# I've Got 99 Problems, But Vibration Ain't One: A Survey of Smartphone Users' Concerns

Adrienne Porter Felt, Serge Egelman, and David Wagner
University of California, Berkeley
{apf, egelman, daw}@cs.berkeley.edu

## ABSTRACT

Smartphone operating systems warn users when third-party applications try to access sensitive functions or data. However, all of the major smartphone platforms warn users about *different* application actions. To our knowledge, their selection of warnings was not grounded in user research; past research on mobile privacy has focused exclusively on the risks pertained to sharing location. To expand the scope of smartphone security and privacy research, we surveyed 3,115 smartphone users about 99 risks associated with 54 smartphone privileges. We asked participants to rate how upset they would be if given risks occurred and used this data to rank risks by levels of user concern. We then asked 41 smartphone users to discuss the risks in their own words; their responses confirmed that people find the lowest-ranked risks merely annoying but might seek legal or financial retribution for the highest-ranked risks. In order to determine the relative frequency of risks, we also surveyed the 3,115 users about experiences with "misbehaving" applications. Our ranking and frequency data can be used to guide the selection of warnings on smartphone platforms.

## Categories and Subject Descriptors

D.4.6 [**Operating Systems**]: Security and Protection

## General Terms

Human Factors, Security

## Keywords

Smartphones, risks, warnings

## 1. INTRODUCTION

Smartphone operating systems like Android, iOS, and Windows Phone expose rich APIs to third-party applications. These APIs allow applications to use hardware (e.g., vibrator and camera), change phone settings, and read data (e.g., text messages and contacts). Unfortunately, malicious and unscrupulous application authors have taken advantage of these resources, to the displeasure of users [9, 11, 18]. Smartphone operating systems use permissions to help protect users from these threats; users see permissions as warnings during installation or at runtime.

The three major smartphone operating systems warn users about different resources: Android 4.0 has 165 permissions, Windows Phone 7 has 16 permissions, and iOS 5 has 2 permissions. Their selection of permissions was not grounded in user research as far as we are aware, and usability problems have emerged as a result. Android users struggle to understand permission warnings, in part because the multitude of permissions is difficult to process and recall [10]. iPhone users were widely outraged when when they discovered that applications can access certain resources without seeing permission warnings [4]. These experiences suggest that existing platforms are not asking users about the right resources.

In order to guide the future selection and design of smartphone warnings, we performed two surveys to rank the level of user concern about a wide range of smartphone resources. In our first survey, we asked 3,115 smartphone users to rate their level of concern about 99 risks corresponding to 54 smartphone permissions. From this, we generated a ranking of risks based on user concerns (Appendix A provides the full ranking). We also asked users about past negative experiences with applications to measure the frequency of risks. In our second survey, we asked 42 smartphone users to state their reactions to low-ranked, medium-ranked, and high-ranked risks. The open-ended responses validate the ranking: participants viewed low-ranked risks as manageable annoyances, whereas they viewed high-ranked risks as severe offenses that may require the help of authorities.

We find that warnings in current smartphone platforms do not correspond to users' concerns. Future permission systems should consider user concerns when deciding which privileges are protected with warnings. Despite the large academic focus on location sharing, we find that improper location sharing is only a mid-ranked risk: users are more concerned about many other permissions. As such, mobile privacy research should be refocused to consider other resources and privileges beyond location.

**Contributions.** We contribute the following:

- We created a ranking of the risks of 54 smartphone application permissions based on user concerns that we collected with two surveys.
- We surveyed users about the risks that they have actually encountered.


*SPSM'12,* October 19, 2012, Raleigh, North Carolina, USA.

## 2. RELATED WORK

Mobile privacy research has traditionally focused on location tracking and sharing. Numerous studies have examined users' privacy concerns about sharing mobile location data. Lederer et al. found that the identity of the location requester matters more than the place in a user's willingness to share his or her location [15], and Anthony et al. focused on the effect of the specific place [1]. Consolvo et al. studied the effect of the person requesting the location on willingness to share [7], Wiese et al. examined social groups [19], and Kelley et al. considered attitudes about sharing location with advertisers [14]. Iachello et al. described how to build appropriate privacy controls into a social location-sharing application [13]. Barkhuus et al. found that people like location services if they are useful [3], and people tend to stop worrying about location-based services after using them for a while [2]. This prior literature thoroughly documents users' privacy concerns about sharing location data.

However, smartphone operating systems provide applications with the ability to access a number of resources beyond location data. Smartphone APIs let applications read many types of data (e.g., photographs) and make changes to the phone (e.g., delete data). Few studies have explored the space of smartphone privacy and security beyond location. Roesner et al. [17] studied smartphone users' privacy and security expectations for copy-and-paste, photography, and text messaging in addition to location. Muslukhov et al. [16] asked a number of smartphone users about the value and sensitivity of eleven types of data on their phones. We previously explored user attitudes towards Internet, location, audio, contacts, and photo permissions with two controlled economic experiments, but the experiments could not be extended to the full set of possible permissions [8]. We aim to further expand the scope of research on users' smartphone concerns by studying users' opinions about 99 risks associated with 54 smartphone permissions.

## 3. METHODOLOGY

We asked 3,115 smartphone users to rate how upset they would be if an application performed certain actions on their phones without user approval. As part of that survey, respondents also provided information about negative experiences with applications. We then performed a follow-up survey where 42 respondents provided open-ended explanations of their feelings about applications performing undesirable actions, which contextualizes the ratings.

### 3.1 Rating Survey

The purpose of the large-scale rating survey was to create an index that ranks the risks of allowing applications to access smartphone resources by degree of user concern. This index was meant to be a relative measure for comparing risks against each other, and not an absolute measure of user concern. We also collected information from survey participants about the causes of dissatisfaction with applications.

