Detecting iPhone Security Compromise in Simulated Stalking Scenarios: Strategies and Obstacles

Andrea Gallardo, Hanseul Kim, Tianying Li, Lujo Bauer, and Lorrie Cranor,
Carnegie Mellon University

https://www.usenix.org/conference/soups2022/presentation/gallardo

This paper is included in the Proceedings of the Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022).

August 8–9, 2022 • Boston, MA, USA

978-1-939133-30-4

Open access to the Proceedings of the Eighteenth Symposium on Usable Privacy and Security is sponsored by USENIX.

Detecting iPhone Security Compromise in Simulated Stalking Scenarios: Strategies and Obstacles

Andrea Gallardo
Carnegie Mellon University

Hanseul Kim
Carnegie Mellon University

Tianying Li
Carnegie Mellon University

Lujo Bauer
Carnegie Mellon University

Lorrie Cranor
Carnegie Mellon University

Abstract

Mobile phones can be abused for stalking, through methods such as location tracking, account compromise, and remote surveillance. We conducted eighteen remote semi-structured interviews in which we presented four hypothetical iPhone compromise scenarios that simulated technology-enabled abuse. We asked participants to provide advice for detecting and resolving each type of compromise. Using qualitative coding, we analyzed the interview data and identified the strategies of non-expert participants and the difficulties they faced in each scenario. We found that participants could readily delete an app and search in iOS settings or the home screen, but they were generally unable to identify or turn off location sharing in Google Maps or determine whether the iCloud account was improperly accessed. When following online advice for jailbreak detection, participants had difficulty finding a root checker app and resetting the phone. We identify underlying factors contributing to these difficulties and recommend improvements to iOS, Google Maps, and online advice to reduce the difficulties we identified.

1 Introduction

Mobile phones can be abused to enable stalking through methods such as location tracking, account compromise, and remote surveillance. For example, victims of intimate partner violence (IPV) may experience such technology-enabled abuse [23, 35, 53, 61, 62]. While experts can help victims detect and recover from technology-enabled abuse, little is known about the ability of victims to do this on their own, with the assistance of non-experts in their social support network, or with the assistance of online educational materials.

We developed four hypothetical iPhone compromise scenarios that simulated technology-enabled abuse based on real-world scenarios faced by IPV victims and other victims of stalking. To gain insights into how non-experts in victims' social support networks might help them, we conducted 18 remote interviews in which we presented these scenarios and asked iPhone users recruited from Craigslist how they would help a friend detect and resolve each security compromise.

We found that while these non-expert participants were familiar with the iOS user interface (UI), most had difficulty detecting and resolving the problems simulated in our scenarios. For example, participants had difficulty associating Google Maps with location sharing controls. The challenges participants encountered were caused by discoverability issues in iOS and Google Maps UIs, such as a lack of indicators showing that another device has iCloud account access or that location is being shared with another user, as well as an absence of features that would help users know whether apps could be used to monitor them. We also found that online advice on detecting jailbreaking and resetting an iPhone often had impractical, inaccurate, or jargon-filled instructions.

Our paper makes the following novel contributions:

- Identifying strategies used by non-experts and specific difficulties they face, such as pinpointing the app transmitting the device's location to another user, as they attempt to detect and resolve four types of security compromise characteristic of technology-enabled abuse;
- Identifying underlying factors, e.g., lack of persistent notifications, contributing to difficulties we identified, most of which may be applicable across apps and platforms;
- Recommending specific changes to iOS, Google Maps, and online advice that would likely reduce the difficulties we identified and make it easier for non-experts to detect device or account compromise; and

USENIX Symposium on Usable Privacy and Security (SOUPS) 2022.
August 7–9, 2022, Boston, MA, United States.

- Highlighting the need to consider the stalking threat and victims' ability to use devices when developing apps.

2 Related Work

In this section, we review prior work on technology-enabled abuse and interventions and online advice to prevent it.

2.1 IPV and Stalking Threat Model

Our study focuses on scenarios in which a malicious user leverages features of iOS, iCloud, and apps downloaded from the Apple App Store ("App Store"), for the purpose of stalking. People may experience such stalking in the context of IPV, also known as domestic violence or domestic abuse, but anyone with access to a victim's mobile phone (e.g. coworkers, employers, roommates, relatives) may carry out these kinds of non-sophisticated (but often difficult to detect) attacks.

Exploitation of Technology by Abusers. The threat model of technology-enabled abuse faced by IPV victims does not require technical sophistication and is characterized by adversaries limited by the functionality of the system's UI [23, 33, 35, 62]. Technology-enabled abusers can take advantage of access to devices and accounts by initially setting them up, enabling features or downloading apps for surveillance. They can also compromise security by guessing passwords or answers to security questions, or threatening or coercing the victim into giving them access to devices, accounts and their live location data [23, 28, 34, 35, 47].

Legitimate Apps Used for Abuse. Some apps have legitimate use purposes (e.g., navigation, anti-theft tracking, or child or employee monitoring) and can be downloaded from mobile app stores, but they can also be used for illegal or harmful purposes, such as stalking or spying [13, 32, 41, 45]. Though sometimes marketed as safety products that should not be used for abuse, they appear in search results for phrases like "track my girlfriend" and may be profitable as stalking tools [13, 16, 20, 46, 59]. Due to their valid purposes and legal ambiguity around use-cases, such "dual-use" apps will likely continue to be allowed on app stores [13, 55]. Researchers have begun developing tools to detect these apps, using machine learning classifiers and graph mining algorithms, and to warn people about potential surveillance [22, 29, 45]. In our study, we challenged participants to detect such an app.

Risk of Escalation. While security assessment tools and interventions can empower victims countering coercive control in tech abuse contexts, they can create new problems or burdens in abusive or coercive situations [48, 61]. Certain behaviors, such as cutting off surveillance methods, may risk endangering the survivor by escalating violence [21]. No prior research has tested general population awareness regarding such risks, so we included a question in our study to do so.

Seeking Advice from Friends. Research shows that most victims disclose abuse to at least one informal social support network member (e.g., friend or family member) [25, 44, 49]. Research on technology-enabled abuse typically does not investigate the ability of these social supports, who are unlikely to be experts in identifying security compromise, to detect and remediate technology-enabled abuse [23, 34, 35].

Need for Usable Tools. IPV advocates have reported insufficient expertise to support victims of tech abuse, due to little to no training in preventing technology-based abuse [29, 35, 47]. Technical and clinical interventions have been developed, and online resources published, to help IPV and stalking victims [4, 6, 11, 24, 29, 57]. While researchers have suggested making usability improvements to UIs [22, 35, 40], they have not detailed specific usability problems. Our study surfaced consistent usability problems and areas for improvement not specifically identified by prior work.

Jailbreaking: Less Common but Dangerous. While increased usability and interventions may help counter unsophisticated attacks, a jailbroken iPhone presents a less common but more sophisticated threat that, if undetected, could endanger victims. Jailbreaking allows downloading apps banned by the App Store, such as spyware, and enables the ability to hide apps, potentially turning smartphones into surveillance devices. [18, 26, 31]. Prior work shows that victims consider the potentially dangerous risk of hidden surveillance when deciding whether to keep, replace, or destroy their devices [29, 35].

2.2 Online Security Advice for Survivors

IPV survivors have expressed a desire to learn more about privacy and to have more control over their digital assets, as well as dissatisfaction about using internet searches to do so [24]. Prior work has shown how unclear advice can make it difficult to assess technology-enabled security threats [54]. Research on information-seeking behaviors and responses to security advice suggests that non-tech savvy users may not effectively prioritize or follow security advice [37, 42, 43].

Many online articles provide advice on how to detect and prevent technology-enabled abuse, including jailbreaking and stalkerware [38, 51, 52, 58]. Advice varies in format and depth, from general advice [2] to concise lists of action items [14, 15] to step-by-step instructions [7, 38]. Some advice is technical and may be too complicated for non-tech-savvy users [36, 50], and some articles are outdated, recommending a jailbreak detection app that is no longer available on the App Store [5, 19]. Given the plethora and variety of such online advice, insight is needed into obstacles faced in implementing this advice. In one of our scenarios, we presented participants with two online articles and evaluated how easy it was for them to follow advice on detecting jailbreaking on an iPhone.

3 Methodology

In our interview study, participants encountered four hypothetical scenarios that reflect risks faced by victims of IPV and

stalking: location tracking, apps with remote access, account compromise, and jailbreaking. In this section, we describe our participant recruitment process, scenario and interview design, analysis process, and the limitations of our methodology.

3.1 Recruitment

We recruited participants who were "interested in mobile phone security" to participate in a 45 to 60 minute interview through Craigslist's "Computer Gigs" section for three cities, Los Angeles, New York, and Pittsburgh, and offered $20 as compensation. We screened for the following criteria: at least 18 years old, located in the U.S., fluent in English, has access to a device that can connect to internet, can run Zoom, and uses an iPhone. We also collected basic demographic information (see Appendix C) to diversify the sample demographics to be reflective of the U.S. population. Our screening survey received 176 responses, and we invited 77 respondents to participate in the study.

We intentionally did not recruit IPV victims or other stalking victims, to avoid re-traumatization by making them revisit memories of abuse [17, 30, 56]. Prior work has suggested taking a participant-centered approach when working with trauma victims and including mental health professionals who can provide services, if needed [29, 60]. However, our study did not involve services or interventions that would address the specific needs of victims.

We thus focused on the ability of members of a victim's social support network to help detect and remediate security compromises, and recruited from the general population rather than self-identifying victims or survivors. We advertised seeking participants "interested in mobile phone security," without screening for experience or expertise, to recruit participants who might have enough interest in mobile phone security to be willing to help a friend with iPhone security issues.

We limited our participants to iPhone users to simplify the study design, as iPhone user experience is relatively uniform compared to Android phones, which vary by manufacturer and Android version. The problems we investigated are consistent across recent iOS versions (Section 5).

3.2 Interview

We conducted remote, semi-structured interviews with 22 participants over Zoom from April through August 2021. We eliminated four interviews from our analysis, as we discovered during the interview that these participants did not meet our screening criteria. We recorded audio and video (of our shared iPhone screen) and transcribed interviews using Zoom and Otter.ai. We conducted two slightly different versions of the interview, each with nine participants (see Section 3.5 for more details). Our interview script is included in Appendix A. All of our study protocols were approved by our IRB.

We presented participants with four distinct exemplar scenarios that we selected based on a range of threats seen in prior work [13, 16, 18, 22, 23, 26, 28, 29, 33, 35, 47, 62], news articles [46, 55], and through one author's experience as a technologist in a techclinic for IPV survivors. To simulate the scenarios, we used Zoom's screen sharing feature to share the live screen of an iPhone (iOS versions 14.5-14.6) that had been reset and set up for this study.

