative results, performed an observational study, and experimentally measured comprehension with multiple metrics. Their study exclusively reports qualitative data and does not address attention or behavior. Additionally, we designed our study to identify specific problems with the way permissions are presented.

Android privacy researchers have built several tools to help users avoid privacy violations. Most research has focused on identifying malicious behavior [14, 18, 13, 12, 45, 32], without considering how to help users make informed security decisions. However, two sets of researchers have focused on usability. Howell and Schechter proposed the creation of a sensor-access widget, which notifies the user visually when a sensor like the camera is active [21]. Roesner et al. proposed user-driven access control; rather than asking users to review warnings, this approach builds permission granting into existing user actions [34]. We focus on the usability of the existing system, rather than providing new tools or user interfaces. Our results should serve as motivation that research on improving permission usability is warranted.

2.3 Warning Research

Wogalter proposed a model of how humans process warning messages, known as the Communication-Human Information Processing (C-HIP) model [43]. The model formalizes the steps of a human's experience between being shown a warning message and deciding whether or not to heed the warning. C-HIP assumes that the user is expected to immediately act upon the warning, which is appropriate for research on computer security dialogs. (Other researchers have focused on situations in which consumers need to recall warnings for later use [29].) Researchers in the area of usable security have begun to use Wogalter's model to analyze the specific ways in which computer security dialogs can fail users.

Cranor used the C-HIP model as the basis for her "human in the loop" framework, which addresses problems for designers of interactive systems [10]. Egelman et al. used the C-HIP model to examine the anti-phishing warnings used by two popular web browsers to determine how they could be improved [11]. They recommend differentiating severe warnings from less severe ones, providing recommendations to the user, and eliminating jargon. Sunshine et al. performed a followup study using the C-HIP model to examine web browser certificate warnings [39]. They concluded that warnings should be designed based on the severity of the threat model, and that it is important to take context into account when offering suggestions to the user. Some of these lessons could be applied to Android permission warnings to improve them.

The Facebook Platform's security warnings are similar to Android's. A permission dialog is triggered when a third-party application requests access to personal data. King et al. asked participants whether they noticed the permission dialog before entering their survey, and only a minority responded affirmatively [25]. However, this result is not necessarily generalizable; the participants knew the survey application had been created by a privacy researcher, which likely decreased their interest in security indicators. They also presented survey participants with general comprehension questions about the Facebook Platform, such as whether Facebook applications are created by Facebook. Half of participants were able to answer each of these questions correctly.

Technology users' feelings about privacy are complicated and often contradictory. When asked directly about their privacy preferences, most surveys have found that people are very protective of their personal data [2, 8]. However, users' actions do not always correspond to their professed preferences [22]. This may be because users overestimate their privacy concerns or do not understand the ramifications of their actions (i.e., the user does not understand that the action violates his or her privacy preferences). As such, we design our inquiry into Android permissions to be robust to over-reporting of security concerns by directly observing users and asking questions about users' past actions.

3. METHODOLOGY

We surveyed 308 Android users with an Internet survey and interviewed 25 Android users in a laboratory study. The two studies were designed to confirm and validate each other. We recruited Internet survey respondents with AdMob ads and laboratory study participants with Craigslist ads; although both recruitment procedures might introduce bias, it is unlikely that the two procedures introduce the same biases. We pre-tested our studies with 50 AdMob-recruited Internet respondents and interviews of acquaintances.

3.1 Internet Survey

In September 2011, we recruited Android users to answer an Internet survey about Android permissions. The purpose of this survey was to gauge how widely understood and considered Android permissions are. To recruit respondents, we commissioned an advertising campaign using AdMob's Android advertising service. Our advertisement was displayed in applications on Android devices in the U.S. and Canada. (The advertisement did not appear on web sites.) As an incentive to participate, each person who completed a survey received a free MP3 download from Amazon.com. The advertisement included our university's name and said, "Survey for free Amazon MP3." We recruited people with AdMob advertisements because doing so restricted survey respondents to those using applications on Android devices.

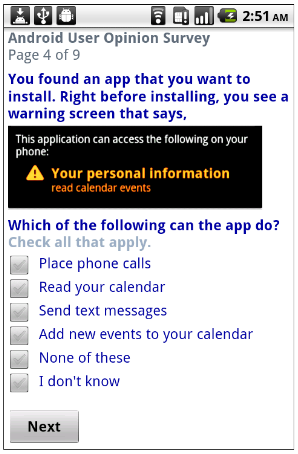
We paid AdMob $\$0.116$ per click and received $31,984$ visitors, of which $1,994$ (1%) began and 350 (17.5%) completed the survey. The rate at which people began the survey was likely influenced by the high rate of accidental clicks on advertisements on mobile devices [1] and our request that only people age 18 and over take the survey. Among people who started the survey, the completion rate was likely influenced by the difficulty of completing a survey on a phone. We ran the advertisement for two hours, and respondents completed it in an average of seven minutes.

We filtered out respondents who (1) stated that they were under 18, (2) had non-Android `user-agent` strings, or (3) appeared to be duplicates based on their IP addresses and `user-agent` strings. This left us with 326 unique responses. We designed our survey to make cheating (i.e., false responses for the purpose of receiving the reward) easy and obvious by making every question optional and providing an "I don't know" option for each question. Survey responses fell into two distinct groups: responses that were complete except for two or three "I don't know" responses, and responses that were incomplete except for one or two completed questions. Thus, we filtered out responses in the latter group. This resulted in a total of 308 valid responses.

The 308 respondents reported that they were 50% male and 49% female, with the remainder declining to report their gender. Respondents indicated that their age distribution was: 28% between the ages of 18 and 28, 28% between the ages of 29 and 39, 22% between the ages of 40 and 50, 15% between the ages of 51 and 61, and 5% over the age of 62. This age distribution is in line with Android age demographics [3], although the gender breakdown of our survey is more balanced than overall Android demographics.

The survey was nine pages long and meant to be completed on an Android smartphone. Each page filled a standard phone screen. We used the first three pages to ask respondents about Android usage information: how long they had owned an Android phone, from where they had downloaded Android applications, and the factors they considered when downloading applications. On each of the three subsequent pages, we randomly displayed 1 of 11 Android permission warnings and asked respondents to indicate what the permission allows the application to do. We gave respondents four choices, in addition to "none of these" and "I don't know." We then asked respondents to complete the three Westin index questions,[1] tell us about their past actions relating to Android permissions, and provide demographics information (age and gender).

[1] The Westin index is a set of three questions designed to segment users into three groups: Privacy Fundamentalists, Privacy Pragmatists, and Privacy Unconcerned [41]. The Westin index is widely used in surveys to gauge users' attitudes towards privacy [26]. Buchanan et al. validated the Westin index for use in a computing context by showing that it correlates with users' privacy concerns and behavior on the Internet [8].



Android User Opinion Survey
Page 4 of 9

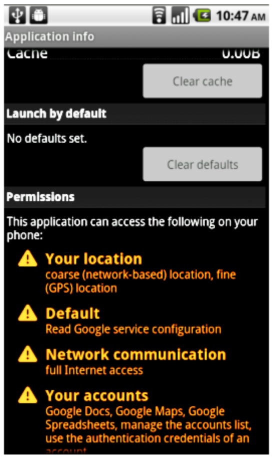
You found an app that you want to install. Right before installing, you see a warning screen that says,

This application can access the following on your phone:
⚠ **Your personal information**
read calendar events

Which of the following can the app do?
Check all that apply.

