USENIX

THE ADVANCED COMPUTING
SYSTEMS ASSOCIATION

AirTag-Facilitated Stalking Protection: Evaluating Unwanted Tracking Notifications and Tracker Locating Features

Dañiel Gerhardt, *CISPA Helmholtz Center for Information Security and Saarland University;* Matthias Fassl, *CISPA Helmholtz Center for Information Security;* Carolyn Guthoff, *CISPA Helmholtz Center for Information Security and Saarland University;* Adrian Dabrowski, *Research Center IT-Security, University of Applied Sciences FH Campus Wien;* Katharina Krombholz, *CISPA Helmholtz Center for Information Security*

https://www.usenix.org/conference/usenixsecurity25/presentation/gerhardt

This paper is included in the Proceedings of the 34th USENIX Security Symposium.

August 13–15, 2025 • Seattle, WA, USA

978-1-939133-52-6

Open access to the Proceedings of the 34th USENIX Security Symposium is sponsored by USENIX.

AirTag-Facilitated Stalking Protection: Evaluating Unwanted Tracking Notifications and Tracker Locating Features

Dañiel Gerhardt
CISPA Helmholtz Center for Information Security and Saarland University

Matthias Fassl
CISPA Helmholtz Center for Information Security

Carolyn Guthoff
CISPA Helmholtz Center for Information Security and Saarland University

Adrian Dabrowski
Research Center IT-Security, University of Applied Sciences FH Campus Wien

Katharina Krombholz
CISPA Helmholtz Center for Information Security

Abstract

Apple introduced *AirTags* in 2021 to help users find lost items. Their small size, affordability, and precise tracking functionality predestined them for technology-facilitated stalking, i.e., consentless tracking of others. As a countermeasure, Apple introduced anti-stalking features to impede misuse of AirTags: *unwanted tracking notifications* and two locating features. However, the reliability and effectiveness of these measures remain unclear.

We present two studies to evaluate unwanted tracking notifications and the tracker locating features. First, we quantify the reliability of unwanted tracking notifications on iOS and Android with $N_A = 50$ fully informed participants. Second, we present a deception study to understand $N_B = 19$ participants' reactions to an unexpected tracking notification. Additionally, we asked participants to locate a hidden AirTag to study the locating features.

We found that unwanted tracking notifications are significantly more reliable and timely on iOS than on Android. Effective and safe responses to the tracking notification depended on prior knowledge about the technology or awareness of technology-facilitated abuse. Many participants disregarded the unobtrusive warning entirely. The Find My app's confusing UI made locating the tracker harder than necessary. We recommend (i) enhancing the urgency and clarity of tracking notifications and (ii) offering a guided UX for identifying and disabling trackers.

1 Introduction

Apple AirTags are tracking devices marketed to locate lost keys or luggage. However, they are also misused for stalking and other malicious purposes [14, 22, 23]. For example, in the context of intimate partner violence, stalking is often a strategy of intimidation and control used by men to force women to remain in relationships [25]. While technology-facilitated stalking is not new [9, 13, 32], AirTags and their tracking ecosystem exacerbate the problem. AirTags are small, affordable, readily available, and allow precise tracking, making them easy-to-use and easy-to-access trackers. Their ecosystem, i.e., the *Find My* network infrastructure and the supporting software on iOS, make them powerful tracking devices.

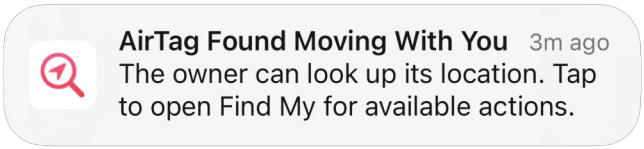

Figure 1: An unwanted tracking notification on Apple's iOS.

To reduce misuse, Apple implemented multiple anti-stalking features to inform potential victims and help them find and disable AirTags and other Find My compatible devices: *Unwanted tracking notifications*, a *Play Sound* feature, and a *Find Nearby* feature. AirTag owners and stalkers are *tracking* the location of their AirTag remotely via the Find My network. Unwanted tracking notifications inform affected users that a Find My compatible device has been traveling with them for an extended amount of time without that device being able to connect to a paired device [3]. Users who suspect they are tracked use a *locating* feature to physically find an AirTag in their immediate vicinity. With the Play Sound feature, users can make AirTags emit a sound to locate them more easily. The Find Nearby feature uses ultra-wideband (UWB) radio signals to direct users to nearby supported Find My devices such as AirTags [5]. Since Apple and Google jointly proposed a new industry specification to address Bluetooth tracker misuse [21], tracking notifications are available across platforms [18].

While these measures are steps in the right direction, stalking incidents and malicious misuse are still prevalent, making effective and practical anti-stalking features crucial. Furthermore, we do not know how reliable unwanted tracking notifications are, whether users understand the notification and the potential threat they signal, and if available locating features work reliably.