To understand participants' existing knowledge, we started three scenarios by asking them to define a mobile phone security concept related to the scenario (spyware, account compromise, and jailbreaking). In each scenario, we presented the iPhone screen remotely via Zoom, read the scenarios aloud to participants, and asked them to give us directions to interact with the iPhone and guide us through their strategies to help a hypothetical friend or coworker investigate their suspicions about stalking, account compromise, and surveillance. At the end of each scenario we asked participants how easy or difficult they had found the tasks, whether they would advise their friend to do anything else, and what they would do if they encountered that scenario in their own life.

We presented scenarios in an open-ended way, without specific instructions for how to approach the problem. However, when participants said they did not know what to do or lingered on irrelevant options, we gave them a hint for how to proceed, having developed a set of hints per scenario as part of our interview script, to help participants complete the task. This prevented us from being limited to observing only early obstacles that might otherwise prevent a participant from completing the task. Participants were not prohibited from using external resources: some directed us to do an internet search, and a few did internet searches on their personal devices.

Scenario 1. The first scenario was designed to explore participants' strategies for determining whether someone had access to the iPhone's location information, how easily they discovered the Location Sharing feature within Google Maps, and how easy they found it to disable this feature. We asked participants to imagine that their coworker asked for help confirming whether or not someone was tracking their (the coworker's) location through their iPhone. Our iPhone's location was being shared with "Mallory" via Google Maps' Location Sharing feature, which can grant access to location information until revoked or for a certain length of time.

If participants attempted to resolve the problem by turning off iOS Location Services, we clarified that the coworker needed it on for navigation purposes and that we wanted to determine whether location was being shared with someone else. We gave participants hints to help them see that the Google Maps app was using their location, as shown in Figure 1.

Scenario 2. In the second scenario, we explored how participants investigated their friend's suspicion that their intimate partner was remotely spying on their phone, whether they could detect that an app could be used to remotely access the device,and whether they could remove the app.

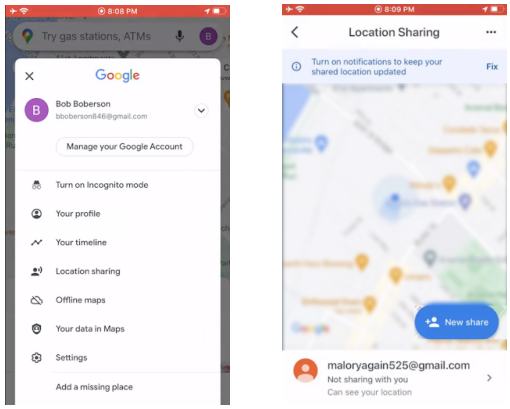

Figure 1: In Google Maps, selecting the top right circle revealed a drop-down menu with a "Location sharing" option (left). Selecting "Location sharing" revealed another account with access to the device's location (right).

We first asked participants to describe what they thought spyware was. We then told them that their friend suspected that their significant other had "hacked" their phone and asked them to help their friend find out whether their significant other was remotely accessing their device using spyware.

On the test device, we installed an app that enables remote access and is marketed as a technical support tool, TeamViewer. Though iOS provides ongoing alerts while TeamViewer remotely accesses an iPhone, we envisioned a threat model in which the friend's significant other has physical access and the passcode to the friend's phone, and finds convenient times to remote into the friend's phone to spy on them or to change settings that might enable spying, without needing to physically access the phone for long periods of time. Our intention was to observe how participants identified which app could remotely access the device, not whether remote access would be detectable while it was taking place.

After we noted their initial search attempts, we gave participants a hint that the suspected "spyware" was an app from the App Store and, if needed, another hint to search among the apps on the phone to find which app could be used as spyware. In the last nine interviews we added a hint to clarify that we were looking for an app that enables remote access to the device, not apps that simply appear suspicious. If participants were not familiar with the app or aware of its capabilities (as none were), we revealed that TeamViewer is an app that can be misused to enable spying, and that the friend's significant other used it to remotely access the device without their friend's permission.We then asked participants what precautions or advice they would suggest that their friend keep in mind, to see if they would consider escalation of abuse to be a possibility (see Section 2.1). We then told them that their friend decided it was safe to remove the spyware and asked them to guide us in removing the app.

We used the term "spyware" to describe what the friend suspected was happening, i.e., spying. While we explained to participants that the TeamViewer app could be legitimately used for remote access or assistance, we continued to use the term "spyware" to capture the app use-case in the scenario's context.

Scenario 3. In the third scenario, we explored whether participants could recognize indicators of iCloud account compromise and remove an unknown device's access to an iCloud account. We asked them to describe what they thought account compromise was, then told them that their friend's photos (and messages, in the second half of our interviews) were appearing and disappearing and asked them to help investigate. In the first nine interviews, we only mentioned photos, not messages (see Section 3.5).

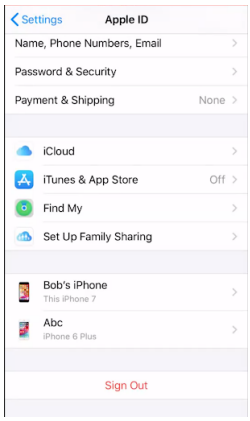

Figure 2: In iOS Settings, selecting the Apple ID and scrolling down revealed a list of devices logged into the iCloud account.

We had logged into an iCloud account with two different devices, the test device and another device, and synced iCloud apps (Photos and iMessage) between them. We wanted to understand whether participants would intuit that changes in photos and messages could be a sign of iCloud compromise and discover an unknown device logged into the iCloud account, as well as how easy it was for them to remove an app from the list of devices logged into iCloud (see Figure 2).

Scenario 4. In this scenario, we investigated how easy it was for participants to follow online advice to detect whether a device is "jailbroken." First, we asked participants to define "rooted" and "jailbroken." We then asked them to imagine that their friend suspected their iPhone was jailbroken and wanted help following online advice for detecting jailbreaking.

We included a jailbreaking scenario because it enables downloading and hiding spyware banned by the App Store (see Section 2.1). As we wanted to study options available to general users, we searched online for articles with advice on how to detect jailbreaking and stalkerware.We chose articles by the FTC [8, 15] and Avast [12] because they might be recognizable, trusted and shared, and had simple instructions. In the first nine interviews, we presented participants with an article that suggests using a root checker app [15], and in the next nine, with an article that recommends checking whether the Cydia app ("Cydia"), a common app store for jailbroken iPhones, is installed on the phone [12]. Both articles suggest resetting the phone, which we asked participants to do in the last nine interviews. See Appendix B for the advice text.

3.3 Data Analysis

We conducted a qualitative thematic analysis of the interviews by coding the interview transcripts as a group. Two of us coded all interviews, initially joined by a third researcher. Any initial disagreements were resolved through discussion. Since we conducted the coding collaboratively, it was not appropriate to calculate inter-rater reliability. We gathered keywords and ideas from the interviews and found common themes. Since the interview was divided into four scenarios, we coded in sessions dedicated to each scenario and developed a code book for each scenario. We reused several codes across scenarios, but there were also codes unique to each one. Our code book can be found in Appendix D.

To get a better idea of what was challenging or intuitive, we also analyzed the number of hints participants required for each scenario and their explanations about what they found easy or difficult about detecting and resolving the problems.

3.4 Limitations

As our study consisted of simulated scenarios, its design did not always reflect a completely realistic or typical situation. Additionally, it has some limitations due to the qualitative and remote nature of the study. While our study is limited to iOS and the apps studied, characteristics underpinning our findings are shared by OSes and apps more generally.

OS and App Selection. Many aspects of our study are applicable beyond iOS and Google Maps. Various navigation apps across OSes, including Google Maps (Scenario 1), Find My, and Waze, do not provide persistent notifications when the device transmits location to another user (see Section 5.1.1). Scenario 2 might be similarly difficult for Android users, as there are no obvious indicators on Android to inform users about apps' spying capabilities. While Scenario 3 is specific to iCloud, other OSes (and apps) offer cloud data syncing across multiple devices (e.g. Google). Popular instructions for detecting jailbreaking and (Android) rooting (Scenario 4) contain similar jargon (see Section 2), though future work could consider the usability of Android root detection apps.

Simulating Detection of Spying Capabilities. We encountered some challenges in designing a scenario to detect a legitimate app that could be misused for spying. In the initial nine interviews, our test phone had only three non-default apps installed: Zoom, Google Maps, and TeamViewer (see the left side of Figure 3). Though a few participants noted their unfamiliarity with TeamViewer, that does not mean they determined it could remotely access the device. See Section 3.5 for our modifications to this scenario. Additionally, we did not include hints to look at app permissions. TeamViewer and most other apps had not been set up or tested, which meant that additional permissions that might suggest remote access capability, such as Screen Recording or Accessibility permissions, had not been granted. While only two participants looked at permissions for TeamViewer (which may have been easier to spot for the first nine participants, given that only three non-default apps were installed on the phone), we could have designed the scenario such that participants could look at app permissions to find that Screen Recording was enabled.

Figure 3: Home screen in version 1 (left) and version 2 (right) of the study. The difference appears to have influenced whether participants noticed the remote access app.

A Remote and Unfamiliar Test Device. In Scenario 3, three participants could not find the list of devices logged into the iCloud account because they did not scroll down. In Scenario 1, one participant said they did not see the "Stop" button (to stop sharing location) at the bottom of the screen, though our screen recording captured it. If the participants had been holding the test device, they may have intuitively scrolled down or been better able to look at the entire screen.

Additionally, if participants had really been helping their friend, they might be more familiar with the names and accounts logged into Google Maps or iCloud (Scenarios 1 and 3) and more suspicious of a stalker's email account or device.

Ordering Effects. Scenario order remained the same across interviews. While there may be ordering effects, each scenario required different skills. We observed participants routinely facing challenges in each subsequent scenario regardless of anything they may have learned from a previous one.

3.5 Study Modifications

We changed Scenarios 2 and 3 for the last nine interviews (P10-P18) to probe the impact of increasing the number of non-Apple apps installed on the phone and the number of apps involved in suspicious iCloud behavior, respectively. We wanted to see whether participants would continue to mention TeamViewer among 32 additional and potentially unfamiliar apps (see Figure 3) in Scenario 2 (they did not—a valuable contrast). We also wanted to see if participants would more easily detect iCloud compromise in Scenario 3, i.e., more intuitively link the suspicious behavior to the iCloud account, if we noted that two apps instead of one, photos *and* iMessage, were appearing and disappearing. In the first version, we only

mentioned photos, and seven of nine participants focused primarily on the Photos app and settings. Yet, responses were roughly the same, with five more participants focusing on photos. We discuss findings in Section 4.2 and Section 4.3.