- ☐ Place phone calls
- ☐ Read your calendar
- ☐ Send text messages
- ☐ Add new events to your calendar
- ☐ None of these
- ☐ I don't know

Figure 2: Screenshot of a quiz question from the Internet survey.



Cache 0.00B

Launch by default

No defaults set.

Permissions

This application can access the following on your phone:

⚠ **Your location**
coarse (network-based) location, fine (GPS) location

⚠ **Default**
Read Google service configuration

⚠ **Network communication**
full Internet access

⚠ **Your accounts**
Google Docs, Google Maps, Google Spreadsheets, manage the accounts list, use the authentication credentials of an account

Figure 3: Screenshot of permissions on an application's Settings page.

Figure 2 depicts one of the quiz questions from the survey, and Table 3 lists the 11 quiz questions and choices. We designed the permission quiz questions to include one completely incorrect choice and one choice to test fine-grained comprehension (e.g., whether they understood that a permission to read calendar events does not include the privilege to edit the calendar). The set of 11 quiz questions included two questions about the `READ_SMS` permission: one to test the distinction between reading and sending SMS messages, and another to test respondents' familiarity with the "SMS" acronym. Survey respondents received only one of these two related questions, so scores for these questions were independent of each other.[2]

All of the quiz questions had one or two correct choices, with the exception of the question about the `CAMERA` permission. This permission controls the ability to take a new photograph or video recording; it does not control access to the photo library. However, we later discovered that all applications can view or edit the photo library without any permission. Consequently, the correct answer to the `CAMERA` permission question is to select all four choices.

3.2 Laboratory Study

In October 2011, we recruited 25 local Android users for a laboratory study. The primary purpose of the laboratory study was to supplement the Internet survey with detailed and explanatory data. We also designed the attention and behavior portions of the interview to avoid any over-reporting problems that might have influenced the Internet survey.

To recruit participants, we posted a Craigslist ad for the San Francisco Bay Area. Our advertisement offered people $60 to participate in an hour-long interview about how they "choose and use Android applications." In order to be eligible for the laboratory study, we required that participants owned an Android phone and used applications. We also asked study applicants to look at a screenshot and tell us whether they had the new or old version of the Android Market; we then secretly limited eligibility to users with the newer version of the Android Market. Google released a new version of the Market in August 2011, and not all phones had yet been upgraded. We decided to focus on users with the new version of the Market to reduce study variability.

Our Craigslist advertisement yielded 112 eligible participants. In order to match our participants' ages to Android demographics [3], we grouped applicants by age and selected a random proportion of people from each age group. We scheduled interviews with 30 participants. Three people failed to attend and two people had technical problems with their phones, leaving us with 25 completed interviews (12 women and 13 men). The age distribution was close to overall Android age demographics by design, with 20% of participants between 18 and 24, 32% between 25 and 34, 20% between 35 and 44, 16% between 45 and 54, and 12% older than 55. None of the participants were affiliated with our institution, although some of the younger participants were students at other universities.

Each interview took 30–60 minutes and had six parts:

1. General Android usage questions (e.g., how many applications they have installed).
2. Participants were instructed to find and install an application from the Android Market, using their own phones. We prompted them to install a "parking finder app that will help [the user] locate your parked car." This task served to confirm that participants were familiar with installing applications from the Android Market.
3. Participants were instructed to find and install a second application from the Android Market using their own phones. We prompted them to:

   > *Pretend you are a little short on cash, so you want to install a coupons app. You want to be able to find coupons and sales for groceries, your favorite electronics, or clothes while you're out shopping. If you already have a coupons app, pretend you don't like it and want a new one.*

   All of the top-ranked applications for search terms related to this scenario had multiple permissions. During this application search process, we asked participants to tell us what they were thinking about while using the Market. We also observed what user interface elements they interacted with.
4. Westin index questions.[1]
5. We asked participants about an application on their phone that they had installed and recently used. We then opened the application's information page in Settings (Figure 3) and asked them to describe and explain the permissions.
6. We asked participants for specific details about past permission-related behaviors, such as whether they have ever looked up permissions or decided not to install an application because of its permissions.

[2] In the remainder of this paper, we refer to these two questions as $\texttt{READ\_SMS}_1$ and $\texttt{READ\_SMS}_2$, as depicted in Table 3.

Two researchers performed each interview, with one acting as the interviewer and the other acting as a notetaker.

To promote a casual atmosphere, we held the interviews at a coffee shop and offered participants coffee, tea, or water. Participants used their own phones to encourage them to behave as they would in the real world. We made an effort to not prime participants to security or privacy concerns until the fourth task, at which point we specifically asked them about their attitudes towards privacy. We introduced ourselves as computer science students and did not reveal that we were security researchers until the end of the study. We prevented participants from determining the security focus of the study in advance by posting the Craigslist advertisement in the name of a researcher with no online presence or prior publications.

4. ATTENTION DURING INSTALLATION

Do users notice Android permissions before installing an application? Attention is a prerequisite for an effective security indicator: a user cannot heed a warning that he or she does not notice. In our Internet survey we asked respondents whether they looked at permissions during installation. To supplement this self-reported statistic, we empirically determined whether laboratory study participants were aware of permission warnings. We also report users' attention to user reviews, which are shown during installation.

4.1 Permissions

4.1.1 Internet Survey

In our Internet survey, we asked respondents, "The last time you downloaded an Android application, what did you look at before deciding to download it?" Respondents were able to select multiple choices from a set of options that included "Market reviews," "Internet reviews," "screenshots," and "permissions."

17.5% of 308 respondents (95%CI: [13.5%, 22.3%]) reported looking at permissions during their last application installation. Respondents who can be classified as Privacy Fundamentalists using the Westin index were significantly more likely to report looking at permissions than other respondents ($p < 0.0005$; Fisher's exact test). While statistically significant, the proportion of Privacy Fundamentalists who claimed to look at permissions was still a minority: 40.5% of the 42 Privacy Fundamentalists reported looking at permissions, whereas 13.9% of the remaining 266 respondents reported looking at permissions.

This self-reported question suffers from two limitations: some people over-report security concerns, and others may read permissions without knowing the technical term that refers to them. We asked survey respondents specifically about their "last installation" to discourage over-reporting, but people may still guess when they cannot remember. Our laboratory study served to confirm the results of the survey on a second population with a different metric.

4.1.2 Laboratory Study

In the follow-up laboratory study, we performed an experiment to empirically determine whether users noticed permissions during installation. We instructed study participants to talk us through the process of searching for and installing a coupon application. We recorded whether they clicked on or mentioned the permissions on the final Market installation page. To avoid priming participants, we did not mention permissions unless the participant verbally indicated that he or she was reading them. After each participant passed through the page with permissions, we asked him or her to describe what had been on the previous page.