To understand the efficacy and practicality of anti-stalking features, we use two consecutive studies to evaluate their

reliability and investigate users' perceptions of them. First, we evaluate the reliability of unwanted tracking notifications with a total of $N_A = 50$ participants on iOS and Android. We measure how long it takes to receive a tracking notification from an AirTag disconnected from paired devices. Second, we investigate user perceptions of anti-stalking features through a deception study with $N_B = 19$ participants. We explore users' reactions to unwanted tracking notifications on iOS when they do not expect them and how well the locating features work for them.

We found that unwanted tracking notifications work significantly better on iOS (100%) than on Android (56%), indicating a different implementation or hardware limitations that leave Android users at risk. On iOS, the notifications are easy to overlook and hard to understand, often depending on prior knowledge about the technology and experience with Bluetooth trackers. Even people who want to protect themselves have difficulty doing so effectively. We recommend redesigning the notification, providing more information and guidance toward safe responses, and creating protection levels that reflect users' risk profiles. This work offers the following contributions:

- Two studies, quantitative and qualitative, which show that unwanted tracking notifications do not work well for several user groups. They are not sufficiently reliable, expect prior knowledge of technology or the threat model, and their user experience does not guide them to a safe response, such as using locating features.
- Three actionable recommendations for platform providers that improve the anti-stalking features, such as enhancing the urgency and clarity of unwanted tracking notifications and offering increased UI guidance for identifying and disabling trackers.
- A deception study methodology that carefully balances ecological validity with ethical concerns, which could be helpful for future work that studies other kinds of safety warnings in the field.

2 Background

AirTags are tracking devices that lack a GPS receiver and do not know their position. Thus, using a crowd-sourced passive tracking approach, the AirTag system relies on nearby Apple devices to locate the trackers.

AirTags behave differently in regular use and when they are lost, which is reflected in one of three basic states: *Connected*, *Nearby*, and *Separated* (from paired devices). Under regular use, AirTags are either in the Connected or Nearby state. In these states, the AirTag's Bluetooth Low Energy (BLE) MAC address changes every 15 minutes to protect the owner's privacy.

When an AirTag cannot communicate with a paired device for 15 minutes, it enters the Separated (or "lost") state where the MAC address (and public key) only changes every 24 hours [21]. In this mode, nearby compatible devices, like iPhones, pick up the AirTag's encrypted broadcasts and send their location (as a proxy for the AirTag's location) to Apple's servers. This data is encrypted with the owner's public key, ensuring only the owner can access the precise location, while bystanders and Apple cannot access the location or ownership details [24, 27, 28]. The ephemeral identification (i.e., MAC, public key) is generated from a shared secret between the AirTag and its owner.

In Separated mode, bystanders can detect a tracker within the 24-hour window with the same MAC address. Client devices use undocumented heuristics to determine if a tracker is truly following them or just nearby. AirTags also help with stalking detection by emitting a faint chirping-like sound at several-hour intervals when they detect movement.

2.1 Tracking & Locating by the Owner

The owner can track their AirTag remotely by downloading location reports from Apple's servers and, when nearby, pinpoint its position with the help of locating features. To view the online location reports, the AirTag owner's device generates private keys from the shared secret, downloads the location reports from Apple servers, and decrypts them. These reports contain the coarse positions of the reporting phones. To increase the accuracy, the Find My client averages several location reports [2]. In Bluetooth vicinity, owners can read the approximate distance and direction with the "Find Nearby" feature based on ultra-wideband (UWB) or use acoustic signals with "Play Sound."

2.2 Locating AirTags with Other Phones

On iPhones, bystanders and tracking victims can only use UWB (where available) and sound to locate the AirTag after being notified about a potentially unknown tracker. Android phones also feature a manual scanning mode that can be triggered anytime, independent of tracking notifications. As a proprietary Apple technology, UWB is not available to Android users. Third-party apps on both platforms may provide more insights, including signal strength readings.

2.3 AirTag Misuse Mitigations

No current system can prevent misuse in the first place. All misuse mitigations are based on detecting stalking and identifying the perpetrator. This may deter stalkers by threatening to reveal their activity and identity. However, this hinges on finding and getting hold of the tracking device. Once a person physically gets hold of an AirTag, an NFC scan reveals the serial number, the last four digits of the associated phone

number, and an optional custom message. If this does not help, the victim can seek help from law enforcement using the AirTag's serial number.

AirTags implement two countermeasures: an autonomous one and one requiring an additional device. As an autonomous countermeasure, AirTags that are not connected to any paired device for a prolonged period emit a chirping-like sound at random intervals during movement. In general, this is neither regular nor strong enough to reliably pinpoint the location but can serve as a warning for those familiar with the signal. However, easy-to-follow tutorials allow for the simple removal of the AirTag's speaker, which is not detected by the software.

The second countermeasure requires a smartphone. iPhones and iPads with iOS or iPadOS 14.5 and later, as well as compatible Android phones running version 6.0 or above (with Google Play services updated since August 2023), continuously collect Bluetooth beacon signals. When the smartphone detects the prolonged proximity to a device-separated tracker, it alerts the user, as shown in Figure 1. There are many corner cases, such as crowded public transport. The specific algorithms are proprietary but likely consider significant locations, time of day, and distance traveled [28]. This implies fundamental limitations, such as that detection is only possible after arriving at a significant place (e.g., someone's home) and that the tracker needs to significantly slow down its address and public key rotation (currently from 15 minutes to 24 hours).