To gain insight into subjective perspectives, we added questions about what participants would do if they experienced the same technical issue and, instead of asking them to rate difficulty on a scale, we made our questions more open-ended, asking how easy or difficult they found the scenario and why.

4 Results

We present findings surfaced by qualitative analysis of interview transcripts for each of the four scenarios. Our reports on frequency of behaviors are useful for understanding our participants but are not generalizable to a larger population.

4.1 Location Tracking

In this scenario, participants were asked to help their coworker find out whether someone (Mallory) was tracking their coworker's phone. Participants had difficulty associating a navigation app, Google Maps, with location sharing controls. While all participants appeared to understand that iOS Location Services were enabled and that Google Maps was always using Location Services, none of them suggested opening the app to investigate or disable location sharing. To stop location sharing, most participants attempted to fully turn off Location Services, which would prevent the co-worker from using navigation apps. With the hint to open the Google Maps app, most participants were able to confirm that location was being shared with Mallory and quickly stopped location sharing, though a few participants had difficulty navigating the UI. Most participants found this scenario to be difficult but suggested that it would have been easy, had they known to explore the app.

4.1.1 Detecting and Stopping Location Sharing

No participants discovered on their own that location was being shared with Mallory through Google Maps' Location Sharing feature. After we provided hints, 15 out of 16 participants[1] (all but P4) eventually discovered this.

Initial Strategies. Eight participants explored other iOS features, such as Tracking, Accessibility, and Control Center, which did not provide location-related information, and two participants used the iOS search bar to search for "location."

Participants' strategies in navigating the iOS Location Services UI varied. Eight participants looked at the Share My Location settings. Three participants, upon seeing that location was not being shared through this setting, concluded that location was therefore not being shared at all.

> *Basically, you just see if Share My Location is on or off. Clearly it's off, so I guess that I would assume that someone is not tracking your location. (P17)*

Ten participants suggested turning off iOS Location Services. This could be impractical if the user depends on using Location Services, e.g., for navigation. Three participants suggested changing Location Services settings for Google Maps, for example from "Always" to "Never," but these solutions do not permanently resolve the issue, as location could be transmitted upon re-enabling Location Services. In addition, three participants suggested turning off Find My iPhone, which would not work, since it was not the app transmitting data.

Hints. Our hints were intended to guide participants to look at the iOS Location Services settings and notice that Google Maps was the only app always using location, which we hoped would inspire them to open the app and investigate its Location Sharing feature. Three of 16 participants required Hint 1, to go into iOS Settings and search for something related to location. Six (including the prior three) required Hint 2, to search in iOS Privacy Settings and Location Services, to see that Google Maps was using location services. These participants had initially been looking at other iOS settings.

All 16 participants required Hint 3, to open Google Maps and check its settings. Seven participants required only this hint. Although three participants noted that Google Maps was set to "Always" use location, no one suggested exploring within-app settings. Four participants remarked on the difficulty, considering the process to involve too many steps:

> *I honestly never do this. It was just too much jumping around and knowing the difference between when to look into settings on the phone, versus when to look on settings in the specific app. (P12)*

After opening Google Maps, six participants required Hint 4 to select the Location Sharing option in the drop-down menu.

Checking Google Maps Settings. Once participants received the hint to open Google Maps (which no participant suggested), nine were able to select the top-right circle and select Location Sharing settings from the resulting drop-down menu (Figure 1 left). Eight of these nine understood that the subsequent screen (Figure 1 right) showed that location was currently being shared with another user, Mallory. However, P7 and P15 did not understand the screen showing Mallory's email. P7 asked whether we were trying to communicate with Mallory, and P15 assumed Mallory's email was the coworker's email. P10 asked us to confirm whether Mallory's email could be trusted. In Section 3.4 we discuss the limitation that participants might be more likely to recognize their own or their coworker's details in a realistic scenario.

Seven participants had some difficulty navigating the Google Maps UI. P12 and P17 directed us to select the blue arrow icon, which only changes the angle of the map's view. P16 told us to look for a "blue thing" next to the iOS time,

[1] We are using data for 16 participants for Scenario 1 strategies, because the interviewer did not properly follow the interview script for P1 and P5.

perhaps referencing an iOS icon that appears when location is being used. P6 selected "Updates" and P9 selected "Contribute" at the bottom of the initial Google Maps screen. P13 said they had not known location could be shared via Google Maps and suggested looking at location search history.

Once participants saw that the location was being shared with Mallory, nine of them suggested that the process would have been easy if they had known to search in Google Maps.

> *You wouldn't really expect to use Google Maps. When it comes to someone sharing your location, you'd assume that it's one of the apps that's pre-installed on the iPhone. That was confusing, because I didn't think that I'd need to go there in the first place. But then, once I did know it's Google Maps and went to settings . . . I can just find the thing that says something to do with sharing a location. (P17)*

> *To go in the app itself, not just the iPhone, but the app settings, that's tricky in itself, so I had a little bit of issue to find that, but I mean, it was all there. (P14)*

Strategies to Stop Location Sharing. After participants observed that location was being transmitted to Mallory, we asked them to guide us to stop location sharing. Eleven participants clicked the arrow next to Mallory's email on the Location Sharing screen, which led to a screen with a "Stop" button, and then selected "Stop." Three participants effectively stopped sharing through an alternate route. P10 and P15 selected the three dots next to Mallory's email and went to the Google Account's Location Sharing settings via Safari to stop sharing, and P7 blocked Mallory. Two participants chose sufficient but temporary solutions. P4 turned on incognito mode in Google Maps. P18 went back to iOS Location Services settings and changed Google Maps location settings from "Always" to "Never." P8 mistook a nudge for a viable option, suggesting we click "Fix"(see the top of Figure 1).

P4 and P7 tried to add a "New Share" in Google Maps, rather than remove an existing share. P7 said that they could not see the "Stop" button at the bottom of the screen when they first saw the screen showing Mallory. P4 thought setting time to zero for a new share might stop the sharing.

Most participants (12 of 16) found stopping location sharing to be easy, with six noting that it was self-explanatory.

4.1.2 Security Precautions

When we asked participants what they would do if they thought someone had access to their location, some discussed additional security precautions they would take. P14 mentioned blocking and, later, consulting the police:

> *I would definitely block the person from my phone, make sure . . . on social media, to get rid of that person, because depending on if it's Facebook or anything [where] you can see the other person's location, you may not know their location is on. (P14)*

P16 raised the possibility of escalation, which was the only mention of escalation in our entire study:

> *Based on my level of paranoia, if it seems like anything serious or fatal, some type of ongoing thing, like, let's say I removed that email and a new email popped up later on, I would try to probably download a VPN on my phone like something to just another layer of security, I guess. (P16)*

Unfortunately, a VPN does not necessarily mask a location that is being shared through a navigation app, so this would not be an effective strategy.

4.2 Spyware and Apps That Can Spy

In this scenario, we asked participants to identify which app could be misused as spyware to remotely access their friend's device. No participants successfully identified the remote access app, and most said they found the task of identifying it to be difficult. To find the app, most participants went into iOS settings and searched for an app with a suspicious name or with keywords such as "spy" in the name. We also asked what precautions or advice they would give to their friend after we revealed that TeamViewer was being used to spy on the friend. Most participants suggested deleting the app, and almost half suggested options that stalking victims may find difficult, such as ending the relationship or not allowing the significant other to access the phone. No participant mentioned the risk of escalating an abusive situation, which could threaten the friend's safety. Most participants said that deleting the app was easy, as the process is the same for all iOS apps. Six participants suggested doing more than deleting the app, such as deleting the account used or deleting the app from the other device. We discuss the results in more detail below.

4.2.1 Definitions of Spyware

Before prompting participants with Scenario 2, we asked them what they thought spyware was. Eleven of eighteen participants described spyware as a virus or malicious file that could discover information about them or spy on them. Four participants did not mention viruses or malware but described spyware as tracking or collecting information about them. Five participants thought spyware had to do with tracking web browsing. Three participants had the misconception that spyware was a tool that could protect them, claiming that it can act as an antivirus (P7), "help prevent your computer from coming into contact with threatening sites" (P9) and "protect you from people trying to hack into your phone" (P16). We did not correct them, but they appeared to realize their misconception after we prompted them with the scenario.

4.2.2 (Not) Identifying the Remote Access App

No participants identified the app, TeamViewer, as an app capable of remotely accessing the friend's device. For the first half of our participants, who saw only three non-default apps installed on the phone (Zoom, Google Maps and Team Viewer), four of nine participants considered TeamViewer to be suspicious because they were unfamiliar with it and suggested deleting it. When 35 non-default apps were installed on the phone, no participants pointed out the TeamViewer app but most participants suggested deleting a hacking-simulation game app called "HackIt."

Initial Strategies. When we asked participants what instructions they would give their friend to see whether there was spyware on their phone, 13 participants suggested going into iOS Settings. Within iOS Settings, four participants visited Control Center, six participants went into Privacy, and two participants visited Accessibility. P14 looked through the iOS home screen. Four participants did not immediately engage with the iOS UI, suggesting other strategies, such as using a search engine to query "How do I find out if there is spyware on my phone?" (P3), installing antivirus software (P8), contacting Apple (P13), or asking their friend if they had "opened any weird emails or texts" (P18).

Hints. All participants except P14 required Hint 1, that the suspected "spyware" is an app downloaded from the App Store. Three participants pointed out that spyware can be hidden. P11 expressed doubt about being able to detect spyware. We describe the the initial attempts to find spyware below.

Three participants required Hint 2 (swipe through the home screen to reach the iOS app library) to search for apps on the phone. All nine participants in version 2 of the study required Hint 3 (look for an app that enables remote access to the device), though it did not appear to help them, since no one was able to figure out which app could have remote access.

Strategies to Find Spyware. Once participants knew that the spyware was an app from the App Store, they took different approaches to detect it. Six participants chose to look at apps by scrolling down on the iOS Settings screen, seven looked at apps on the home screen, two went to the App Store, and one used the iOS search bar. Two participants were not sure where to look and were given Hint 2.

Out of six participants who reviewed apps at the bottom of the iOS Settings, only P5 and P9 looked at app permissions:

> *There's three apps on this iPhone, I would probably go through every single app, and see if there's a certain setting that causes a red flag... (P5)*

As we did not grant TeamViewer extra iOS permissions (see Section 3.4), P5 concluded that "there [was] nothing suspicious." P9 considered background app refresh suspicious.