#### 3.1.1 Instrument Design and Validation

Our instrument was designed to elicit user concerns about different resources. We faced two design constraints. First, we aimed to measure opinions about risks rather than application features. (For example, a user might view an application that deletes files as useful or harmful depending on whether the deletion was intentional.) Second, we did not want to scare participants by mentioning malware or viruses. We suspected that participants would report high levels of concern for *any* action that they were told is associated with malware. As such, we needed to ensure that respondents were aware that we were asking about undesirable actions, without mentioning how or why those actions were initiated (e.g., by malware).

We performed two preliminary surveys that asked respondents about situations in which applications performed an action "without my knowledge" or "when you believed [the app] had no reason to do so." The results of these surveys were inconsistent. Subsequent interviews revealed that participants were unsure whether the listed actions were negative side-effects or positive features. We conducted one-on-one interviews and a focus group with Craigslist-recruited smartphone users to generate new wording.

We validated our final instrument by asking four smartphone users to take the survey and speak with an interviewer. These participants were selected from applicants on Craigslist to represent a diverse cross-section of smartphone users. We found that the respondents understood that the questions asked about risks rather than features, and they used the full range of the scale. When asked to describe how the scenarios in the questions could occur, all four participants listed both buggy and compromised applications. Some participants also mentioned viruses, bad UI design, or aggressive marketing. This indicated that all four participants had a firm grasp of the meaning of the questions without specifically focusing on malware.

#### 3.1.2 Instrument

The survey began by asking respondents to think about negative side-effects of applications. First, we asked participants to answer a free-response question: "If you have ever un-installed apps because they misbehaved, please tell us what the apps did that you didn't like." Next, we prepared respondents for the risk-based questions:

> *Every once in a while, an app might do something on your phone without asking you first. Depending on what the app does to your phone, your feelings could range from indifference (you don't care) to being very upset.*

We then asked participants about various risks:

> *How would you feel if an app [insert risk], without asking you first?*

For example: "How would you feel if an app added new contacts, without asking you first?" Respondents answered using a horizontal five-point scale that ranged from "Indifferent" to "Very upset," with unlabeled intermediate points.

Each survey participant saw 12 questions on one page, selected at random from a set of 99 potential questions. Appendix A shows the risks that participants were asked about. We compiled the set of questions by assigning risks to Android, Windows Phone 7, and iOS permissions. The three platforms define a total of 191 permissions, but we grouped equivalent permissions (e.g., "power device on or off" and "force device reboot") and discarded irrelevant permissions (e.g., "enable application debugging") to arrive at 54 permissions. We then assigned risks to the actions using documentation and domain expertise. Some actions are associated

with multiple risks, and we assigned at least four risks to each type of smartphone data:[1] "publicly shared your [data type]," "shared your [data type] with your friends," "shared your [data type] with advertisers," "sent copies of [data type] to their servers (but didn't share them with anyone else)."

On the last page of the survey, we collected demographic information about participants and their cell phones.

#### 3.1.3 Deployment and Demographics

We deployed the survey on Mechanical Turk for 13 days. Participants were paid $1 each for completing the survey, and we limited the survey to respondents in the United States. We filtered responses for validity based on users' survey completion time, responses to short open-ended questions, and the self-reported type of phone.[2] After filtering, we obtained 3,115 valid responses from smartphone users.

Participants' ages ranged from 18 to 80 ($\mu$=29.7), while 47.9% were female and 51.9% were male. Although the population was younger than the U.S. population overall (65% of respondents were below the age of 30), it was only slightly younger than U.S. smartphone user demographics [6]. Participants reported many occupations: healthcare workers, software engineers, financial advisors, federal government employees, graphic designers, etc. However, the predominant occupations were students, stay-at-home parents, and the unemployed. Self-reported completed levels of education ranged from some high school to doctorates.

Participants reported owning the following smartphones: 49.5% Android phones, 39.7% iPhones, 7.7% Blackberries, and 1.7% Windows phones. The remainder stated that they owned Palm, Symbian, or multiple phones. There was no incentive to lie about phone ownership because we paid participants regardless of whether they owned smartphones.

### 3.2 Open-Ended Survey

The purpose of the open-ended survey was to associate participants' own words with the large-scale survey ratings.

#### 3.2.1 Instrument

The open-ended survey asked participants the following short essay questions about risks:

1. How would you feel if an app [insert risk], without asking you first?
2. Why would you feel that way?
3. What would you do if this happened?

Each participant was asked about three of nine risks, which we selected based on the results of the large-scale study. We chose the three lowest-ranked risks, three mid-ranked risks, and three of the highest-ranked risks:

- *Lowest-ranked risks:*
  - vibrated your phone
  - connected to a Bluetooth device (like a headset)
  - turned your flash on
- *Mid-ranked risks:*
  - added new contacts
  - took screenshots when you're using other apps
  - un-muted a phone call
- *Highest-ranked risks:*
  - deleted all of your contacts
  - sent premium text messages from your phone (they cost money)
  - made phone calls to 1-900 numbers (they cost money)

We showed each respondent one of the lowest-ranked risks, one of the mid-ranked risks, and one of the highest-ranked risks. We displayed one page for each risk, and participants could not move backwards in the survey. The last page of the survey collected demographic data.

#### 3.2.2 Deployment and Demographics

We deployed the survey on Mechanical Turk for two days. Participants were paid $8 each. The survey was advertised as being worth $3, with an additional $5 reward for complete sentences and correct grammar. We ran the survey until we had 42 valid responses (with a target of 40) from people in the United States. The participants were evenly split by gender, with an average age of 30.3. All of the respondents said that they have used smartphone applications, with an average of 29 applications installed on their phones.