Attention to Permissions	**Number of users**		95% **CI**
Looked at the permissions	4	17%	5% to 37%
Didn't look, but aware	10	42%	22% to 63%
Is unaware of permissions	10	42%	22% to 63%

Table 1: Attention to permissions at installation (Lab Study, $n = 24$)

We categorized participants into three groups:

- Participants who looked at permissions during the installation. These participants either told us that they were looking at permissions while on the page with permissions or they were later able to provide specific details about the contents of that page. They were also able to discuss permissions in general, indicating that the laboratory study was not the first time that they had viewed permissions. For example, one participant opened the page with permissions and stated,

  > *The only thing I started doing recently, is kinda looking at these – is there anything really weird.*

  When questioned, that participant described concern over "the network stuff."
- Participants who did not look at the permissions for this specific application, but were able to tell us that the final installation page listed permissions. In order to answer our question, these participants must have paid attention to permissions at some point in the past. For example, one participant in this category responded,

  > *I've seen a lot of them...A lot of 'em have full network access, access to your dialer, your call logs, and GPS location also.*
- Participants who were unaware that the final installation page included a list of permissions. For example, one participant said, "I don't remember. I just remember 'Download and install'." Another said, "I don't ever pay attention. I just accept and download it."

We did not require knowledge of the term "permissions"; participants typically used other phrases (e.g., "little warning things") to describe what they saw or remembered.

Table 1 shows the number of study participants that fall into each of the three categories. Fourteen participants (58% of 24) noticed permissions during the experimental installation or reported paying attention to permissions in the past.[3] The remaining participants were unaware of the presence of permissions on the final installation page in the Market. We did not observe a relationship between Westin indices and participants' attention to permissions.

Of the ten participants who did not look at permissions during the study but were aware of them, three volunteered that they used to look at permissions but no longer do. For example, one participant said, "I used to look...I just stopped doing that." These participants might have experienced warning fatigue, since users see permission warnings for about 90% of applications [17]. One participant said that she used to be concerned about the location permission, but gradually lost her concern because so many of the applications that she installed requested this permission.

Of the ten participants who had never paid attention to permissions, two knew that they were accepting an agreement on the final installation page. They both described the page as containing legal terms of use, with one incorrectly elaborating that the text specified

[3] For this statistic, we omit one participant who had never previously completed an installation without help.

Importance	Read reviews	Didn't read reviews
A lot	68%	4%
Somewhat	16%	4%
Mistrust	4%	0%
Unknown	0%	4%
Total	88%	12%

Table 2: We observed whether users read reviews, and later asked how much importance they place on reviews (Lab Study, $n = 25$)

legal restrictions on the use of the application. Due to their lack of interest in legal text, neither had ever read the screen so they were unaware that the text pertains to security and privacy.

The self-reported survey and observational study results both suggest that 17% of users routinely look at permissions when installing an application. We also find that 42% of study participants could not possibly benefit from permission information because they had never noticed it. The remaining 42% of participants are aware of permissions but do not always consider them.

4.2 Reviews

Like permissions, user reviews have the ability to convey privacy and security information during installation. User reviews can warn people about undesirable or privacy-invasive applications.

4.2.1 Internet Survey

We asked survey respondents, "The last time you downloaded an Android application, what did you look at before deciding to download it?" A total of 219 survey respondents (71.1% of 308; 95%CI: [65.5%, 76.2%]) reported looking at some type of review before installation. Of these, 193 respondents (62.7% of 308; 95%CI: [57.0%, 68.1%]) indicated that they looked at Market reviews during their last application installation, and 42 respondents (13.6% of 308; 95%CI: [10.0%, 18.0%]) stated that they had looked at other reviews on the Internet. Twenty-six respondents (8.4% of 308; 95%CI: [5.6%, 12.1%]) reported that they had looked at both Internet and Market reviews. We did not find that any age, gender, or Westin group was more or less likely to look at reviews.

4.2.2 Laboratory Study

In our follow-up laboratory study, we observed whether participants actually considered reviews during application installation. We instructed participants to tell us what they were reading and considering while selecting and installing a coupon application. We did not mention reviews or ratings unless the participant first spoke of or clicked on them. After participants mentioned reviews or ratings, we asked them how much importance they placed on reviews and whether they trusted them to be correct. If a participant did not consider reviews during installation, we asked the participant for his or her opinion of reviews after the installation task.

Table 2 shows participants' opinions of reviews and whether they considered reviews during the installation. All but three participants mentioned application reviews during installation; of the three that did not read reviews, two later claimed when questioned that they read reviews in some situations. The majority of participants placed a lot of importance on reviews. For example,

> *[Reviews] let me know if it's a decent app or not. Because most people will put on there whether it's a good app or a bad app.*

A few participants reported that they read reviews but simply treated them as one factor among many, rather than using them as their primary decision-making factor. One of these participants described the rating system as "a starting point," and another said that reviews are "just a place to start." One of the 25 participants actively mistrusts positive reviews because she has written reviews for her company's products on websites. Despite this, she still looks at reviews to identify negative traits of applications.

At the end of the study, we asked participants whether they had ever tried to find out what a permission means or why an application was asking for it. Eight of the study participants (32% of 25) responded affirmatively, with six (24% of 25) people stating that they found this information in some type of review. Three of these participants stated that they had read user reviews to determine whether an application's permissions were appropriate, and another two said that they had read news articles that reviewed applications' permissions. Another participant said that he read about permission information in reviews, but that he had never noticed that the same permission information was available on the final installation page. One of the six said,

> *If I'm not sure about an app I'll research it and see what other people say about the permissions. Like, 'It does this,' ...and, 'It's necessary.' And there will be an argument or a discourse about the permissions that need to be on there or don't need to be.*

This suggests that reviews are an important part of communicating permission information, especially for users who do not understand permission warnings on their own.

5. COMPREHENSION OF PERMISSIONS

Do users understand how permissions correspond to application privileges? Users can only make correct security decisions based on permissions if they understand what the permission warnings mean. We used three metrics to measure subjects' understanding of permission warnings. First, we tested Internet survey respondents with multiple-choice questions (Section 5.1). Second, we graded laboratory study participants' ability to describe the permission warnings of a familiar application (Section 5.2). Third, we asked study participants whether the application's set of permissions gave it the ability to send text messages (Section 5.3).

5.1 Permission Comprehension Quiz

Internet survey respondents answered three randomly-selected quiz questions from the set of eleven questions in Table 3. Six respondents omitted one or more questions; we filtered those participants out of this analysis, leaving us with 302 respondents who answered three quiz questions.

Eight respondents (2.6% of 302) answered all three questions correctly. On average, respondents correctly answered 21% of the three questions. We considered the relationship between respondent scores and demographics:

- We did not observe a correlation between respondent scores and the length of Android phone ownership.
- No significant differences were observed between the genders or with regard to Westin index classifications.
- There was a negative correlation between age and the number of correct answers ($r = -0.257$, $p < 0.0005$); younger people were more likely to understand permissions.
- We compared the scores of respondents who did and did not report looking at permissions in a past application installation. Respondents who reported looking at permissions scored higher on average (30.3% vs. 18.6%). The difference was statistically significant ($U = 5,293.0$, $p < 0.007$, $r = 0.16$) but small in absolute terms.