We asked participants what they were looking for. Six participants said they were looking for keywords like "spyware" or app names they found weird or suspicious:

> *I would say apps with weird foreign names like Russian letters, Chinese letters or something. (P8)*

Other participants suggested that connections across multiple apps (P6), power consumption (P6), and location sharing (P5) could be indicators of spyware. Some participants did not know what they were looking for:

> *I didn't really know what I was looking for. TeamViewer doesn't seem very malicious, but if it was my phone I would recognize that there is an app that I didn't download, you know, so yeah, it'd be different if it were my phone. (P11)*

Recognizing and Understanding Apps. Fourteen participants found identifying the app capable of remote access or spying to be difficult. No participants were familiar with the app, so they were likely not aware of its ability to allow others to remotely control devices. P18 said that they had not known that remote access was possible. Three participants noted that solving the problem might involve being able to recognize unfamiliar apps or having their friend indicate which apps they might not recognize or remember downloading. After we showed P16 the App Library, they asked:

> *How would you know? Does the friend know what apps they already had and what they didn't? (P16)*

This highlights the difficulty of finding such an app on behalf of someone else, a challenge faced by advocates, who may not know what apps the survivor installed or not:

> *It's weird looking at someone else's phone, it's like another world. (P10)*

Participants also found it difficult to understand or learn the full capabilities of downloaded apps, including whether an app could be used as spyware.

> *It's kind of hard to tell. Sometimes you don't really know if someone has access to an app and is able to access your phone. (P8)*

4.2.3 Removing the App and Deleting Data

All 18 participants found deleting the app to be easy, with seven saying that this was because they have done it before. Some participants thought that deleting the app on the phone would delete the app's data.

> *I believe, if we just like, completely delete the app, it should delete everything associated, all the data associated with that app. (P13)*

Six participants, who were concerned about account data, suggested taking more steps after deleting the app, including erasing app data.

The only thing you would have to worry about is after you delete it, you know, make sure to erase your information, so you still don't have an active account with them. (P14)

Some participants' suggestions may not be feasible in IPV contexts, such as "delete the other half" of the spyware app on the significant other's phone (P2).

4.2.4 Advice to Friend Experiencing Tech Abuse

This scenario was the only scenario we situated within the context of IPV by asking the participant to imagine that their friend was being monitored by their significant other. Before asking participants to help their friend delete the app, we asked participants what precautions or advice they would suggest that their friend keep in mind.

Twelve participants said they would advise their friend to delete the app and ten suggested not letting other people handle or download things onto their device. Five participants suggested confronting the significant other, to figure out their intentions. Two of these suggested leaving the relationship:

Well, she didn't download it. Her loser boyfriend did. Get rid of the boyfriend. (P1)

I would definitely encourage them to leave the relationship. (P3)

4.3 iCloud Account Compromise

In this scenario, we asked participants to help their friend find out why some photos and messages were disappearing and new ones were appearing. With hints, we led them to discover an unknown device logged into the friend's iCloud account.

While most participants were familiar with the concept of iCloud and the iCloud account UI, they had difficulty discovering the list of devices on the Apple ID UI, even when they knew (or were given the hint) to search iCloud settings. Many participants looked at the iOS Photos settings, searching for things like Shared Albums. However, iOS Photos and Messages settings do not offer indications of other devices or device activity, so we had to nudge several participants towards the iCloud settings in iOS Settings. After seeing that an unknown device was logged into the iCloud account, most participants found it easy to remove the device. More than half of them suggested enhancing authentication mechanisms by changing the password or enabling multi-factor authentication.

4.3.1 Definitions of Account Compromise

Before starting the scenario, we asked participants what they thought account compromise was. Fifteen participants associated account compromise with another person (not the account holder) gaining access to the account or data in it. Six participants mentioned password compromise, three participants mentioned data leaks, and one mentioned a different device being used to access the account.

4.3.2 Finding Devices Logged into the iCloud Account

Only P11 and P13 were able to quickly find the unknown device in the device list on the Apple ID UI. With hints, 13 of 18 participants were able to eventually find the device. While it appeared to be intuitive for most participants to check settings related to the apps showing suspicious behavior, i.e., the Photos or Messages settings or iCloud Photos settings, there is no indication in these settings that another device is logged into the iCloud account and syncing with the apps.

Initial Strategies. Four participants appeared to initially connect changes in the Photos or iMessage apps to iCloud syncing with another device and immediately checked iCloud settings. However, two still required a hint to find the list of devices logged into the iCloud account.

Twelve participants focused on the Photos app and checked the Photos app, Photos app settings in iOS Settings, or iCloud Photos settings. Of the six of these who checked Photos app settings from the iOS Settings, three checked whether the Shared Albums feature was enabled and tried to turn it off.

My thought process for Shared Albums would be, if it's sharing it with other people, there would be an option to see who, like if there's a drop down to see who else can see the photos. (P12)

Five participants opened the Photos app, and two of those five checked the Albums UI for any "Hidden" items. P6 checked whether the iCloud Photos feature was enabled.

Participants also checked other settings before reaching the iCloud settings. Three out of nine participants looked at Messages settings in iOS settings and asked whether the email address appearing next to "Send & Receive" was supposed to be logged in. We confirmed that this was the iCloud account of the device owner in the scenario. P17 thought the problem was caused by another third-party app.

Hints. We provided hints to help participants understand that syncing with other devices might be occurring (Hint 1) and that this syncing was occurring through iCloud (Hint 2), and to guide them to the iCloud settings in iOS Settings (Hint 3), which might lead them to the Apple ID UI's list of devices.

Only P11 and P13 did not require a hint, though we had to redirect P13 after they guided us to change the iCloud password, which can stop syncing the iCloud with other devices but does not help us discover another device. After this redirection, P13 immediately located the device list.

Eleven participants required Hint 1, that their friend used to sync their photos with other devices. Seven of those required Hint 2, which noted that the changes were happening due to

iCloud account syncing. Three of those 11 required Hint 3, which led them to the Apple ID UI. P5 only needed Hint 1.

Five participants who did not require Hint 1, about device syncing, still required at least one of the other hints about iCloud. One participant required all three hints.

Navigating the iCloud Settings. To see the list of devices logged into the device owner's iCloud account, participants had to select the Apple ID (iCloud account) from the iOS Settings and scroll down. Half of them had difficulty finding this device list. Nine participants went into other options (including "Password & Security," "Name, Phone Numbers, Email," "Family Sharing," and "iCloud,") in the iCloud settings to find the device list. Three participants mentioned that they were familiar with iOS and iCloud but that finding the device list in the iCloud settings was not immediately apparent:

> *I think I knew generally to look under iCloud, but I just didn't know the full screen. (P3)*

P7 and P9 reached the screen listing logged-in devices but did not register its significance:

> *I didn't even know that that was another phone that was interfering or connecting into. (P7)*

4.3.3 Removing the Device from the iCloud Account

After finding the list of devices, 13 participants directed us to select the unknown device and select "Remove from Account" in the resulting screen showing the device information. Six participants noted how intuitive it was to identify the removal option, with two mentioning its red color. Five participants did not know how to proceed after finding the list of devices.

4.3.4 Security Precautions and Advice

Participants were asked what further advice they might give their friend or what they would do in the same scenario. Nine participants suggested changing the iCloud password and two of them also suggested using multi-factor authentication.

4.4 Online Advice to Detect Jailbreaking

In this scenario, we asked participants to help their friend follow online advice to find out whether an iPhone is jailbroken. After reading the online advice we showed them, most participants understood the instructions, but implementing the advice was not always easy. In our first nine interviews, we asked participants to follow online advice to find a "root checker app" (see Appendix B.1), and we found that no participants were able to successfully find such an app after searching in the App Store and on the web. In the next nine interviews, we asked participants to follow different online advice (see Appendix B.2), to search for an app called Cydia and "restore factory settings." Most participants found it easy to search for Cydia, but to "restore factory settings," most participants chose the wrong option.

4.4.1 Definitions of Rooted or Jailbroken

We started the fourth scenario by asking participants what they thought "rooted" or "jailbroken" meant. Since "jailbroken" is more commonly used in the context of iPhones than the term "rooted," it was unsurprising that 13 of 18 participants (all iPhone users), were familiar with the term "jailbroken," while only one participant was familiar with the term "rooted." Five participants described jailbreaking as beneficial, for customizing devices or downloading paid apps for free, and two participants suggested it meant the device was stolen or hacked. However, some participants, including ones who indicated they were familiar with the term, expressed difficulty understanding the concept of jailbreaking.

4.4.2 Searching for a Root Checker App

In our first nine interviews, we asked participants to follow the FTC's online advice to find a "root checker app" [8, 15]. We found that no participants were able to successfully find such an app. Six participants critiqued the article for not including any example apps, lacking details, and not being helpful.

To find a root checker app, seven participants searched in the App Store using the following terms: "root checker," "root checking," "jailbreaker," "jailbreak checker," "root checker app," "rooted," "root," "security check," "stalk," and "stalker." The most prominent app results for searches containing "root checker" and "jailbreak" were game apps. Four participants used web searches to look for a root checker app, and three of these said they would download apps mentioned in search results. However, these apps were either no longer available on the App Store or not able to detect jailbroken status. Two participants suggested that tutorial videos they discovered in their web searches would lead to a root checker app.

4.4.3 Finding Cydia and Resetting the Phone

In the last nine interviews of our study, participants followed Avast's two-step online advice to: 1) check for the Cydia app, and 2) restore factory settings.

Finding Cydia. Eight participants used the iOS search bar to search for Cydia, an alternative app store for jailbroken iPhones. When Cydia did not appear in search results, five participants concluded that the app was not installed on the phone, but three participants were unsure whether it was installed or not. P14 and P17 appeared to think they were searching for Cydia in order to use it and suggested we download Cydia.

Restoring Factory Settings. To follow the advice's second instruction, to "restore factory settings," six of nine participants selected the "Reset All Settings" option, which does not delete apps or data, rather than "Erase All Content and Settings," which does, from the iOS Reset menu. The article used the phrase "restore to factory settings," but there is no menu or option using the word "factory setting" or "factory reset." Five participants suggested that the wording of the

advice as well as of the iOS reset menus made implementing the instruction more difficult.

> *I would expect it to say factory reset and not have three different options that look very similar. (P17)*

5 Discussion

In this section, we discuss usability challenges in Google Maps and iOS, recommendations to mitigate these challenges, the importance of effective online advice, and how our findings underscore the existing need for usable security options to detect and counter stalking and technology-enabled abuse.

Most of our recommendations focus on preventing easily exploitable threats (e.g., location sharing), since abusers often resort to unsophisticated attacks [22, 33, 35, 62]; one recommendation, to improve Reset options, targets sophisticated attacks (jailbreaking). Implementing better status indicators or persistent notifications of transmission of data to other users would likely have the most impact on users' ability to identify and remediate threats, since adversaries would be less able to leverage common or native apps. Such recommendations are in line with Jakob Nielsen's heuristic, "visibility of system status" [27], which emphasizes communicating current status "to keep users informed about what is going on, through appropriate feedback within reasonable time" and building trust by ensuring that "no action with consequences to users should be taken without informing them."