## 4. RANKING RESULTS

We used the results of the large-scale survey to rank the severity of the risks (Section 4.1). The open-ended survey provides supplementary qualitative data to add context to the large-scale survey results (Section 4.2). We then discuss how these results can be interpreted (Sections 4.3 and 4.4).

### 4.1 Large-Scale Survey

Our goal is to rank the severity of potential risks. We obtained an average of 376.7 ratings per risk.

**Ranking Metric.** In our large-scale survey, respondents rated how upset they would be if certain risks occurred, using a five-point scale. Our resulting metric for the severity of a risk is the percentage of respondents who indicated that they would be "very upset" if the given risk occurred. We refer to this metric as the *VUR rate* (the "very upset" respondent rate). We consider the percentage of "very upset" respondents instead of medians because the responses were not normally distributed. Despite this, ordering the risks by medians returns a very similar ranking. The VUR rate is a metric for comparing risks against each other, rather than an absolute measure of user concern.

The confidence interval for a given risk's VUR rate depends on the specific question's sample size and how close the VUR rate is to 50%. The tightest confidence interval for a VUR rate is $\pm$1.4% at a 95% confidence level, and the widest confidence interval for a VUR rate is $\pm$5.0% at a 95% confidence level. This indicates that differences between risks with similar VUR rates may not be meaningful, but risks with VUR rates that differ by more than 5% are likely ranked correctly relative to each other.

**Ranking Characteristics.** The highest-ranked risk is "permanently disabled (broke) your phone," with a 98.2% VUR rate. The lowest-ranked risk is "vibrated your phone," with a 15.6% VUR rate. Table 1 shows the ten highest-ranked and ten lowest-ranked risks, and Appendix A provides the VUR rates for all of the 99 risks in our survey.

[1]Due to a survey programming error, we accidentally omitted one of these risks for three types of data.

[2]We discarded responses with implausibly short times or nonsense answers for the open-ended questions. We also discarded responses if the participant's self-reported phone model was not a smartphone.

| Risk | VUR Rate |
|---|---|
| permanently disabled (broke) your phone | 98.21% |
| made phone calls to 1-900 numbers (they cost money) | 97.41% |
| sent premium text messages from your phone (they cost money) | 96.39% |
| deleted all of your contacts | 95.89% |
| used your phone's radio to read your credit card in your wallet | 95.15% |
| publicly shared your text messages | 94.48% |
| deleted all of the information, apps, and settings on your phone | 94.39% |
| publicly shared your e-mails | 93.37% |
| deleted all of your other apps | 93.14% |
| shared your text messages with your friends | 92.49% |
| ... | ... |
| inserted extra letters into what you're typing | 45.48% |
| read files that belong to other apps | 44.33% |
| sent your phone's unique ID to their servers (but didn't share it with anyone else) | 42.16% |
| added new browser bookmarks | 39.22% |
| sent the list of apps you have installed to their servers (but didn't share it with anyone else) | 34.92% |
| turned the sound on your phone down really low | 36.96% |
| sent your location to their servers (but didn't share it with anyone else) | 29.88% |
| turned your flash on | 29.67% |
| connected to a Bluetooth device (like a headset) | 27.47% |
| vibrated your phone | 15.62% |

**Table 1: The highest- and lowest-ranked risks.**

Risks that involved permanent data loss or financial loss (e.g., sending premium text messages or spying on credit card numbers) evinced the highest levels of concern. The lowest-ranked risks pertain to phone settings or sending data to servers. Unlike the highest-ranked risks, many of the lowest-ranked risks are revertible: settings can be reset, unwanted browser bookmarks can be removed, the phone's vibrator can be turned off, etc.

**Data Sharing.** Respondents' concerns about data sharing depend on who the data is being shared with. We surveyed respondents about four types of data sharing: public sharing, sharing with friends, sharing with advertisers, and removing the data from the phone without sharing it with another party. Figure 1 shows these results for the eleven data types. For all of the data types, publicly sharing the data is approximately twenty percentage points more concerning than sending the data to a server. Sharing with friends and advertisers rank in the middle, between public sharing and sending the data to a server. Notably, illicit location sharing has the lowest or second-lowest VUR rates of the eleven smartphone data types in our survey.

**Diversity of Opinion.** We observed different amounts of diversity of opinion between risks. Eighteen risks had a standard deviation greater than 1, whereas six had a standard deviation less than .37. In general, the risks with high VUR rates have low standard deviations, whereas the risks with low VUR rates have larger standard deviations. One interpretation is that there is user consensus about what *is* very upsetting, but not about what is *not* very upsetting. It may also be an artifact of our five-point scale: some users might have selected something stronger than "very upset" if such an option were available, which would have resulted in greater variance among high-ranked risks.

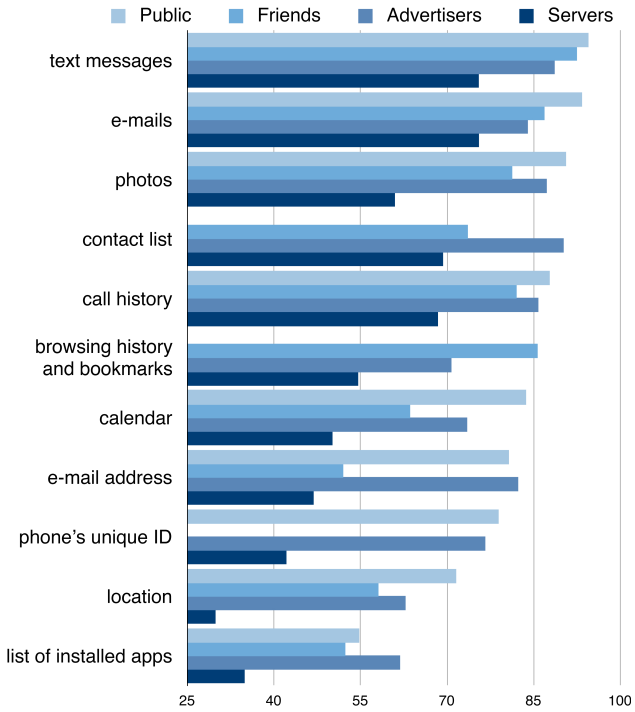


**Figure 1: The VUR rates for 11 data types. We asked participants to rate how upset they would be if applications shared their data: "publicly," "with your friends," "with advertisers," and "sent ... to their servers (but didn't share it with anyone else)."**