Permission	*n*	Options	Responses	
INTERNET Category: Network communication Label: Full Internet access	109	✔ Send information to the application’s server	45	41.3%
		✔ Load advertisements	30	27.5%
		✗ None of these	16	14.7%
		✗ Read your text messages	13	11.9%
		✗ Read your list of phone contacts	11	10.1%
		I don’t know	36	33.0%
READ_PHONE_STATE Category: Phone calls Label: Read phone state and identity	85	✔ Read your phone number	41	47.7%
		✗ See who you have called	37	43.0%
		✔ Track you across applications	20	23.3%
		✗ Load advertisements	11	12.8%
		✗ None of these	10	11.6%
		I don’t know	15	17.4%
CALL_PHONE Category: Services that cost you money Label: Directly call phone numbers	83	✔ Place phone calls	30	35.3%
		✗ Charge purchases to your credit card	27	31.8%
		✗ None of these	16	18.8%
		✗ See who you have made calls to	14	16.5%
		✗ Send text messages	11	12.9%
		I don’t know	16	18.8%
WRITE_EXTERNAL_STORAGE Category: Storage Label: Modify/delete SD card contents	92	✔ Read other applications’ files on the SD card	41	44.6%
		✔ Change other applications’ files on the SD card	39	42.4%
		✗ None of these	16	17.4%
		✗ See who you have made phone calls to	15	16.3%
		✗ Send text messages	11	12.0%
		I don’t know	15	16.3%
WAKE_LOCK Category: System tools Label: Prevent phone from sleeping	81	✔ Keep your phone’s screen on all the time	49	60.5%
		✔ Drain your phone’s battery	37	45.7%
		✗ None of these	7	8.6%
		✗ Send text messages	4	4.9%
		✗ Delete your list of contacts	4	4.9%
		I don’t know	13	16.0%
CHANGE_NETWORK_STATE Category: System tools Label: Change network connectivity	66	✔ Turn your WiFi on or off	36	52.9%
		✗ Send information to the application’s server	13	19.1%
		✗ Read your calendar	7	10.3%
		✗ None of these	7	10.3%
		✗ See who you have made calls to	5	7.4%
		I don’t know	17	25.0%
READ_SMS$_2$ Category: Your messages Label: Read SMS or MMS	54	✔ Read text messages you’ve sent	30	54.5%
		✔ Read text messages you’ve received	25	45.5%
		✗ Send text messages	10	18.2%
		✗ Read your phone’s unique ID	6	10.9%
		✗ None of these	4	7.3%
		I don’t know	11	20.0%
READ_SMS$_1$ Category: Your messages Label: Read SMS or MMS	77	✔ Read text messages you’ve received	44	56.4%
		✗ Read e-mail messages you’ve received	30	38.5%
		✗ Read your call history	13	16.7%
		✗ None of these	8	10.3%
		✗ Access your voicemail	8	10.3%
		I don’t know	13	16.7%
READ_CALENDAR Category: Your personal information Label: Read calendar events	101	✔ Read your calendar	56	53.3%
		✗ None of these	18	17.1%
		✗ Add new events to your calendar	12	11.4%
		✗ Send text messages	12	11.4%
		✗ Place phone calls	9	8.6%
		I don’t know	19	18.1%
READ_CONTACTS Category: Your personal information Label: Read contact data	86	✔ Read your list of contacts	52	60.5%
		✔ Read your call history	19	22.1%
		✗ None of these	14	16.3%
		✗ Delete your list of contacts	9	10.5%
		✗ Place phone calls	5	5.8%
		I don’t know	14	16.3%
CAMERA Category: Hardware controls Label: Take pictures	72	✔ Take pictures when you press the button	27	37.0%
		✔ Take pictures at any time	27	37.0%
		✔ See pictures taken by other applications	16	21.9%
		✔ Delete pictures taken by other apps	13	17.8%
		✗ None of these	13	17.8%
		I don’t know	17	23.3%

Table 3: Survey respondents were each asked three multiple choice questions, randomly selected from this set. Respondents could select “None,” “I don’t know,” or one or more of the four definitional choices. This table orders the choices by popularity.

	Permission	n	Correct Answers	
1 Choice	READ_CALENDAR	101	46	45.5%
	CHANGE_NETWORK_STATE	66	26	39.4%
	READ_SMS$_1$	77	24	31.2%
	CALL_PHONE	83	16	19.3%
2 Choices	WAKE_LOCK	81	27	33.3%
	WRITE_EXTERNAL_STORAGE	92	14	15.2%
	READ_CONTACTS	86	11	12.8%
	INTERNET	109	12	11.0%
	READ_PHONE_STATE	85	4	4.7%
	READ_SMS$_2$	54	0	0%
4	CAMERA	72	7	9.7%

Table 4: The number of people who correctly answered a question. Questions are grouped by the number of correct choices. n is the number of respondents. (Internet Survey, $n = 302$)

- In the survey, we asked respondents whether they typically used the Android Market or unofficial application stores. Respondents who typically used the Android Market were significantly more likely to understand the permissions ($U = 2,474.0, p < 0.001, r = 0.20$). The 28 respondents who did not use the Market had an average score of 4.7%, whereas the remaining 274 respondents had an average score of 22.3%.

Although we found statistically significant differences between certain groups, no group performed well on an absolute scale.

Table 3 depicts the popularity of each question choice. For each individual question, a plurality of respondents selected at least one correct choice. For six questions, a majority of participants selected at least one correct choice. This indicates that survey respondents were not randomly guessing, and most had some understanding of the permission warnings. Despite this, respondents still scored poorly overall because they selected too few choices (i.e., the response was incomplete) or too many choices (i.e., the response contained both incorrect and correct choices).

Not every question had a single correct choice: four of the questions had a single correct choice, six had two correct choices, and one had four correct choices due to a design error on our part. We consider an answer correct if that respondent specified all of the correct choices and no incorrect choices. Users performed significantly worse on questions with multiple correct choices ($r = -0.59$, $p < 0.028$; one-tailed), so we can only directly compare permissions with the same number of possible correct choices. Table 4 depicts the eleven permissions and the number of survey respondents who got each one completely correct. The table is sorted by the number of correct choices for each question.

We hypothesize that some respondents made decisions based primarily on the category headings, which are featured in a much larger font than the specific permission labels. This may have led respondents to overstate the meanings of permissions (i.e., they selected incorrect as well as correct choices). Respondents' answers to all but one of the permissions seem consistent with this hypothesis (Table 3). For example, the CALL_PHONE permission illustrates this type of error: the large category heading says "Services that cost you money," and nearly as many respondents selected the incorrect answer of "Charge purchases to your credit card" as the correct answer of "Place phone calls." The one question that does not fit this model is READ_SMS$_2$; most respondents were able to correctly determine that the READ_SMS$_2$ permission grants the ability to read but not send text messages.

5.2 Free-Form Permission Descriptions

We hypothesized that users might understand permission warnings better when the permissions are associated with a familiar application. For example, a user who does not understand the INTERNET permission in isolation might know that the permission is needed to fetch news from the Internet when he or she sees that the permission is associated with a news application. As such, we designed our follow-up laboratory study to ask users about the meaning of permissions in the context of a familiar application.

During the laboratory study, we asked each participant to view the permissions of an application that he or she had recently used on his or her phone. The participant was therefore familiar with the application's functionality. We asked participants to read each permission aloud and explain what it meant. We gave participants three chances to demonstrate their understanding of the permissions: we asked what the permissions meant, why the application had them, and whether each permission was necessary or unnecessary for the respective application.