5.1 Usability Challenges

Our findings highlight usable security problems in Google Maps and iOS settings. While participants were relatively familiar with security risks, resolving security problems proved to be difficult or unintuitive. Despite iOS and app updates since we conducted our interviews, the features we explored (Google Maps' Location Sharing, iOS Apple ID/iCloud device list, and iOS Reset and Location Services menus) have remained essentially the same from April 2021 through June 2022 (iOS 14.5 through iOS 15.5).

5.1.1 Google Maps Usability Issues

In a threat model that assumes physical or remote access to a phone, an abuser can enable surveillance by misusing legitimate apps, such as navigation apps like Google Maps. Indeed, while Google bans stalkerware, which it defines as "[c]ode that collects and/or transmits personal or sensitive user data from a device without adequate notice or consent and doesn't display a persistent notification that this is happening," such navigation apps (Google Maps, Waze, Find My) do not provide persistent notifications that location is being transmitted to another user [9]. All participants had difficulty detecting another person's real-time access to the device's location, as they did not check settings in Google Maps. Seven of them needed help locating the Location Sharing feature within Google Maps. Below, we make recommendations for how security, notifications, and transparency could be improved to alert users that their real-time location is being shared.

Authentication. Google Maps does not require users to re-authenticate to share their real-time location with another user by adding a New Share. This enables anyone with access to the phone to begin sharing with another user. The security of the device owner could be improved by requiring authentication to enable location sharing with a New Share.

Notifications. When a Google Maps user begins sharing their location with someone, two email notifications are immediately sent, one to the user and one to the contact with whom they're sharing, and a periodic email notification is sent to the user. While these are helpful, users who do not check their email often or at all, or whose notifications may have been deleted, could benefit from persistent notifications or periodic ones in different forms, e.g., SMS or in-app notifications.

Indicators. Upon opening the Google Maps app, there are no indicators that location is currently being shared. Users have to take the initiative to check the "Location Sharing" settings. To improve transparency, an indicator could alert users to the fact that they are currently sharing their location with someone. Some participants recommended such an "immediate indicator" (P6), e.g., a "glowing button" (P8).

While system status notifiers, persistent or periodic notifications, and security suggestions may be inconvenient for some users, if acted upon, they would reduce some range of opportunities for malicious parties to exploit apps for spying.

5.1.2 iOS UI Usability Issues

We identified some opportunities to improve the iOS UI's usability for people who are concerned about stalking.

Apps Using Location Services. iOS takes steps to protect users who use Location Services, by providing indicators during usage as well as periodic notifications about background location use [3]. However, none of the participants found it intuitive to investigate within-app settings in Google Maps (Scenario 1). iOS could further help users by informing them that apps using Location Services may be able to share the location with other people (even when only in limited modes, such as "While Using the App") and by recommending that users periodically check location settings within apps. While it would be impractical to catalog how to investigate settings in all apps, at least informing users of the possibility of location sharing could improve user awareness.

No Indicators of Devices in iOS App Settings. In Scenario 3, participants missed critical information about an unknown device because the Photos and iMessage app settings' UIs did not indicate that there was another device accessing the app data. Without our hint(s), many participants could not figure out that an unknown device was making changes in

the Photos and iMessage apps, and 16 participants required some hints to find the list of devices logged into the iCloud account. We recommend adding indicators regarding device access and activity within app settings.

Additionally, the list of logged-in devices and the "Remove Device" feature were placed at the bottom of their respective UI screens, which requires users to scroll down. Such critical information would ideally be more immediately visible.

Multiple Reset Options. In Scenario 4, participants struggled to choose between various reset options. There are six reset options in the reset menus of iOS 14 and iOS 15. Only upon selecting an option is a user given more information. We suggest providing clearer information to users about the differences between the reset options, especially regarding the difference between "Reset All Settings" and "Erase All Content and Settings." Given that the latter option could potentially undo the changes made to the phone's operating system by jailbreaking, while the former would not, highlighting the differences in an accessible way would make a considerable difference in a safety-critical situation.

Changes in iOS 15 and 16. Though iOS 15, released in September 2021, still has the issues we identified (e.g., multiple reset options), the "Record App Activity" feature in iOS Privacy Settings, which allows users to save a 7-day summary of when apps access their data, may help users identify apps using location or camera data and become more aware of app capabilities and activity. Apple announced in June 2022 that iOS 16 will include a tool called Safety Check, designed to help IPV victims revoke an abuser's access to location and data [10]. This seems likely to address unknown or unwanted iCloud logins and privacy permissions, but it is unclear if it could revoke non-Apple apps' within-app permissions. We encourage researchers and advocates to investigate whether these are usable security tools for victims of IPV and stalking.

5.1.3 Effective Communication and Advice

Participants had difficulty implementing advice to find a "root checker app" or "restore factory settings," due to a lack of clear explanations and implementable instructions to end users about security.

Online Advice. All participants struggled to implement the FTC's advice to find a root checker app. As there do not appear to be apps in the Apple App Store that are marketed as "root checker apps," and Apple does not support a jailbreak detection feature for app developers [1], it does not seem practical to recommend that iPhone users seek out such apps. Additionally, it may be helpful to clarify which operating systems "rooting" and "jailbreaking" are associated with.

Though participants found the Avast article's instructions relatively easy to implement, several encountered difficulty following the instruction to "restore factory settings." We recommend that in online advice, instructions should match the language on the UI and should be updated to reflect changes in the UI. In this case, it would help to note that the relevant option is "Erase All Content and Settings."

Understanding Spyware and Its Many Forms. Additionally, given that three participants defined spyware as something beneficial that could protect them against online privacy or security threats, we discovered a potential issue with the term "spyware." More research is needed on how to communicate effectively using computer security terms.

5.2 Including the Stalking Threat Model

Our study highlights the importance of including the stalking threat model in usable security design and research, i.e., focusing not only on use but also abuse of technology. Even though some of our participants suggested turning off certain settings as a solution, survivors should not have to give up using technology that may be essential to them, such as navigation apps [39]. As expected, most of our participants did not consider the risk of escalation, and some even gave advice to confront the abuser. The stalking threat model could be used to develop usable and intuitive UIs that help users safely detect and combat technology-enabled abuse and stalking.

Psychological Factors. While we did not interact with self-identifying victims of trauma, the confusion that our non-tech savvy participants expressed suggests that solving the problems we presented may be stressful.

> *After doing all these tasks, I just feel honestly a bit overwhelmed, but you know, good learning experience. . . . It's just that I don't know anything, and . . . it was a little like, a lot of booby traps. And yeah, it was just confusing, very, very confusing. (P12)*

IPV and stalking victims experiencing trauma might also feel overwhelmed, likely more than our participants, as they try to detect surveillance. Usable tools and interfaces could make the process of detecting surveillance less difficult and confusing, and thereby perhaps cause less undue stress. While technology is a vector for abuse, it can also be a tool for survivors to enhance and maintain their safety.

6 Conclusion

This study focused on the qualitative analysis of 18 semi-structured interviews in which participants responded to four simulated-risk mobile phone security scenarios.

In four realistic scenarios simulating stalking and surveillance, the majority of non-tech savvy participants encountered significant usable security challenges, failing to use iOS and Google Maps UIs to detect and resolve security compromises. We recommend that companies make improvements to their interfaces and that writers of online security articles ensure their advice is clear and implementable. More research is needed on developing usable security tools and options to better detect and counter technology-enabled abuse.

Acknowledgments

This research was funded in part by the first author's GEM fellowship. We would also like to thank Sarah Pearman, Kevin Kim, and Chanaradee Leelamanthep for their work on an earlier version of this study.

References

[1] Jailbroken detection check without App Store rejection. https://developer.apple.com/forums/thread/66363?answerId=191199022#191199022, Oct 2016.

[2] Abuse of trust: How to identify and remove stalkerware. https://nordvpn.com/blog/how-to-identify-stalkerware/, Jul 2019.

[3] About privacy and location services in iOS and iPadOS. https://support.apple.com/en-us/HT203033, Feb 2021.

[4] Citizen Clinic - CLTC UC Berkeley Center for Long-Term Cybersecurity. https://cltc.berkeley.edu/about-us/citizen-clinic/, 2021.

[5] Detecting and removing stalkerware. https://goaskrose.com/stalkerware/, 2021.

[6] Safety net apps. https://www.techsafety.org/safetynetapps, 2021.

[7] Stalkerware: Understanding and stopping technology-facilitated domestic violence. https://staysafeonline.org/wp-content/uploads/2021/04/Stalkerware-Tip-Sheet-2021.pdf, 2021.

[8] Stalking apps: What to know. https://www.consumer.ftc.gov/articles/stalking-apps-what-know, May 2021.

[9] Developer Program Policy - Play Console Help. https://support.google.com/googleplay/android-developer/answer/11987217?hl=en&ref_topic=9877065, May 2022.

[10] Keynote - WWDC22 - Videos. https://developer.apple.com/videos/play/wwdc2022/101/, Jun 2022.

[11] Laura Brignone and Jeffrey L. Edleson. The dating and domestic violence app rubric: synthesizing clinical best practices and digital health app standards for relationship violence prevention smartphone apps. *International Journal of Human–Computer Interaction*, 35(19), 2019.

[12] Carly Burdova. What is jailbreaking and is it safe? https://www.avast.com/c-jailbreaking#topic-6, May 2021.

[13] Rahul Chatterjee, Periwinkle Doerfler, Hadas Orgad, Sam Havron, Jackeline Palmer, Diana Freed, Karen Levy, Nicola Dell, Damon McCoy, and Thomas Ristenpart. The spyware used in intimate partner violence. In *2018 IEEE Symposium on Security and Privacy (SP)*, 2018.

[14] Jacqueline Connor. Who's stalking: what to know about mobile spyware. https://staysafeonline.org/blog/whos-stalking-know-mobile-spyware/, Oct 2016.

[15] Jacqueline Connor. Who's stalking: what to know about mobile spyware. https://www.consumer.ftc.gov/blog/2016/09/whos-stalking-what-know-about-mobile-spyware, Sep 2016.

[16] Nicki Dell, Karen Levy, Damon McCoy, and Thomas Ristenpart. How domestic abusers use smartphones to spy on their partners. *Vox*, May 2018.

[17] Melanie P. Duckworth and Victoria M. Follette. *Retraumatization: Assessment, treatment, and prevention*. Routledge, 2012.

[18] Brett Eterovic-Soric, Kim-Kwang Raymond Choo, Helen Ashman, and Sameera Mubarak. Stalking the stalkers – detecting and deterring stalking behaviours using technology: A review. *Computers & Security*, 70:278–289, 2017.