**Demographics.** Individual respondents' scores are not directly comparable to each other because they received different questions, but we can compare groups of respondents. People above the age of 50 rank risks higher than people below the age of 30 do ($\mu_{<30} = 4.46, \mu_{>50} = 4.67$; $p < 0.0005$, $z = 5.943$, Wilcoxon-Mann-Whitney test), with a medium effect size ($d = 0.51$). We do not find a significant difference between the types of phones that participants owned ($\chi^2 = 4.487$, $p = 0.6110$, Kruskal-Wallis test).

Women rank risks higher than men do ($\mu_M = 4.47, \mu_W = 4.55$; $p < 0.0005$, $z = -4.269$, Wilcoxon-Mann-Whitney test), although the effect size is very small ($d = 0.18$). We hypothesized that men might be more concerned about sharing their browsing history with friends, and women might be more concerned about sharing their location publicly or with friends. However, gender did not have a significant effect on sharing browsing history with friends ($p = 0.9688$, $z = 0.039$, Wilcoxon-Mann-Whitney test), sharing location publicly ($p = 0.0215$, $z = 2.300$, Wilcoxon-Mann-Whitney test), or sharing location with friends ($p = 0.2537$, $z = 1.142$, Wilcoxon-Mann-Whitney test).

## 4.2 Open-Ended Responses

The VUR rate is a relative metric that allows us to compare risks against each other. However, the metric does not provide us with any context for how users interpret "very upset." Our open-ended survey assigns user-supplied meaning to the metric. It also serves as a second measure to evaluate whether there are differences in users' concerns across risks.

| | Low-Ranked Risks | | | | Mid-Ranked Risks | | | | High-Ranked Risks | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **Avg** | vibrate | Blue-tooth | flash | **Avg** | added contacts | screen-shots | un-muted | **Avg** | deleted contacts | $ SMS | $ calls |
| nothing | **21%** | 29% | 20% | 15% | **12%** | 18% | 0% | 15% | **5%** | 0% | 5% | 10% |
| tinker with app | **33%** | 50% | 27% | 23% | **12%** | 6% | 33% | 0% | **0%** | 0% | 0% | 0% |
| uninstall the app | **62%** | 42% | 73% | 69% | **74%** | 71% | 67% | 85% | **76%** | 67% | 80% | 80% |
| contact developer | **12%** | 7% | 7% | 23% | **17%** | 18% | 8% | 23% | **40%** | 25% | 45% | 5% |
| write a review | **5%** | 0% | 7% | 8% | **14%** | 12% | 8% | 23% | **21%** | 25% | 20% | 20% |
| contact press | **5%** | 0% | 13% | 0% | **5%** | 6% | 0% | 8% | **5%** | 0% | 10% | 0% |
| call service provider | **0%** | 0% | 0% | 0% | **2%** | 0% | 8% | 0% | **17%** | 17% | 15% | 20% |
| replace/wipe phone | **0%** | 0% | 0% | 0% | **5%** | 0% | 8% | 0% | **5%** | 8% | 0% | 10% |
| contact authorities | **0%** | 0% | 0% | 0% | **2%** | 6% | 8% | 0% | **19%** | 25% | 15% | 20% |
| pursue legal action | **0%** | 0% | 0% | 0% | **0%** | 0% | 0% | 0% | **12%** | 17% | 5% | 20% |

**Table 2: Forty-two survey respondents told us how they would react if certain risks occurred. We categorized their responses; some responses fall into multiple categories.**

We asked participants what they would do if certain risks occurred. Table 2 displays the frequency with which participants mentioned certain reactions. Respondents' stated reactions fell into the following categories:

- **Nothing.** Some participants stated that they would ignore the risk or simply reverse the undesirable action.
- **Tinker.** Participants said that they would try to change the application's settings or determine what UI element was causing the undesirable behavior. This was often the first of multiple proposed steps. For example,

  > *I would first try to change the settings so that it doesn't connect. If I can't find the settings to turn such a feature off, I would immediately delete the app.*

- **Uninstallation.** The most common recourse was to uninstall the application.
- **Contact the developer.** Many people said that they would try to contact the developer of the application to complain or request a refund.
- **Reviews.** Some participants said that they would try to make others aware of the application's problems by writing negative reviews. For example,

  > *...for the first time ever, I would probably review [the] app. I would type (probably even in all caps!) about what it does.*

- **Contact the press.** Participants sometimes said that they would warn other users by contacting blogs or "watchdog news groups."
- **Contact the phone company.** Several participants said that they would contact their service provider to reverse charges or restore data. Surprisingly, many participants in this category said that they would blame their service providers for negative application behavior. For example, one respondent wrote,

  > *If this happened I would consult my service provider to try and retrieve my contacts, and probably cancel my service.*

- **Replace or wipe the phone.** Although none of the risks in the survey were permanent side-effects, some participants said that they would get a new phone or wipe their existing phone so that it would be like having a new phone. One participant wrote,

  > *[If] this happened and I could not turn off this feature in the settings, then I would not continue using the phone and I would try to either get a refund or to sell it.*