To evaluate user understanding, we graded participants' descriptions of permissions. A participant's free-form explanation of a permission could be:

- *Correct.* A correct answer completely explains the meaning of a permission. For example, one participant correctly stated that the BLUETOOTH_ADMIN permission allowed the application to "create a Bluetooth connection" and "disconnect Bluetooth to save battery."
- *Correct but overly broad.* This type of answer contained correct information, but the participant believed that the permission granted more privileges than it actually does. For example, one participant understood that the INTERNET permission could be used to send or retrieve data, but he also believed it gave the application the ability to "check my GPS or see where I'm going." (In this example, the application did not have a location permission.)
- *Incomplete.* Incomplete answers show that the participant had a partial understanding of the permission, but lacked comprehension of an important aspect of the permission's meaning. For example, one participant understood that the RECEIVE_SMS permission was related to text messages but was not sure how.
- *Incomplete and overly broad.* This type of answer is incomplete, and the participant also believed that the permission grants more privileges than it actually does. One participant described the READ_PHONE_STATE permission as,

  > *Phone calls is probably like the call log or the phone calls that are made. It tells you their names and maybe a picture.*

  This description is partially correct because the permission relates to call state, but it is incomplete because the permission also provides access to the participant's own identity. The participant also incorrectly stated that the permission grants access to contacts' names and pictures.
- *Wrong.* In a wrong answer, the participant's statement was incorrect. Rather than omitting information, the participant made a statement that is actively wrong. For example, one participant said that the INTERNET permission was for "installing" Internet onto a phone.
- *Wrong and overly broad.* In a wrong and overly broad answer, the participant's incorrect statement included substantially more privileges than the truth. For example, several participants stated that the READ_PHONE_STATE permission gives applications the ability to listen to their phone

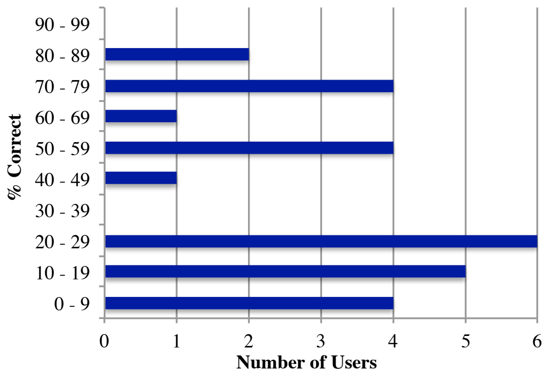


Figure 4: A histogram of participants' grades. (Lab Study, $n = 25$)

calls. This confusion likely occurred because the category heading for that permission is "Phone Calls."

- *Unable to answer.* We placed responses in this category when the participant read the permission aloud and then stated that he or she could not describe the permission.
- *Omitted.* Participants often skipped permissions that were present on the screen, and we were not always able to prompt them to address the skipped permission. In these cases, we have no way of knowing whether the participant would have been able to answer correctly.

Figure 4 depicts each laboratory study participant's grade, where a person's grade is the percentage of descriptions that are correct. We calculated this percentage after filtering out permissions that they omitted; omitted permissions are excluded because we do not know why they were omitted. Two participants received grades of 0%, the highest grade was 83%, and the average was 39%. Contrary to our initial hypothesis, comprehension rates are still low when permissions are associated with a familiar application.

Six participants received grades of 70% or higher. We observed two of the six high scorers looking at permissions during installation (Section 4.1), and another three indicated that they had looked at permissions in the past. The permission system could potentially help these five participants (20% of 25) because they sometimes pay attention to and understand permission warnings. The sixth high scorer expressed some familiarity with permissions but did not know that the Market displayed them prior to installation.

Other participants commonly said that they did not know what the warnings meant: 25% of the times that a participant read a permission, he or she was completely unable to describe it. Several participants mentioned that they understood all of the vocabulary but did not know how that information pertained to their phones. As one participant said,

> *I think I know what they mean as a person who has zero electronics or programming training, just in terms of what I think the words mean...I know what they mean in terms of the face value of the words. I don't really know what they mean in terms of complicated, in terms of technicalities...*

Participants' grades are not directly comparable to each other because each participant viewed a different application's permissions. However, a few popular permissions were present in 11 or more participants' applications. Table 5 shows how participants performed when describing these permissions. Notably, participants performed better on the three permissions that refer to general computer concepts: Internet access, hard drive storage, and putting the phone to "sleep." Participants were less able to describe the two smartphone-specific permissions.

Participant response:	**Yes**	**No**	**Unsure**
Correct	4%	32%	-
Incorrect	44%	12%	-
Total	48%	44%	8%

Table 6: Can an application send text messages? The correct answer depends on the application that the given user selected. (Lab Study, $n = 25$)

We observed that participants tended to place more emphasis on the category heading than the specific permission text. (Figure 1 shows examples of categories and specific permissions.) One side effect of this behavior was that participants erred in the direction of overstating the privileges associated with permissions. Descriptions were overly broad 18% of the time, and all but 3 of the overly-broad responses could be attributed to the category heading. Many of the wrong answers also stem from over-emphasizing the category heading. For example, the `READ_CONTACTS` permission is under the heading of "Personal Information." Upon seeing that warning, one participant stated that the permission provided access to his passwords, and another believed that the permission encompassed all of the data on her phone. Others listed types of personal information that might not be in their list of contacts (such as their own names and addresses). Similarly, the `READ_PHONE_STATE` permission is under the heading of "Phone Calls." Participants inferred that the warning referred to a wide variety of phone-related behavior, such as giving a company permission to make telemarketing calls to the participant.

5.3 Specific Permission Comprehension

After each participant described the set of permissions, we asked him or her whether the selected application had the ability to send text messages without his or her knowledge. If the participant asked for clarification, we elaborated that we wanted to know whether the application *can* send text messages, not whether it does. This privilege is granted with the `SEND_SMS` permission, which is in the "Services that cost the user money" category with the specific permission label of "Send SMS messages." This question was designed to gauge whether people can determine the tasks that an application can do on their phones, given its permissions. We chose the `SEND_SMS` permission for this question because we thought that all participants would be familiar with text messages, and the permission is associated with malware [16, 45].

Table 6 presents participants' responses. The correct answer depends on the application that the given user selected. Only nine of the participants (36% of 25) answered correctly. Participants' answers were not significantly different from guessing: twelve responded affirmatively and eleven negatively.

Four participants selected applications with the `SEND_SMS` permission, and three of them incorrectly stated that the application could not send text messages. One of these participants had asked us about the meaning of the `SEND_SMS` permission during the previous step of the laboratory study, and she correctly repeated our explanation. Despite this, she still responded that the application could not send text messages. She re-examined the permission warning after our question and stated,

> *Well, I don't know now. Cause it said that it could – I don't know. I'm going to say no.*

Another participant was aware that her chosen application could send text messages because of her experience with the application,

	READ_CONTACTS	WAKE_LOCK	WRITE_EXTERNAL_STORAGE	READ_PHONE_STATE	INTERNET
Correct	0%	54%	47%	0%	68%
Correct but overly broad	9%	9%	0%	0%	4%
Incomplete [and overly broad]	18%	0%	18%	45%	9%
Wrong [and overly broad]	45%	0%	23%	20%	9%
Unable to answer	27%	36%	12%	35%	9%
Total number of participants	11	11	17	20	22

Table 5: The grades of free-form participant responses for popular permissions. (Lab Study, $n = 25$)

but she still believed that it was not capable of sending text messages without her express approval. She seemed to believe that all applications require user approval to send text messages, regardless of the permissions. The third person looked at the category heading ("Services that cost the user money") and incorrectly decided that it referred to Internet data and phone calls but not text messages.