[19] Blake Flournoy. How to check if an iPhone has been jailbroken. https://www.techwalla.com/articles/how-to-check-if-an-iphone-has-been-jailbroken, Dec 2018.

[20] Lorenzo Franceschi-Bicchierai. Inside the "stalkerware" surveillance market, where ordinary people tap each other's phones. *WIRED*, Apr 2017.

[21] Cynthia Fraser, Erica Olsen, Kaofeng Lee, Cindy Southworth, and Sarah Tucker. The new age of stalking: Technological implications for stalking. *Juvenile and Family Court Journal*, 61(4), 2010.

[22] Diana Freed, Sam Havron, Emily Tseng, Andrea Gallardo, Rahul Chatterjee, Thomas Ristenpart, and Nicola Dell. "Is my phone hacked?" Analyzing clinical computer security interventions with survivors of intimate partner violence. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW), Nov 2019.

[23] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. "A stalker's paradise": How intimate partner abusers exploit technology. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, Apr 2018.

[24] Diana Freed, Jackeline Palmer, Diana Elizabeth Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. Digital technologies and intimate partner violence: A qualitative analysis with multiple stakeholders. *Proceedings of the ACM on Human-Computer Interaction*, 1(CSCW), Dec 2017.

[25] Jessica R. Goodkind, Tameka L. Gillum, Deborah I. Bybee, and Cris M. Sullivan. The impact of family and friends' reactions on the well-being of women with abusive partners. *Violence Against Women*, 9(3):347–373, 2003.

[26] Diarmaid Harkin and Adam Molnar. Operating-system design and its implications for victims of family violence: The comparative threat of smart phone spyware for android versus iPhone users. *Violence Against Women*, 27(6-7):851–875, 2021.

[27] Aurora Harley. Visibility of system status. *Nielsen Norman Group*, Jun 2018.

[28] Tirion Elizabeth Havard and Michelle Lefevre. Beyond the power and control wheel: How abusive men manipulate mobile phone technologies to facilitate coercive control. *Journal of Gender-Based Violence*, 4(2):223–239, Jun 2020.

[29] Sam Havron, Diana Freed, Rahul Chatterjee, Damon McCoy, Nicola Dell, and Thomas Ristenpart. Clinical computer security for victims of intimate partner violence. In *28th USENIX Security Symposium (USENIX Security 19)*, Aug 2019.

[30] Tad Hirsch. Practicing without a license: Design research as psychotherapy. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 2020.

[31] Alison Grace Johansen. Is jailbreaking legal and safe? https://us.norton.com/internetsecurity-mobile-is-jailbreaking-legal-and-safe.html, Mar 2019.

[32] Cynthia Khoo, Kate Robertson, and Ronald Deibert. *Installing Fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications*. Number 20 in Citizen Lab Research. Jun 2019.

[33] Roxanne Leitão. Digital technologies and their role in intimate partner violence. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*, 2018.

[34] Roxanne Leitão. Technology-facilitated intimate partner abuse: a qualitative analysis of data from online domestic abuse forums. *Human–Computer Interaction*, 36(3), 2021.

[35] Tara Matthews, Kathleen O'Leary, Anna Turner, Manya Sleeper, Jill Palzkill Woelfer, Martin Shelton, Cori Manthorne, Elizabeth F. Churchill, and Sunny Consolvo. Stories from survivors: Privacy & security practices when coping with intimate partner abuse. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 2017.

[36] Nick Mooney. Jailbreak detector detector: An analysis of jailbreak detection methods and the tools used to evade them. https://duo.com/blog/jailbreak-detector-detector, Jan 2019.

[37] James Nicholson, Lynne Coventry, and Pamela Briggs. "If it's important it will be a headline": Cybersecurity information seeking in older adults. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 2019.

[38] David Nield. How to check your devices for stalkerware. *WIRED*, Jul 2020.

[39] Erica Olsen. Device and account security in safety planning for relocation with NortonLifeLock. https://vimeo.com/631313869/ab089b7b24, Oct 2021.

[40] Cheul Young Park, Cori Faklaris, Siyan Zhao, Alex Sciuto, Laura Dabbish, and Jason Hong. Share and share alike? An exploration of secure behaviors in romantic relationships. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, Aug 2018.

[41] Christopher Parsons, Adam Molnar, Jakub Dalek, Jeffrey Knockel, Miles Kenyon, Bennett Haselton, Cynthia Khoo, and Ronald Deibert. The predator in your pocket: A multidisciplinary assessment of the stalkerware application industry. Citizen Lab Research Report No. 119. Jun 2019.

[42] Elissa M. Redmiles, Sean Kross, and Michelle L. Mazurek. How I learned to be secure: A census-representative survey of security advice sources and behavior. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016.

[43] Elissa M. Redmiles, Noel Warford, Amritha Jayanti, Aravind Koneru, Sean Kross, Miraida Morales, Rock Stevens, and Michelle L. Mazurek. A comprehensive quality evaluation of security and privacy advice on the web. In *29th USENIX Security Symposium (USENIX Security 20)*, Aug 2020.

[44] L. E. Rose, J. Campbell, and J. Kub. The role of social support and family relationships in women's responses to battering. *Health Care for Women International*, 21(1):27–39, Feb 2000.

[45] Kevin A. Roundy, Paula Barmaimon Mendelberg, Nicola Dell, Damon McCoy, Daniel Nissani, Thomas Ristenpart, and Acar Tamersoy. The many kinds of creepware used for interpersonal attacks. In *2020 IEEE Symposium on Security and Privacy (SP)*, 2020.

[46] Aarti Shahani. Smartphones are used to stalk, control domestic abuse victimes. *NPR*, Sep 2014.

[47] Cynthia Southworth, Jerry Finn, Shawndell Dawson, Cynthia Fraser, and Sarah Tucker. Intimate partner violence, technology, and stalking. *Violence Against Women*, 13(8):842–856, Aug 2007.

[48] Evan Stark. *Coercive Control: How Men Entrap Women in Personal Life*. Oxford University Press, Mar 2009.

[49] Kateryna M. Sylaska and Katie M. Edwards. Disclosure of intimate partner violence to informal social support network members: A review of the literature. *Trauma, Violence & Abuse*, 15(1):3–21, Jan 2014.

[50] Shashank Thakur. How to detect if an iOS device is jailbroken. https://hackernoon.com/how-to-detect-if-an-ios-device-is-jailbroken-263u3tdj, Oct 2020.

[51] National Network to End Domestic Violence. App safety considerations for survivors of abuse. https://www.techsafety.org/resources-survivors/app-safety-considerations, 2014.

[52] National Network to End Domestic Violence. Technology safety plan: A guide for survivors and advocates. https://www.techsafety.org/resources-survivors/technology-safety-plan, 2018.

[53] Emily Tseng, Rosanna Bellini, Nora McDonald, Matan Danos, Rachel Greenstadt, Damon McCoy, Nicola Dell, and Thomas Ristenpart. The tools and tactics used in intimate partner surveillance: An analysis of online infidelity forums. In *29th USENIX Security Symposium (USENIX Security 20)*, August 2020.

[54] Sarah Turner, Jason Nurse, and Shujun Li. When googling it doesn't work: The challenge of finding security advice for smart home devices. In *International Symposium on Human Aspects of Information Security and Assurance*, pages 115–126, 2021.

[55] Jennifer Valentino-DeVries. Hundreds of apps can empower stalkers to track their victims. *The New York Times*, May 2018.

[56] Jodie Valpied, Abigail Cini, Lorna O'Doherty, Ann Taket, and Kelsey Hegarty. "Sometimes cathartic. sometimes quite raw": Benefit and harm in an intimate partner violence trial. *Aggression and Violent Behavior*, 19(6):673–685, 2014. Violence and Health: Current Perspectives from the World Health Organization (WHO) Violence Prevention Alliance.

[57] Douglas M. Walls, Brandy Dieterle, and Jennifer Roth Miller. Safely social: User-centered design and difference feminism. *Composing Feminist Interventions*, page 391, 2018.

[58] Kaitlyn Wells and Thorin Klosowski. Domestic abusers can control your devices. Here's how to fight back. *The New York Times*, April 2020.

[59] Rhiannon Williams. Google is failing to enforce its own ban on ads for stalkerware. *MIT Technology Review*, May 2022.

[60] Taylor Paige Winfield. Vulnerable research: Competencies for trauma and justice-informed ethnography. *Journal of Contemporary Ethnography*, 51(2), 2022.

[61] Delanie Woodlock. The abuse of technology in domestic violence and stalking. *Violence Against Women*, 23(5):584–602, 2017.

[62] Delanie Woodlock, Mandy McKenzie, Deborah Western, and Bridget Harris. Technology as a weapon in domestic violence: Responding to digital coercive control. *Australian Social Work*, 73(3):368–380, Jul 2020.

A Appendix - Interview Questions

A.1 Scenario 1

In this first scenario, imagine your coworker tells you that they think someone is tracking their location through their phone. They show you their screen and ask you to help them find out if this is happening.

1. Could you guide us through how you would confirm whether someone is tracking your coworker's location?
    - HINT 1: Where in the phone settings could you go to find the source of location sharing?
    - HINT 2: If we go to the Privacy settings, is there anything here that we could do to find the potential source of location sharing, since your coworker wants to confirm whether or not it is happening? We see here a list of apps, and it looks like the app sharing location is Google Maps.
    - HINT 3: We see that Google Maps is tracking their location, but your coworker needs to use Google Maps to get places and doesn't want to turn location services off. Let's check the settings in Google Maps. What would you inspect here, in the app, to see if location is being shared with someone else?
    - HINT 4: Let's take a look at this drop-down menu when clicking the circle here. Is there anything here that might help?
    - SOLUTION: The last step is . . . to go to this option, Location sharing, and you can see that they're sharing their location with Mallory.
2. How easy or difficult was it to find the source of location sharing? Could you tell us why?
3. Your friend wants to stop sharing their location. What directions would you give to your friend to stop the location sharing?
4. How easy or difficult was it to stop the location sharing? Could you explain why?
5. Have you encountered the Google Maps app before?
6. After stopping location sharing, would you suggest your coworker do anything else or take any other actions?
7. If you thought your location was being tracked, like in this situation, what would you do?
    - (If they don't mention what steps they would take) Would you follow the same steps or do it differently?
    - Would you ask for advice? Who would you ask or where would you go for advice?

A.2 Scenario 2

Now, we'll move on to scenario two.