- **Contact authorities.** Some participants said that they would notify authorities about the application's misbehavior so that the application would be punished or removed from the store. For example,

  > *I would call up the FBI or other organizations to look into how my information might have been mishandled.*

- **Legal action.** In some cases, participants wrote that they would seek legal action against the application developer. For example,

  > *...I may seek legal counsel to solve the issue and perhaps receive compensation for the inconvenience and trouble that the application developer put me through.*

As Table 2 shows, participants' reactions increased in severity from the lowest-ranked risks to the highest-ranked risks. Participants' responses to risks with similar rankings are fairly similar. This supports the validity of the ranking from the large-scale rating survey. For low-ranked risks, participants would attempt to resolve the situation themselves or complain. Responses to mid-range risks contain a greater emphasis on complaining in reviews or to the developer. For high-ranked risks, many participants would seek help from external parties like service providers, police, or lawyers.

## 4.3 Limitations

The ratings and open-ended questions are not absolute measures of user concern because our surveys explicitly asked respondents about privacy and security. Surveys that directly ask questions about privacy suffer from inflated user concerns about privacy [5] and therefore are not reliable measures of absolute levels of concern. We expect this applies to our study as well. We intentionally primed respondents to think about the negative side-effects of applications because we did not want users to mix risks and features. Instead, our surveys provide a basis for comparing risks against each other. The same set of priming biases are applied equally to all of the risks presented in the surveys, so this effect should not influence our ranking.

We do not claim to predict how users will act when confronted with actual problems on their phones because our study relies on self-reported data. As with the priming bias, we do not believe that self-reporting affects the validity of our ranking because this bias is equally present for all risks.

We also do not claim to predict how likely a user is to grant a given permission. Our survey reflects participants' stated levels of concern about each potential outcome, which is only one factor among several that might influence a user's decision to grant permissions. Users are likely to weigh their concerns about risks against their trust of a given application developer, their need for the application, etc.

We relied on Mechanical Turk workers for survey data. As discussed in Section 3.1.3, the workers who completed our study did not proportionately represent the smartphone population in terms of occupation. Our survey did not reach many highly-paid professionals, who may have different concerns. However, our survey was taken by a large number of participants with varying ages and socio-economic statuses. Secondary studies may be needed to target specific groups that could plausibly have their own privacy and security concerns, such as doctors (patient data), lawyers (client data), or executives (corporate data).

## 4.4 Discussion

**Data Sharing.** Participants discriminate between publicly sharing data and sharing data with only the application's developers (Figure 1). For some types of data (e.g., contacts, e-mail address), there is a large difference in the VUR rates for sharing with advertisers and other types of sharing. Based on this finding, we suspect that warnings about data access that do not specify where the data is being sent to do not provide users with enough information to gauge the risk of sharing the data with the application. This motivates further work on tools like AppFence [12] that tell users whether data is being sent to advertisers or other known third parties. Alternately, developers could provide annotations that reflect their privacy policies, and this information could be incorporated into warnings or data access requests.

**Location.** Most mobile privacy and security research has focused on location. However, we find that improper location sharing is not viewed as dangerous in comparison to the other risks of using applications. All of the location-related risks rank in the bottom half of risks, and location is the second-lowest data type. Consequently, we believe that the privacy community should refocus their efforts on other types of smartphone data that evoke higher levels of user concern, such as text messages, photos, and contacts.

**Android Warnings.** We can compare our ranking to Android's categorization of permissions. Android divides permissions into three levels of severity. We find that their categorization differs from our survey respondents' concerns in many cases. For example, Android places the `SET_TIME` permission in the highest-severity category, yet it falls in the bottom third in our ranking. As another example, access to photos ranks in the top quartile in our study, yet Android does not restrict access to photos with any permission at all.

**iOS Warnings.** We can also compare our ranking to iOS's selection of warnings. iOS only prompts users for consent for location data and pop-up notifications. However, we find that both rank low in comparison to other privileges; this may indicate that iOS does not ask users about the correct privileges. Although iOS applications cannot perform all of the actions in our ranking, they can perform many of the actions that rank higher than location and notifications without a consent dialog. Given our ranking, iPhone users' complaints about the lack of a consent dialog for contacts [4] is not surprising.

| **Undesirable behavior** | **Number of respondents** |
|---|---|
| Spam | 243 (7.8%) |
| Ads in the notification bar | 30 (1.0%) |
| Other misuses of the notification bar | 46 (1.5%) |
| Drained the battery | 85 (2.7%) |
| Used too much memory | 58 (1.9%) |
| Used too much Internet data | 21 (0.7%) |
| Other negative behaviors | 154 (4.9%) |

**Table 3: The number of respondents who report experiencing each of the undesirable application behaviors. Some participants' responses fall into multiple categories. Percentages are from the $3,115$ total survey respondents.**

**Service Providers.** In our qualitative study, 19% of participants said that they expect their service provider to remedy any data loss or data theft. Several participants stated that they would consider switching service providers if an application severely misbehaved. In practice, service providers do not provide backup services by default, nor do they control what applications are listed in application markets. This suggests that some users may not understand the security or liability implications of installing and using smartphone applications. In contrast, some participants said that they would contact their service providers to refund fraudulent SMS or phone charges; this expectation is likely well-founded for some service providers.

# 5. REASONS FOR UNINSTALLATION

As part of our large-scale survey, we asked participants to tell us about instances in which they had uninstalled "misbehaving" applications. The purpose of this was to measure the prevalence of resource abuses. A permission system designer might want to guard a low-risk resource with a more severe warning if the likelihood of abuse is high.