Twenty-one participants selected applications that do not have the SEND_SMS permission. Of those, eleven participants incorrectly thought that their applications could send text messages. When asked why, six participants explained that various other permissions allow this behavior. Two people said that the INTERNET permission (listed under the "Network communication" category heading) allows an application to send a text message. For example,

> *It has access to my network, so I assume it could send a message if it wanted to.*

Four people believed that the READ_PHONE_STATE permission (listed under the "Phone calls" category heading) grants the ability to send text messages. For example,

> *Well, yeah, because of the phone calls. Because of the phone calls, they can read the phone calls, so obviously they can.*

A sixth participant believed that the application could combine the personal information, phone calls, and network communication categories together to send a text message.

One of our participants said he had a small amount of experience as an Android developer. He was among the eleven participants who incorrectly stated that an application could send text messages. When asked for an explanation,

> *I've done some programming but I don't know all the permissions. ... I just don't know if the permissions are so fine grained that they make texting a special permission that you have to add.*

The participant then reasoned that two other permissions likely include that ability. Without knowing the full list of possible Android permissions, it is difficult for a user – even a highly experienced, technically competent user – to determine whether an application cannot perform an action. In other words, users need to know what permissions their application does not have in order to comprehend the scope of the permissions that it does have.

6. INFLUENCE ON USER BEHAVIOR

Do permissions influence users' installation decisions? Users are shown permissions on the final installation page of the Market so that they can refrain from downloading an application if they dislike its requested permissions. We asked users whether they have ever decided not to install an application because of its permissions.

6.1 Internet Survey

The survey asked, "Have you ever not installed an app because of permissions?" Respondents were shown the following four choices:

- Yes, I didn't like the permissions
- Yes, there were too many permissions
- No
- I don't know

A respondent could select both of the affirmative options, and the answers were not randomly ordered.

Self-Reported Behavior	**Respondents**
Yes	56.7%
Didn't like permissions	*32.6%*
Too many permissions	*16.0%*
Both	*8.1%*
No/I don't know	43.3%

Table 7: Respondents who claim they did not install an application due to permissions. (Internet Survey, $n = 307$)

Self-Reported Behavior	**Participants**	
Yes	5	20%
Probably	2	8%
No	18	72%

Table 8: Participants who claim they did not install an application due to permissions, with confirming details. (Lab Study, $n = 25$)

We received 307 responses. Table 7 shows the results: 56.7% of respondents (95%CI: [52.1%, 62.3%]) claim to have decided not to install an application because of its permissions. We find that respondents who can be classified as Privacy Fundamentalists using the Westin index are more likely than other respondents to report not installing an application due to its permissions (χ^2=5.6161, $p = 0.016$): 73.8% of the 42 Privacy Fundamentalists (95%CI: [60.5%, 87.1%]) responded affirmatively, compared to 53.9% of the 265 remaining respondents (95%CI: [47.9%, 59.9%]).

The number of affirmative responses to this question may be artificially inflated because of position bias; people display a slight preference for the first choice over later choices [7]. Survey respondents viewed this question after seeing the permission quiz questions, which also may have increased their likeliness to respond affirmatively. We asked survey respondents about a past action rather than a preference to mitigate over-reporting, but people may err with a bias when they cannot remember the answer.

6.2 Laboratory Study

In our follow-up laboratory study, we asked participants the same question: "Have you ever not installed an app because of permissions?" However, we designed the laboratory study question to avoid over-reporting. If a person responded affirmatively, we asked for detailed information about the application and why he or she objected to the permissions. Although people often over-report their security concerns when asked abstract questions, we feel it is unlikely that a participant would fabricate specific details of his or her application installation history in an in-person interview.

Table 8 shows how study participants responded to this question. Two participants thought that they had chosen not to install an application because of its permissions, but they were uncertain and unable to provide details.

We asked the five affirmative participants to explain why and how often they had decided not to install certain applications based on their permissions. Here, we excerpt their concerns:

- One person decided not to install a social networking application because "with exact location then they could post that on my page or something like that."
- "At least five. I felt it was asking for too much, or it was going to do too much data, and I didn't feel comfortable."
- One participant became alarmed after reading a Wall Street Journal article about Android applications' permissions and privacy policies [42]. "I haven't really downloaded very many apps since... And there have been a few I haven't downloaded because they asked for a bunch of accesses."
- "In the zone of maybe one out of four, roughly. Mostly most of them look fairly benign to me in terms of my concerns, but there are some of them that just look like they're overkill. I must say that in the beginning of installing apps, I – and I believe most people – are more hesitant about installing apps that reveal your location."
- Another person was aware of permissions but did not read them on his own. Instead, he would look for reviews about certain permissions pertaining to battery life. "Some of the ones that people say, 'It runs at startup,' and, 'You can't stop it,' or something like that...then I won't download it."

Two of the five participants who said that they had not installed an application because of permissions scored very poorly on the comprehension study (Section 5.2). One was unable to describe any permissions correctly, and the other described only two of seven permissions correctly. This shows that people may act on permission information even if they do not correctly understand it.

Through our attention and comprehension studies, we identified five participants who were aware of and understood permissions relatively well. Two of those participants said that they had cancelled installation due to permissions in the past. In other words, 8% of 25 participants paid attention to, understood, and previously acted on permissions. It is unclear why the other three participants who paid attention to and understood permissions have never cancelled installation because of permissions; it is possible that they lack motivation, lack trust in the permission system, or have simply not yet encountered a suspicious application.

7. IMPLICATIONS

We evaluated whether the Android permission system can help users avoid security- and privacy-invasive applications. We now assess the significance of our findings and several recommendations for improving the usability of permissions.

7.1 Effectiveness of Permissions

Our studies demonstrated that the majority of Android users do not pay attention to permissions or understand permission warnings. Nearly half of the laboratory study users were completely unaware that permission warnings are displayed in the Market. Since attention and comprehension are prerequisites for informed security decisions, our study indicates that the current Android permission system does not help most users make good security decisions.

However, we also find that permissions are effective at conveying security information to a minority of users. 24% of the laboratory study participants were aware of permissions and demonstrated a reasonable degree of understanding. It is possible that this is sufficient; a small fraction of expert users could write negative reviews when they encounter troubling permission requests, thereby protecting other consumers. Researchers have found that negative product reviews can influence product sales in other contexts [37, 46], and 24% of laboratory study participants (all of whom were non-expert users) said that they had relied on user reviews or news reports to provide them with information about permissions.

7.2 Recommendations

Our studies identified several factors that contribute to the low attention and comprehension rates. We now present a set of design recommendations aimed at addressing these problems.