1. In your own words, what do you think spyware is?

   Imagine your friend suspects that their significant other has "hacked" their phone. It seems like they have knowledge about messages, emails, downloaded apps, and other information. Even though they share passwords, your friend rarely leaves their phone out of reach, so they don't know when their partner would have had the time to look at this information. Your friend asks you for advice on finding out whether their significant other is remotely accessing their device.
2. What directions would you give your friend to see whether there is spyware or not on their phone?
    - HINT 1: While some spyware can be hidden, in this scenario, the spyware is an app that was downloaded from the app store. How can you tell if one of your friend's apps might be spyware?
    - HINT 2: We could review all your friend's apps. One way to do this is to look at the app library by swiping right on the home screen.
    - HINT 3: We are looking for an application that enables remote access to the device, not the one that has potential security vulnerabilities. Are you familiar with such remote access apps?
3. What are/were you looking for when you are/were looking for an app that can be used as spyware?

   Now you and your friend search through every single app on the phone. Your friend points out this app, TeamViewer. Your friend has never used this app, and they remember that their significant other put this app on their phone, falsely claiming it was an antivirus. TeamViewer is what we call a dual-use app that can be used to share the screen, but also can be used as spyware. This app allows another person to temporarily control the device.
4. Were you familiar with the app, TeamViewer?
5. How easy or difficult was it to identify the spyware app? Could you tell us why?
6. After finding out that TeamViewer was being used to remotely access the device without your friend's permission, what precautions or advice would you suggest that your friend keep in mind?
7. Your friend decides that it is safe to remove the spyware. What steps would you take to remove the app?
8. How easy or difficult was it to remove the spyware app? Cloud you tell us why?

9. After removing the app, would you advise your friend to do anything else?
10. Let's say the phone settings had been changed or tampered with, what could your friend do to make sure they were changed back?
11. If you suspected someone "hacked" your phone, What would you do?
    - (If they don't mention what steps they would take) Would you follow the same steps or do it differently?
    - Would you ask for advice? Who would you ask or where would you go for advice?

A.3 Scenario 3

So now we will move on to secenario 3.

1. What do you think it means when your account is compromised? Imagine that you and a different friend suspect that someone has access to photos they have stored on their iPhone. Some of their photos disappear, and new photos they didn't take appear in their albums. Your friend also notices that new iMessages are appearing, which they never sent. Your friend asks you to help them figure out what is going on.
2. What are some steps you could take to figure out whether someone can see your friend's photos and messages? Could you walk me through this? (What are you looking for?)
    - HINT 1: Your friend says they used to sync their photos and messages onto other devices, but they're not sure how this works. Through what account might this be happening?
    - HINT 2: So we figure out it's probably happening through iCloud account syncing with another device. Where can we go on the phone to check on other devices logged into the iCloud account?
    - HINT 3: Let's go to the iCloud account settings by clicking on [Apple ID/iCloud account settings]. Is there somewhere here where you might find the list of devices?
    - SOLUTION: If we scroll down, we can see that another device is logged in. This is the source of the photo and message syncing.

    You and your friend figure out that their iCloud account is synced with another device. Your friend says they don't recognize this device.
3. How easy or difficult was it to find the other device? Could you tell us why?
4. What are the steps you would tell your friend to take to remove the other person from the iCloud account?
5. How easy or difficult was it to remove the other device? Could you tell us why?
6. Would you recommend anything else to your friend?
7. If you thought your iCloud account was compromised, what would you do?
    - (If they don't mention what steps they would take) Would you follow the same steps or do it differently?
    - Would you ask for advice? Who would you ask or where would you go for advice?

A.4 Scenario 4 Version 1

1. What do you think "rooted" or "jailbroken" means? Imagine your friend tells you they think they are being stalked by a coworker, and they went to this FTC website: https://www.consumer.ftc.gov/blog/2016/09/whos-stalking-what-know-about-mobile-spyware. Your friend shows you this part, titled "What can I do if I think a stalking app is installed on my phone?" (see Appendix B.1). They ask you about the second option, "Check to see if your phone has been rooted or jailbroken." Please let us know after you have read through that part the text.

    Now, your friend tells you that they want to follow the website's advice and check whether their phone is rooted or jailbroken. They ask for your help finding the kind of app mentioned on the website.
    - Is the meaning of rooted or jailbroken clear from the advice?
    - In your own words, what do you think it means when a person gets full control of the operating system?
    - Can you identify the website's recommendation for people who think a stalking app might be installed on their phone?
2. How would you help your friend find the kind of app mentioned on the website?
3. (If they find apps) Would you recommend any of these apps to your friend? Why or why not?
4. What would your criteria be for recommending a root checker app to your friend?
5. How practical do you think the FTC website's advice to find an app, on a scale from 1 to 5, 1 being very easy to implement and 5 being very difficult to implement? Why did you give this rating?

A.5 Scenario 4 Version 2

1. What do you think "rooted" or "jailbroken" means? Now imagine that your friend tells you that they think their iPhone is jailbroken, and they went to this Avast website: https://www.avast.com/c-jailbreaking#topic-6. Please read this section called, "What does jailbreaking an iPhone do?" (see Appendix B.2.1) and let us know after you have read through that part of the text.
    - Is the meaning of "jailbroken" clear from the text?
    - In your own words, what do you think "modifies the operating system" means?
    - In your own words, what do you think giving "unauthorized root access" means?

    Your friend then shows you this part, starting with: "Nevertheless, if you think you have a jailbroken iPhone, there are some things you can do" (see Appendix B.2).
2. Can you identify the website's recommendations for people who think their iPhone may be jailbroken?
3. Your friend wants to look for Cydia first. How would you do this?
    - HINT: Search for apps using search bar in settings, search bar, or on home screen
4. It looks like Cydia is not on the phone. Your friend now wants to follow step two, which suggests performing a factory reset. Can you help your friend do this?
    - HINT: The option may be in Settings
    - HINT: We could look in "General" settings.
    - HINT: At the bottom, there is a "Reset" option.
    - HINT: Restoring to factory settings means deleting all data and settings. Which option here would do that?
5. Have you encountered this [reset menu] screen before?
6. How easy or difficult was the process of looking for Cydia? Could you tell us why?
7. How easy or difficult was the process of doing a Factory Reset? Could you tell us why?
8. How straightforward or easy to follow were the instructions provided by the website? Could you tell us why?
9. If you thought your phone was jailbroken and wanted to check your device, what would you do?
    - (If they don't mention what steps they would take) Would you follow the same steps or do it differently?
    - Would you ask for advice? Who would you ask or where would you go for advice?

B Appendix - Online Advice for Jailbreak Detection (Scenario 4)

Below are excerpts from Scenario 4's online advice articles.

B.1 Advice to Find a Root Checker App.

Our study used advice from a now unavailable FTC blog post, which directed people who suspect they are being stalked to download a "root checker app," in order to detect whether their phone is rooted or jailbroken [15]:

> **Check to see if your phone has been "rooted" or "jailbroken."** Stalking apps aren't sold through typical app stores. In addition, they usually can be installed only on a phone that has been "rooted" or "jailbroken," which allows a person full control over the phone's operating system. If your phone is rooted or jailbroken and you didn't do it, a stalking app could be installed. "Root checker" apps can quickly tell you whether a phone has been rooted or jailbroken.

Since beginning this study, the FTC published an article about stalking apps containing similar advice [8]:

> **Check to see if your phone has been "rooted" or "jailbroken."** Stalking apps can be installed only on a phone that has been "rooted" or "jailbroken," which gives a person full control over the phone's operating system. "Root checker" apps can quickly tell you whether a phone has been rooted or jailbroken. But if there is stalkerware on the device, the abusive person may see this activity. If you find that your phone has not been rooted or jailbroken, but the person knows more than they should about your phone or online activities, it may be that they are getting that information from your phone another way.

B.2 Advice to Find Cydia and Reset

In the second version of the interview, advice from Avast [12] was presented to the participants. The article recommends some actions readers can take if they think their iPhone may be jailbroken. We showed the participants two parts: 1) the section called "What does jailbreaking an iPhone do?" B.2.1 that explains jailbreaking and what it allows the users to do on their device, and 2) the section called "Can you tell if a phone has been jailbroken?" that has instructions we asked participants to follow B.2.2.

B.2.1 What does Jailbreaking an iPhone do

Jailbreaking an iPhone **modifies the operating system**, giving you **unauthorized root access** to the jailbroken device's

core software and structure. So, what can you do with a jailbroken iPhone? Besides slipping through the wormhole to the underground jailbreaking community, and potentially exposing your device to hackers and viruses, there are some reasons why jailbreaking an iPhone or other iOS device might be desirable. With a jailbroken phone, you can:

- Freely do as you please with your phone or tablet.
- Access third-party apps outside the official App Store.
- Customize and personalize your phone and its settings more deeply.
- Unlock carrier restrictions.

B.2.2 Can you tell if a phone has been jailbroken?

Nevertheless, if you think you have a jailbroken iPhone, there are some things you can do.

1. Find Cydia: On your iPhone, search for Cydia, the alternative app store. Even if it's hidden, this search will find the app. If Cydia is there, it's a jailbroken phone.

2. Restore factory settings: If you don't want to worry about whether or not your phone was jailbroken, an easy way around is to restore factory settings. Restoring factory settings brings back whatever may have been lost to jailbreaking.

C Appendix - Demographics

Our screening survey included questions about age, gender, race/ethnicity[2], education[3], computer science and/or internet technology (CS/IT) education, CS/IT work experience, and income. Only P4 had CS/IT education and CS/IT work experience.