## 5.1 Results

Of the $3,115$ respondents, $2,427$ respondents provided us with short essays about negative experiences with applications that they had uninstalled. We identified 559 responses (17.9% of the total respondents) that described undesirable behaviors that pertain to abuses of resources. We categorized these behaviors into the following categories (Table 3):

**Spam.** Some participants reported having uninstalled applications because the applications caused their phones to send or receive e-mail, text message, or Facebook spam. In order to send spam, applications read users' contact lists and send messages from their accounts. For example,

> *[the app] used information on my contact list to send over a hundred spam texts and emails.*

Another person wrote that an app:

> *added a contact then sent email from that contact telling my friends I liked the app and they should install it.*

**Ads in notifications.** Under the rules of the Android Market and iOS App Store, applications are not supposed to use notifications to display advertisements. Despite this restriction, some users report having uninstalled applications for this reason. One participant wrote,

> *it always put spam in my notification bar, for example: You have won a $50 ATT giftcard! Claim it now!*

Our categorization (in Table 3) may underestimate the number of people who experienced this; 165 additional participants complained about "pop-up" advertisements, but it was unclear whether they were referring to standard in-application advertisements or abuse of the notification bar.

**Other misuses of the notification bar.** Other applications misused notifications for reasons other than advertisements. For example,

> *The only one I remember in particular was one that kept sending me push notifications even though I almost never used it. I know you can turn push off on an iPhone, but I thought it'd be easier to just delete the app.*

Additionally, a bug in some versions of iOS allows applications to send push notifications even if it has been disabled; some users reported experiencing this, e.g.,

> *Some apps continued to pester me with notifications even though I was more than certain that I had disabled notifications for that app.*

**Resource consumption.** Some participants felt that applications used up too much battery life, memory, or Internet data. For example, one participant uninstalled several applications because the applications

> *racked up extra mb of data [while] they were running in the background without me realizing it.*

**Other negative behaviors.** Participants also reported a number of behaviors that were too vague or infrequent to categorize. Some vague responses included descriptions of "viruses" and "buggy apps." Infrequent reasons included deleting contacts, deleting photographs, recording location, transmitting contacts, and altering contacts.

## 5.2 Limitations

Participants may have failed to list their negative experiences with applications due to forgetfulness or uncertainty over the open-ended question. Additionally, we only collect information on negative experiences that upset participants enough to uninstall the offending applications; users may have simply ignored other negative experiences that are not described here. On the other hand, we can assume that all of the participants' stories are true because there was no incentive to lie. Consequently, the statistics in Table 3 should be viewed as a lower bound: the true rate of negative experiences may be higher.

As discussed in Section 4.3, this survey represents the experiences of Mechanical Turk users, who tend to be young and not high-income. Older and higher-income smartphone users might have different concerns and experiences.

## 5.3 Discussion

Nearly 8% of all participants say that they have uninstalled applications because of spam. Spam is related to several high-VUR risks: sending text messages, spamming contacts with event invitations, sending spam to the user's contact list, and sending spam from the user's e-mail account. Consequently, emphasizing the significance of permissions that are associated with high-VUR risks would simultaneously promote spam prevention.

Fewer participants reported dissatisfaction due to notification abuse or resource consumption. The risks related to notifications and resource consumption are low-VUR risks: notifications rank $83^{rd}$ and draining the battery ranks $75^{th}$. Although these risks might deserve slightly more scrutiny than the other low-VUR risks, our study finds that fewer than 3% of respondents mentioned these risks as causes of uninstallation. However, further research is needed to confirm the true rate of dissatisfaction because our study represents a lower bound.

Among the behaviors that we classified as "other negative behaviors," most correspond to mid- or high-VUR risks. However, none of these behaviors were individually frequent enough to suggest that they might be significant enough to require additional emphasis in a permission system.

# 6. CONCLUSION

We surveyed 3,115 smartphone users on Mechanical Turk about potential risks of smartphone applications. Participants rated how upset they would be if the risks occurred. From this data, we developed a ranking of risks by user concern. A follow-up, open-ended survey of 41 smartphone users found that users view the lowest-ranked risks are annoyances that they can resolve, whereas the highest-ranked risks are serious offenses that may require external parties. Our ranking could be used to guide warning design, and our results show that location is not a high-ranked user concern. We also found that some users hold service providers responsible for abusive applications.

## Research Ethics

We received advance approval from the Institutional Review Board at the University of California, Berkeley to perform this work. Survey data was collected anonymously. The interviews that we conducted to test the large-scale survey instrument were not anonymous, but we did not ask interviewees to provide any confidential or sensitive information.

## Acknowledgments

We would like to thank Coye Cheshire and Galen Panger for their insightful comments and discussion. This material is based on work supported by a Facebook Fellowship, NSF grant CCF-0424422, and the Intel Science and Technology Center for Secure Computing. Any opinions, findings, conclusions, or recommendations expressed here are those of the authors and do not necessarily reflect the views of Facebook, the National Science Foundation, or Intel.

# 7. REFERENCES


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

[2] L. Barkhuus. Privacy in location-based services, concern vs. coolness. In *Workshop on Location System Privacy and Control at MobileHCI*, 2004.

[3] L. Barkhuus and A. Dey. Location-based services for mobile telephony: a study of users' privacy concerns. In *INTERACT*, pages 702–712, 2003.

[4] C. Bonnington. Apple Says Grabbing Address Book Data Is an iOS Policy Violation. *Wired: Gadget Lab*, February 15 2012. `http://www.wired.com/gadgetlab/2012/02/apple-responds-to-path/`.

[5] A. Braunstein, L. Granka, and J. Staddon. Indirect Content Privacy Surveys: Measuring Privacy Without Asking About It. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, 2011.

[6] comScore Data Mine. US Smartphone Owners by Age. `http://www.comscoredatamine.com/2011/06/us-smartphone-owners-by-age`, June 2011.