Categories. We find that category headings widely confused users. As Figure 1 shows, the final installation page uses a multi-layer user interface to convey permissions. The large category headings are short, simple, and non-technical; below them, the smaller text includes more information about the specific permissions. Multi-layer user interfaces are intended to simultaneously satisfy novice, average, and expert users by providing subsequently more information at each layer of the user interface [38, 27]. However, the category headings are currently so broad that they cause users to overestimate the scope and risk of the requested permissions. Overestimation undermines the warning system because it causes users to believe that they are granting dangerous permissions to more applications than they are. This likely has a negative impact on the amount of attention that users pay to permissions; there is little reason to read individual permission warnings if one believes that all applications receive dangerous privileges.

We recommend re-organizing and re-naming categories to shape user expectations more appropriately. In particular, the "Personal Information" and "Phone Calls" categories misled many of the users in our studies. Although the category headings need to be redesigned, we do not recommend removing them; the categories reduce warning fatigue by decreasing the number of warnings that are shown on the screen. (E.g., a user sees only three warnings for eight permissions if the eight permissions fall into three categories.)

Risks, Not Resources. We find that many users cannot connect permission warnings to risks, even if they understand all of the technical terms in a permission warning. Currently, most of the warnings are resource-centric and value-neutral (e.g., "full Internet access" and "read phone state and identity"). Users are left to decide on their own how the resources might be used, which causes them to underestimate or overestimate the risks of permissions. It is important for warnings to clearly convey specific risks [44]. We cannot expect non-expert users to understand the relationship between resources and risks, and users cannot provide informed consent if they do not realize the risks. The long explanation dialog specifies the risks for a few permissions, but the majority lack risk information; also, we did not observe any users reading the long dialogs. We recommend that permission warnings focus wholly on risks (i.e., potential negative outcomes) instead of resources. For example, "full Internet access" could be replaced with "use your data plan." To balance the risks with benefits, developers could be given space in the UI to justify why they need the permissions.

Low-Risk Warnings. We observed evidence of users experiencing warning fatigue. Warning fatigue is exacerbated by unnecessary warnings. To avoid devaluing the warnings, we recommend that permissions without clear risks should not be shown to users. For example, the ability to connect to a Bluetooth device is unlikely to cause a user harm. Warnings that do not convey real risks teach the user that all warnings are unimportant [40, 11], and there are limits on how much information people can process when making decisions [6, 19]. Currently, some permissions are not displayed to users unless they choose to "See more" because the permissions are considered non-dangerous; we recommend that more permissions should be classified as non-dangerous (and hidden by default).

Absent Permissions. Our SMS comprehension study demonstrated that people cannot reason about the absence of permissions. A user cannot say with certainty that a permission does *not* encompass a privilege unless the user knows that another permission exists to address that privilege or no permission permits the action. Consequently, users overestimate the scope and risk of the permissions that are present. Currently, it is infeasible for any user to remember all of the permissions, given that Android has more than 100 permissions. We recommend coalescing or paring down the list of permission warnings to a set that is small enough for users to look up and remember with accuracy.

Optional Permissions. Several researchers have suggested that users should be able to grant or deny an application's permissions individually, rather than as a bundle [31, 32]. This would give users finer-grained control over the resources that applications have access to. We do not recommend adopting this proposal until user understanding of permissions can be improved with other measures. The low comprehension rates suggest that users cannot currently make informed decisions about individual permissions. Even the users that displayed comprehension competency during the laboratory study did not receive perfect comprehension scores. As such, individual permission granting would add complexity to the user interface without increasing user control.

7.3 Open Problems

Larger changes are needed to improve the relevance of permission warnings and reach users who are currently unaware of permission warnings. We present a set of open problems and future research directions that are motivated by our studies.

Reviews. We identified a small minority of "expert" users who could potentially protect others by sharing their concerns about permissions. One direction is to re-think how a system could support the sharing of privacy and security concerns. How can we incentivize writing reviews about permissions? How can we help interested users determine what applications are doing with permissions so that they can write useful reviews? How can other readers confirm claims about privacy and security? Currently, Android does not provide any way to audit an application's permission usage, although researchers have developed tools for computer scientists [12, 15, 20]. However, users with interests in privacy and security are not necessarily computer scientists, despite some familiarity with smartphone technology; none of our "expert" users had any formal technical education, and we do not expect that they would be able to use any of the existing research tools.

Customization. We hypothesize that different users have different types of privacy and security concerns. For example, a mother told us that she worried a lot about people knowing her daughter's location via their shared phone, whereas another user said he was concerned only about whether applications will excessively drain his phone's battery. When users read permissions aloud to us for the comprehension study, they often told us (without prompting) that they did not care about certain permissions. Warnings will likely be more effective if they are relevant to users' specific concerns about applications. The challenge is to identify users' concerns without expecting all users to fill out surveys or provide feedback. It might be possible to learn which warnings are likely to be relevant to particular users, classes of users, or users generally.

Timing. Android shows users permission information during installation instead of when they are using the application. This design decision was made because "over-prompting the user causes the user to start saying 'OK' to any dialog that is shown" [4]. Indeed, many studies have shown that users click through security dialogs that are presented when the user is trying to perform a task with an application [30, 40, 36]. However, we find that the install-time permission dialog is similarly dismissed by most users. Additionally, install-time permissions lack context; unlike dialogs shown at runtime, there is no way to know what application functionality the install-time permissions correspond to. This suggests that completely new solutions that avoid dialogs, such as sensor-access widgets [21] or access-control gadgets [34], may be needed.

8. CONCLUSION

This paper represents a first step in understanding the effectiveness of Android permissions. Our two studies indicate that Android permissions fail to inform the majority of users, but permissions are not wholly ineffective despite researchers' predictions [17, 14]. A minority of users demonstrated awareness and understanding of permissions, and we found that permissions helped some users avoid privacy-invasive applications. This motivates continued effort towards the goal of usable permissions. However, low rates of user attention and comprehension indicate that significant work is needed to make the Android permission system widely accessible.

We identified a set of issues that are impeding awareness and comprehension. In particular, category headings are confusing, some users cannot connect resource-based warnings to risks, some users cannot reason about the absence of permissions, and some users are experiencing warning fatigue. We provide a set of recommendations to address these issues. Our results also support three directions of future work for improving permission systems: connecting reviews to permissions, customizing warnings to users' concerns, and investigating new types of warning dialogs.

Acknowledgments

We thank Angie Abbatecola for her help with survey and study logistics, and Jennifer King for her insightful comments and discussion. This material is based upon work supported by Facebook and National Science Foundation Graduate Research Fellowships. Any opinions, findings, conclusions, or recommendations expressed here are those of the authors and do not necessarily reflect the views of Facebook or the National Science Foundation. This work is also partially supported by National Science Foundation grant CCF-0424422, a gift from Google, and the Intel Science and Technology Center for Secure Computing.

9. REFERENCES

[1] How Consumers Interact with Mobile App Advertising. Harris Interactive Survey, December 2011.

[2] M. Ackerman, L. Cranor, and J. Reagle. Privacy in e-commerce: examining user scenarios and privacy preferences. In *ACM Conference on Electronic Commerce*, 1999.

[3] AdMob. AdMob Mobile Metrics Report, 2010.

[4] Android Open Source Project. Android Security Overview, 2012.