ID	Age	Gender	Race	Education	Income
P1	57	F	W	M	$60-70k
P2	22	F	W	SC	$20-30k
P3	34	F	W	M	$20-30k
P4	75	M	AS	P	Prefer not to respond
P5	23	F	AS	B	$10-20k
P6	36	M	AS	B	$50-60k
P7	50	M	AS	B	$60-70k
P8	26	M	H, W	B	$70-80k
P9	36	F	H, NL	B	$90-100k
P10	37	F	W	B	$100-150k
P11	24	M	W	B	$50-60k
P12	22	F	H, W	B	$90-100k
P13	22	F	AS	B	$90-100k
P14	24	F	AA, H	A	$\leq$ $10k
P15	27	M	AS	B	$10-20k
P16	19	F	AA, W	SC	$70-80k
P17	23	M	AA	B	$40-50k
P18	30	M	H, NL	M	$50-60k

[2]Race/ethnicity: AA = African American/Black, AS = Asian, H = Hispanic/Latino/Latina/Latinx, W = White, NL = Not Listed

[3]Education: A = Associate's degree (2-year), B = Bachelor's degree (4-year), M = Master's degree, P = Professional degree (JD, MD), SC = Some college, no degree

D Appendix - Codebook

Category	Codes	Definition	Scenario(s)	Participant Count
Advice Given by Participant	backup	Back up photos/messages	S3	1
	blocking	Block the person who was tracking the location	S1	1
	change passcode	Change password	S2, 3	3, 9
	confrontation	Directly confront the person responsible for stalking or surveillance, e.g. find the stalker, have a conversation with abusive partner	S1, 2	1, 5
	consult personal contact	Ask friends, family members, or personal contacts for advice; tech savvy personal contacts - could be in negative form (e.g. don't know anyone to consult)	S1, 2, 3, 4.2	2, 4, 2, 2
	consult police	Consult police or law enforcement	S1, 2	1
	delete app	Delete the app	S2	9
	delete more	Take more steps to delete the app, beyond just removing app (deleting app purchase history, deleting from cloud, deleting it from the other phone, etc)	S2	7
	do nothing	Would not advise the friend to do anything else	S1, 2, 3	4, 2, 1
	don't allow	Do not let other people take some action (e.g. download an app on your device)	S2	10
	internet	Use internet (search engine, forums, YouTube)	S1, 2, 3, 4.2	5, 5, 6, 6
	investigate	Find out how the situation happened and conduct test to look into the issue	S1, 2	1, 10
	log out	Log out other devices from the iCloud account	S3	1
	manual check	Go through settings manually and change them back	S2	9
	mfa	Use multi-factor authentication	S2, 3	1, 2
	monitoring	Regularly check and review apps, settings, details, and/or logged in devices	S1, 2, 3	6, 10, 7
	no advice	Wouldn't ask for advice	S1, 3, 4.2	2, 3, 3
	other apps	Check or change settings on other apps (e.g. social media or messaging apps)	S1	2
	remove device	Remove device from iCloud setting (suggested this before being prompted)	S3	2
	reset	Reset the device	S2, 3	10, 1
	restart the phone	Turn off phone and turn it back on	S1, 2, 3	2, 2, 2
	tech support	Consult customer service	S1, 2, 3, 4.2	2, 4, 3, 3
	turn off location service & bluetooth	Set location service setting to "Not Allow" and turn off bluetooth	S3	1
	VPN	Use a VPN	S1, 2	1,4
Criteria for recommending a root checker app to your friend?	ask device owner	Would ask device owner what they were ok with	S4.1	1
	internet	Would search online for an app	S4.1	8
	privacy	Apps should be clear about how personal informatio is being used	S4.1	1
	security	App itself should be secure	S4.1	1
	user review	Many views on a video, good feedback/review for the app	S4.1	2
	videos	Would watch videos to get information leading to a root checker app	S4.1	4
Difficulty	clear or simple	The advice was clear or simple to participants; easy to understand	S4.2	7
	confused	Participant stated they were confused	S2	3
	deleting is easy	All participants found removing the app to be easy	S2	18
	difficult	Resolving the problem was difficult.	S2, 3, 4.1	14, 8, 3
	don't know	Participant said they did not know or had no idea	S1, 2, 3	9, 14, 8
	don't know full capability	Paritipant did not know apps' full capabilities of e.g. assumed capabilities solely by the name/logo of the app	S2	6
	easy	Resolving the problem was easy.	S1, 2, 3, 4.1, 4.2	1, 18, 17, 2, 7
	familiar app search	Participant was familiar with the process of searching for an app	S4.2	2
	familiar reset	Participant was familiar with the process to reset a device	S4.2	3
	few steps	Process did not take many steps	S1, 3	2, 3
	find-source difficult	Finding the source of location sharing is the Google Maps was difficult.	S1	8
	find-source easy	Finding the source of location sharing is the Google Maps was easy.	S1	3
	find-source moderate	Finding the source of location sharing is the Google Maps was moderate.	S1	5
	frustrated	Ready to give up, struggled, expressed frustration or exasperation	S2	1
	hard to find	Participant appeared to struggle to find the right options/settings (observation)	S1, 2, 3	4, 9, 10
	if I knew	After getting the hint or being shown the solution, participants said they would have found it easy to resolve the problem, if they had known this	S1, 2, 3, 4.2	9, 5, 5, 2
	interview format limitation	Limitations caused by the interview formation: not being able to control screen, not recognizing emails or user IDs	S1, S3	2, 5
	intuitive	Process was self-explanatory, easy	S1	6
	many steps	Process took a lot of steps	S1	4
	moderate	Resolving the problem was neither easy or difficult.	S2, 4.1, 4.2	2, 3, 3

	not me	Problem is not personally relevant (e.g. never thought someone tracking me, i'm not that interesting, haven't experience this before)	S1, S2	2, 2
	obvious label	The settings menu/option is easily recognizable and comprehensive (e.g., red big bold "remove" [button])	S3	6
	order	Participant found the order in the instructions helpful	S4.2	1
	reset is easier	Participant considered the reset step to be easier than finding the Cydia app	S4.2	1
	stop-source difficult	Stopping sharing from the Google Maps location sharing screen was difficult.	S1	1
	stop-source easy	Stopping sharing from the Google Maps location sharing screen was easy.	S1	12
	stop-source moderate	Stopping sharing from the Google Maps location sharing screen was neither easy or difficult.	S1	1
	unfamiliar	Had not heard of it or wasn't aware of the process	S2, 3, 4.2	4, 6, 2
	unfamiliar with app	Unfamiliar with TeamViewer	S2	9
	unfamiliar with reset	Didn't know how to reset device, expressed lack of familiarity with reset	S2	2
	unintuitive	Unintuitive to navigate or solve problem	S3	2
	wording	Unsure which menu options/labels to choose; found wording confusing	S4.2	5
Other	conditional	Participant's mentioned technical/personal condition or preferences e.g. depends on how paranoid they were	S1,2	2,3
	escalation	Participant mentioned personal experience relating to scenario or to the strategy used in the scenario (e.g., sharing location with family members)	S1	1
	recommendation	Recommended or imagined a feature that does not currently exist	S1, 2, 3, 4.2	4, 3, 1, 5
	study design limitation	Participant was influenced or limited by study design	S2	2
	exception	Participant mentioned social condition for exception to privacy & security advice due to trust or consent, e.g. if you trust them	S2	3
	trusted source	Mentioned that they trust the information on the website or provided by us	S4.2	3
Practicality of FTC advice	more details	Need more clarification, more elaboration, better keywords for finding app	S4.1	3
	no example	No example app given	S4.1	2
	no results	Nothing came up from search	S4.1	2
Search Keywords Used by Participant	best app to tell if your iPhone is jailbroken		S4.1	1
	best root checker app		S4.1	1
	how to check if my iPhone has been jailbroken		S4.1	1
	how to diagnose jailbroken iPhone		S4.1	1
	jailbreak checker		S4.1	1
	jailbreaker		S4.1	1
	root		S4.1	1
	root checker		S4.1	5
	root checker app		S4.1	2
	root checking		S4.1	1
	rooted		S4.1	1
	security check		S4.1	1
	stalk		S4.1	1
	stalker		S4.1	1
	add a new share	Attempted to add a new person to share location with	S1	3
	antivirus	Suggested using antivirus to solve problem	S2	1
	app store	Went to Apple's App Store to review apps	S2, 4.1	2, 7
	change location services	Changed location service settings, e.g. from Always to Never, or Precise Location, only while using	S1	3
	change other google maps' setting	Incognito mode, block person, go to myaccount.google.com and click X	S1	4
	change privacy settings	Suggested changing privacy settings	S2	5
	change TeamViewer app setting	Changed TeamViewer app setting (background app refresh)	S2	1
	check device list	Checked the device list	S3	1
	concluded there's no app	Concluded that Cydia is not installed on the device	S4.2	5
	confused by other apps	Confused by many unfamiliar apps, also includes participants who mistakenly identified HackIt or other app as spyware	S2	4
	confused by other features in an app	Confused by other Google Maps features, e.g., click "fix" for notifications pop-up, clicked blue arrow	S1	6
	control center	Suggested looking at Control Center settings in iOS	S1	1
	download Cydia	Suggested downloading Cydia or using an alternate app store to find it	S4.2	2

Participant Strategy	engage with suspicious app	Engaged with (opened or tried to sign up for) a suspicous or unknown app	S2	5
	Erase All Content and Settings	Chosen reset option	S4.2	3
	experience	Mentioned personal experience relating to scenario or to the strategy used in the scenario (e.g., sharing location with family members)	S1, 2, 3	1, 8, 5
	factory reset	Suggested doing a factory reset	S2	1
	false alarm	Misunderstood or got suspicious on settings that are irrelevant	S4.1	1
	familiar	Familiar with the app, feature or process	S3	4
	get rid of phone	Suggested getting rid of the phone	S2	2
	guessing	Guessed	S2	1
	hidden	Mentioned possibility of hidden apps or files	S2, 3	3, 2
	home screen	Searched for Cydia on the home screen	S4.1, 4.2	2, 2
	internet	Use internet (search engine, forums, YouTube) for strategy or advice	S4.1	8
	messages	Went into "Messages" settings	S3	3
	not my phone	Mentioned how it might be different if it were their phone, or if they need to take a look at their own phone to figure it out	S2	3
	not possible	Mentioned that doing something was not possible (e.g., finding source of iCloud login)	S3	1
	other apps	Mentioned checking or changing settings on other apps, like social media apps or messaging apps	S3	1
	other iCloud settings	Searched in iCloud settings but could not easily find device list and looked into different settings	S3	9
	password & security setting	Went into "Password and Security" iOS iCloud account setting to try to find other device	S3	4
	photos	Went into "Photos" settings	S3	12
	recognition	Asked interviewers if the friend recognizes the app	S2	5
	reset all settings	Chose "Reset All Settings" in the reset menu, which doesn't delete the entire data	S4.2	7
	scroll down in settings	How participant reviewed the apps	S2	9
	search bar	Utilized iOS search bar (from settings or home screen)	S1, 2, 4.2	2, 1, 8
	search in settings	Searched Cydia from the search bar in the Settings	S4.2	1
	settings	Searched Settings to find a root checker app	S4.1	3
	Share my location	Looked at Share My Location or Find My settings	S1	8
	shared album	Checked or commented on "Shared Albums" setting in iOS Photos settings	S3	6
	tracking	Went to "Tracking" setting	S1, 2	5, 3
	turn off location service	Turned off the location service completely	S1	11
	unsure if app is installed	Unsure whether Cydia could still be on the phone, after not finding the app	S4.2	4
What were participants looking for?	cross-app	Connection across multiple apps could be an indicator of spyware	S2	1
	data analytics	Spyware may look similar to data analytics	S2	1
	keywords	This could be an indicator of spyware	S2	5
	location sharing	This could be an indicator of spyware	S2	1
	power consumption	This could be an indicator of spyware	S2	1
	spyware finder app	Finding an app to look for spyware apps	S2	1
	weird name	Spyware app may have peculiar name	S2	2