[7] 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 *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*, 2005.

[8] S. Egelman, A. P. Felt, and D. Wagner. Choice Architecture and Smartphone Privacy: There's A Price For That. In *Workshop on the Economics of Information Security (WEIS)*, 2012.

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

[10] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner. Android permissions: User attention, comprehension, and behavior. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, 2012.

[11] D. Goodin. Backdoor in top iPhone games stole user data, suit claims. *The Register*, November 2009.

[12] P. Hornyack, S. Han, J. Jung, S. Schechter, and D. Wetherall. These Aren't the Droids You're Looking For: Retrofiting Android to Protect Data from Imperious Applications. In *ACM Conference on Computer and Communications Security (CCS)*, 2011.

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

[14] P. G. Kelley, M. Benisch, L. F. Cranor, and N. Sadeh. When are users comfortable sharing locations with advertisers? In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*, 2011.

[15] S. Lederer, J. Mankoff, and A. K. Dey. Who wants to know what when? Privacy preference determinants in ubiquitous computing. In *CHI Extended Abstracts on Human Factors in Computing Systems*, 2003.

[16] I. Muslukhov, Y. Boshmaf, C. Kuo, J. Lester, and K. Beznosov. Understanding Users' Requirements for Data Protection in Smartphones. In *ICDE Workshop on Secure Data Management on Smartphones and Mobiles*, 2012.

[17] F. Roesner, T. Kohno, A. Moshchuk, B. Parno, H. Wang, and C. Cowan. User-Driven Access Control: Rethinking Permission Granting in Modern Operating Systems. In *Proceedings of the IEEE Security & Privacy Symposium*, 2012.

[18] S. Thurm and Y. I. Kane. Your apps are watching you. *The Wall Street Journal*, December 2010.

[19] 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 *Proceedings of the 13th International Conference on Ubiquitous Computing (UbiComp)*, 2011.


# APPENDIX

# A. FULL RESULTS

Table 4 shows the VUR rates for all of the 99 risks that were in our survey, ordered by rank. Table 5 lists the permissions that we used to generate the risks.

| Risk | Very Upset Rate |
|---|---|
| permanently disabled (broke) your phone | 98.21% |
| made phone calls to 1-900 numbers (they cost money) | 97.41% |
| sent premium text messages from your phone (they cost money) | 96.39% |
| deleted all of your contacts | 95.89% |
| used your phone's radio to read your credit card in your wallet | 95.15% |
| publicly shared your text messages | 94.48% |
| deleted all of the information, apps, and settings on your phone | 94.39% |
| publicly shared your e-mails | 93.37% |
| deleted all of your other apps | 93.14% |
| shared your text messages with friends | 92.49% |
| recorded your credit card # when you entered it into a different app | 92.35% |
| publicly shared your photos | 90.60% |
| changed your keylock/pattern/PIN | 90.46% |
| sent text messages from your phone | 90.42% |
| shared your contact list with advertisers | 90.19% |
| spammed your contacts with event invitations | 89.73% |
| made phone calls | 89.62% |
| shared your text messages with advertisers | 88.63% |
| sent spam to people on your contact list | 87.95% |
| publicly shared your call history | 87.77% |
| shared your photos with advertisers | 87.26% |
| shared your e-mails with your friends | 86.87% |
| shared your call history with advertisers | 85.80% |
| shared your browsing history and bookmarks with friends | 85.68% |
| shared your e-mails with advertisers | 83.96% |
| publicly shared your calendar | 83.68% |
| recorded the passwords that you enter into other apps and websites | 83.38% |
| sent spam from your e-mail account | 82.76% |
| shared your call history with your friends | 82.04% |
| shared your photos with your friends | 81.28% |
| shared your e-mail address with advertisers | 82.31% |
| deleted or changed files used by other apps on your phone | 82.14% |
| inserted spam messages at the end of a text message you sent | 81.15% |
| hung up your phone when you're talking | 81.00% |
| publicly shared your e-mail address | 80.70% |
| publicly shared your phone's unique ID | 78.92% |
| recorded you speaking with your phone's microphone | 78.86% |
| installed other apps onto your phone | 78.46% |
| took a photo with your front-facing camera | 77.30% |
| muted a phone call when you're talking | 77.27% |
| deleted all of the events on your calendar | 76.89% |
| shared your phone's unique ID with advertisers | 76.61% |
| posted to your Facebook wall | 76.30% |
| used your data plan to download data when you were roaming | 75.57% |
| sent your e-mails to their servers (but didn't share them with anyone else) | 75.51% |
| sent your text messages to their servers (but didn't share them with anyone else) | 75.48% |
| turned your keylock/pattern/PIN off | 74.72% |
| deleted other apps' saved passwords | 73.96% |
| shared your contact list with friends | 73.59% |
| took a photo with your rear-facing camera | 73.54% |
| shared your calendar with advertisers | 73.47% |
| publicly shared your location | 71.57% |
| shared your browsing history and bookmarks with advertisers | 70.74% |
| un-muted a phone call | 70.73% |
| took screenshots when you're using other apps | 70.23% |
| deleted all of your browser bookmarks and RSS feeds | 69.87% |
| added new contacts | 69.57% |
| sent your contact list to their servers (but didn't share it with anyone else) | 69.29% |
| force quit all your other apps | 69.29% |
| sent your call history to their servers (but didn't share it with anyone else) | 68.41% |