[5] L. Barkhuus and A. Dey. Location-based services for mobile telephony: a study of users' privacy concerns. In *International Conference on Human-Computer Interaction*, 2003.

[6] J. R. Bettman. *An Information Processing Theory of Consumer Choice*. Addison-Wesley Publishing Company, 1979.

[7] N. J. Blunch. Position Bias in Multiple-Choice Questions. *Journal of Marketing Research*, 1984.

[8] T. Buchanan, C. Paine, A. N. Joinson, and U.-D. Reips. Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology*, 2007.

[9] 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 *ACM CHI Conference on Human Factors in Computing Systems*, 2005.

[10] L. F. Cranor. A Framework for Reasoning about the Human in the Loop. In *Conference on Usability, Psychology, and Security*. USENIX Association, 2008.

[11] S. Egelman, L. F. Cranor, and J. Hong. You've Been Warned: An empirical study of the effectiveness of web browser phishing warnings. In *ACM CHI Conference on Human Factors in Computing Systems*, 2008.

[12] W. Enck, P. Gilbert, B.-G. Chun, L. P. Cox, J. Jung, P. McDaniel, and A. N. Sheth. TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones. In *Symposium on Operating Systems Design and Implementation (OSDI)*, 2010.

[13] W. Enck, D. Octeau, P. McDaniel, and S. Chaudhuri. A study of Android application security. In *USENIX Security*, 2011.

[14] W. Enck, M. Ongtang, and P. McDaniel. On lightweight mobile phone application certification. In *ACM Conference on Computer and Communication Security (CCS)*, 2009.

[15] A. P. Felt, E. Chin, S. Hanna, D. Song, and D. Wagner. Android Permissions Demystified. In *ACM Conference on Computer and Communication Security (CCS)*, 2011.

[16] A. P. Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner. A Survey of Mobile Malware in the Wild. In *ACM Workshop on Security and Privacy in Mobile Devices (SPSM)*, 2011.

[17] A. P. Felt, K. Greenwood, and D. Wagner. The Effectiveness of Application Permissions. In *USENIX Conference on Web Application Development (WebApps)*, 2011.

[18] A. Fuchs, A. Chaudhuri, and J. Foster. SCanDroid: Automated Security Certification of Android Applications. Technical report, University of Maryland, 2009.

[19] G. J. Gaeth and J. Shanteau. Reducing the Influence of Irrelevant Information on Experienced Decision Makers. *Organizational Behavior and Human Performance*, 33, 1984.

[20] P. Hornyack, S. Han, J. Jung, S. Schechter, and D. Wetherall. These Aren't the Droids You're Looking For: Retrofitting Android to Protect Data From Imperious Applications. In *ACM Conference on Computer and Communication Security*, 2011.

[21] J. Howell and S. Schechter. What you see is what they get. In *IEEE Workshop on Web 2.0 Security and Privacy*, 2010.

[22] C. Jensen, C. Potts, and C. Jensen. Privacy practices of Internet users: Self-reports versus observed behavior. In *International Journal of Human-Computer Studies*, 2005.

[23] P. Kelley, M. Benisch, L. Cranor, and N. Sadeh. When are users comfortable sharing locations with advertisers? In *ACM CHI Conference on Human Factors in Computing Systems*, 2011.

[24] P. G. Kelley, S. Consolvo, L. F. Cranor, J. Jung, N. Sadeh, and D. Wetherall. A Conundrum of Permissions: Installng Applications on an Android Smartphone. In *Workshop on Usable Security (USEC)*, 2012.

[25] J. King, A. Lampinen, and A. Smolen. Privacy: Is There An App for That? In *Symposium on Usable Privacy and Security (SOUPS)*, 2011.

[26] P. Kumaraguru and L. F. Cranor. Privacy Indexes: A Survey of Westin's Studies. Technical report, Carnegie Mellon University CMU-ISRI-5-138, 2015.

[27] R. Leung, L. Findlater, J. McGrenere, P. Graf, and J. Yang. Multi-Layered Interfaces to Improve Older Adults' Initial Learnability of Mobile Applications. *ACM Transactions on Accessible Computing (TACCESS)*, 2010.

[28] J. Lindqvist, J. Cranshaw, J. Wiese, J. Hong, and J. Zimmerman. I'm the mayor of my house: examining why people use Foursquare - a social-driven location sharing application. In *ACM CHI Conference on Human Factors in Computing Systems*, 2011.

[29] W. A. Magat, W. K. Viscusi, and J. Huber. Consumer Processing of Hazard Warning Information. *Journal of Risk and Uncertainty*, 1, 1988.

[30] S. Motiee, K. Hawkey, and K. Beznosov. Do windows users follow the principle of least privilege?: investigating user account control practices. In *Symposium on Usable Privacy and Security (SOUPS)*, 2010.

[31] K. Mueller and K. Butler. Flex-P: Flexible Android Permissions. IEEE Symposium on Security and Privacy, Poster Session, 2011.

[32] M. Nauman, S. Khan, M. Alam, and X. Zhang. Apex: Extending Android Permission Model and Enforcement with User-defined Runtime Constraints. In *ACM Symposium on Information, Computer and Communications Security (ASIACCS)*, 2010.

[33] P. Nickinson. Android Market now has more than a quarter-million applications, 2011.

[34] F. Roesner, T. Kohno, A. Moshchuk, B. Parno, H. Wang, and C. Cowan. User-Driven Access Control: Rethinking Permission Granting in Modern Operating Systems. Technical report, Microsoft Research MSR-TR-2011-91, 2011.

[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*, 2009.

[36] S. E. Schechter, R. Dhamija, A. Ozment, and I. Fischer. The Emperor's New Security Indicators. In *IEEE Symposium on Security and Privacy*, 2007.

[37] S. Sen and D. Lerman. Why are you telling me this? An

examination into negative consumer reviews on the web. *Journal of Interactive Marketing*, 21, 2007.

[38] B. Shneiderman. Promoting universal usability with multi-layer interface design. In *Conference on Universal Usability (CUU)*, 2003.

[39] J. Sunshine, S. Egelman, H. Almuhimedi, N. Atri, and L. F. Cranor. Crying Wolf: An Empirical Study of SSL Warning Effectiveness. In *USENIX Security Symposium*, 2009.

[40] J. Sunshine, S. Egelman, H. Almuhimedi, N. Atri, and L. F. Cranor. Crying Wolf: An Empirical Study of SSL Warning Effectiveness. In *USENIX Security Symposium*, 2009.

[41] H. Taylor. Most People are "Privacy Pragmatists" Who, While Concerned about Privacy, Will Sometimes Trade It Off for Other Benefits. Harris Interactive, March 2003.

[42] S. Thurm and Y. I. Kane. Your apps are watching you, 2010.

[43] M. S. Wogalter. Communication-Human Information Processing (C-HIP) Model. In *Handbook of Warnings*. Lawrence Erlbaum Associates, 2006.

[44] M. S. Wogalter. Purpose and scope of warnings. In *Handbook of Warnings*. Lawrence Erlbaum Associates, 2006.

[45] 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 *Network and Distributed System Security Symposium (NDSS)*, 2012.

[46] F. Zhu and X. Zhang. Impact of Online Consumer Reviews on Sales: The Moderating Role of Product and Consumer Characteristics. *Journal of Marketing*, 74, 2010.