| Risk | Very Upset Rate |
|---|---|
| used your data plan to download data | 67.83% |
| turned your Internet connection off while you were using the Internet | 64.84% |
| logged in to your Facebook account | 64.34% |
| prevented other apps from running | 63.99% |
| shared your calendar with your friends | 63.59% |
| shared your location with advertisers | 62.80% |
| shared the list of apps you have installed with advertisers | 61.85% |
| prevented your phone from being backed up to your computer | 61.39% |
| sent your photos to their servers (but didn't share them with anyone else) | 60.95% |
| used your phone's unique ID to track you across apps | 60.33% |
| changed the time on your phone | 60.00% |
| logged in to your saved Google account | 59.38% |
| shared your location with your friends | 58.10% |
| restarted your phone | 57.56% |
| drained your battery | 55.61% |
| publicly shared the list of apps you have installed | 54.77% |
| sent your browsing history and bookmarks to their servers (but didn't share them with anyone else) | 54.59% |
| set alarms on your phone | 54.05% |
| changed your phone's wallpaper | 52.51% |
| shared the list of apps you have installed with your friends | 52.36% |
| turned the sound on your phone up really high | 52.12% |
| shared your e-mail address with your friends | 52.00% |
| showed you lots of pop-up notifications | 51.90% |
| prevented your phone from being backed up to the cloud | 50.52% |
| sent your calendar to their servers (but didn't share it with anyone else) | 50.14% |
| slowed down your phone | 50.00% |
| disconnected you from a Bluetooth device (like a headset) while you were using the Bluetooth device | 48.63% |
| sent your e-mail address to their servers (but didn't share it with anyone else) | 46.87% |
| turned your WiFi back on when you were on a plane | 45.52% |
| inserted extra letters into what you're typing | 45.48% |
| read files that belong to other apps | 44.33% |
| sent your phone's unique ID to their servers (but didn't share it with anyone else) | 42.16% |
| added new browser bookmarks | 39.22% |
| turned the sound on your phone down really low | 36.96% |
| sent the list of apps you have installed to their servers (but didn't share it with anyone else) | 34.92% |
| sent your location to their servers (but didn't share it with anyone else) | 29.88% |
| turned your flash on | 29.67% |
| connected to a Bluetooth device (like a headset) | 27.47% |
| vibrated your phone | 15.62% |

**Table 4: The number of respondents who indicated they would be "Very upset" if a given risk occurred. We asked 99 questions about risks; each respondent saw 12 of those questions.**

| |
|---|
| Run all the time. System tools: automatically start at boot; System tools: make application always run; System tools: prevent device from sleeping |
| Default: control system backup and restore |
| Default: delete applications |
| Default: directly install applications |
| Default: permanently disable device |
| Default: power device on or off; Device: force device reboot |
| Modify keyboard output. Default: press keys and control buttons; Default: bind to an an input method |
| Read screen outputs and keyboard inputs. Default: read frame buffer; Default: record what you type and actions you take; Default: bind to an an input method |
| Default: reset system to factory defaults |
| Hardware controls: change your audio settings |
| Hardware controls: control flashlight |
| Hardware controls: control vibrator |
| Hardware controls: record audio; Default: audio file access |
| Front-facing camera. Hardware controls: take pictures and videos |
| Rear-facing camera. Hardware controls: take pictures and videos |
| Network Communication: Control Near Field Communication |
| Network Communication: Create bluetooth connections; System tools: Bluetooth administration |
| Data access while roaming. Network Communication: Full Internet access; Network Communication: Receive data from Internet |
| Data access while not roaming. Network Communication: Full Internet access; Network Communication: Receive data from Internet |
| Network Communication: View network state; Network Communication: View Wi-Fi state; Your location: coarse (network-based) location; Your location: fine (GPS) location |
| Read photo library |
| Notifications |
| Phone calls: modify phone state |
| Unique phone ID (eg IMEI). Phone calls: read identity |
| Call history. Phone calls: read phone state; Phone calls: intercept outgoing calls |
| Premium phone calls. Services that cost you money: directly call phone numbers |
| Non-premium phone calls. Services that cost you money: directly call phone numbers |
| Premium SMS. Services that cost you money: send SMS messages |
| Non-premium SMS. Services that cost you money: send SMS messages |
| Read the SD card. Storage: modify/delete USB Storage contents modify/delete SD card contents |
| Write to the SD card. Storage: modify/delete USB Storage contents modify/delete SD card contents |
| System tools: Change network connectivity; System tools: Change Wi-Fi state |
| Change keylock. System tools: disable keylock |
| Remove keylock. System tools: disable keylock |
| Kill other apps. System tools: force stop other applications; System tools: kill background processes; Default: prevent app switches; Default: monitor and control all application launching |
| System tools: retrieve running applications |
| System tools: set time zone; Default: set time |
| System tools: set wallpaper; System tools: set wallpaper size hints |
| Your accounts: discover known accounts; Your accounts: view configured accounts; Default: discover known accounts |
| Your accounts: manage the accounts list |
| Your accounts: use the authentication credentials of an account |
| Your location: coarse (network-based) location; Your location: fine (GPS) location |
| Read e-mail. Your messages: Read Email attachments; Your messages: read Gmail; Your messages: read Gmail attachment previews; Your messages: read instant messages |
| Your messages: read SMS or MMS; Your messages: receive MMS; Your messages: receive SMS; Your messages: receive WAP |
| Your messages: Send Gmail; Your messages: modify Gmail; Your messages: write instant messages |
| Modify calendar events. Your personal information: add or modify calendar events and send emails to guests |
| Send calendar invitations. Your personal information: add or modify calendar events and send emails to guests |
| Your personal information: read browser's history and bookmarks; System tools: read subscribed feeds |
| Your personal information: read calendar events |
| Your personal information: read contact data |
| Your personal information: set alarm in alarm clock |
| Your personal information: write browser's history and bookmarks; System tools: write subscribed feeds |
| Your personal information: write contact data |

**Table 5: The 54 permissions we used to generate the risks.**