After an alert (or manual scan, which is only possible on Android), the user can locate the tracker by playing a sound on it or using Find Nearby with UWB (only on newer iOS devices), as described above.

3 Related Work

This section describes prior work on technology-facilitated abuse, Apple's Find My network and AirTags, and unwanted tracking notifications.

3.1 Technology-Facilitated Abuse

Technology is used to monitor, harass, and threaten people in the context of intimate partner abuse and interpersonal abuse (IPA) [13]. Freed et al. [17] show that many attacks involving technology are technologically unsophisticated, using UIs and ready-made applications to spy on victims. However, even unsophisticated attacks can be highly damaging to victims and challenging to counteract. Yet, experts on IPA also demonstrate inadequate expertise to cope with technology-facilitated abuse due to insufficient best practices and lacking supporting technologies.

To support this point, Fassl et al. [16] show that user perceptions and expectations of anti-stalkerware apps used to detect stalkerware on mobile phones do not align with the apps' capabilities. This makes it more difficult for users to use such tools to protect themselves from stalking effectively. Chatterjee et al. [13] identified several apps that can be used for intimate partner surveillance, the majority of which are "dual-use" apps that have a legitimate purpose (e.g., anti-theft) but can easily be repurposed for spying on a partner. Anti-spyware tools universally fail to identify these apps.

In a large-scale qualitative analysis of smart devices used in IPA, Stephenson et al. [30] identify a range of devices, including smart home devices such as appliances, security systems, and vehicles used to harass victims. Further, entertainment devices such as headphones and tracking devices like AirTags are misused to spy on people. The authors apply their abuse vectors framework to provide recommendations for improvements. They recommend making it easy for potential victims to detect dual-use devices such as AirTags so they are not as easily used for covert spying.

3.2 Find My Network

Previous work presents technical analyses of Apple's Find My network and AirTags. Heinrich et al. [19] developed OpenHaystack, an open-source framework for locating Bluetooth devices using Apple's existing Find My network. To achieve this, they reverse-engineered the Find My network. Their work gave us an initial understanding of how the devices behave and communicate when pairing, when lost, and during searching and finding.

Mayberry et al. [24] build on the work by Heinrich et al. and analyze the Find My protocol to understand what information the BLE broadcasts sent by AirTags and other Find My devices contain. The authors showed that building a device with modified behavior that does not trigger unwanted tracking notifications is possible, which is an issue. They concluded that some issues could be fixed easily while others would require a substantial redesign of the Find My protocol.

Roth et al. [27] investigate the AirTag hardware and firmware in detail and present further attacks on both. They extract the tracker's firmware and modify it, allowing firmware downgrades. They found issues rooted in the underlying hardware and software architecture, making them hard to patch. However, the authors mention that the proposed attacks do not pose a big risk for end users.

Beyond the custom-built devices demonstrated by Mayberry et al., Apple's Find My network accommodates other alternative uses. Tonetto et al. [31] show that the network makes crowd sensing and out-of-band mobile communication possible. They illustrate the possibility of coarse crowd monitoring, including determining density and flows. Further, they demonstrate a covert data channel without awareness of the devices partially carrying the information. Bellon et al. also show how the Find My network can be used to communicate arbitrary data [10].

3.3 Unwanted Tracking Notifications

Shafqat et al. [28] investigated the factors that trigger unwanted tracking notifications on iPhones. They found that a later time of day results in an earlier delivery of an unwanted tracking notification. Other factors, such as distance between devices and whether the significant locations feature is enabled, influence the delivery of the tracking notifications. Mode of transportation, device model, manual activation of the lost mode, battery status, and other factors do not seem to be relevant for the delivery of the notification. The authors also demonstrated a novel cloned AirTag that circumvents unwanted tracking notifications.

In another work by Heinrich et al. [20], the authors analyze user and survey data collected from their tracking detection app AirGuard [20]. They found that the app sends out 1,400 tracking alarms daily, and 44% of the surveyed stalking victims had been subject to location tracking with trackers hidden in cars, backpacks, and purses. The authors advocate for more effective tracking detection mechanisms integrated into smartphones by default and supportive measures for individuals without smartphones.

Turk and Hutchings [33] investigated the effectiveness of anti-stalking features on multiple Bluetooth location trackers, such as AirTags, using a gamified approach in an Assassins game [33]. However, only one participant attempted to use any features to check for trackers manually. The other participants relied on background scanning, which only detects devices part of the Find My network on iOS.

4 Methodology

We evaluate the effectiveness of features intended to protect users from stalking implemented in AirTags and its ecosystem. We chose AirTags since their anti-stalking features are considered the most robust at the time of writing [12, 29] and because they are within the most extensive crowd-sourced location tracking network. As described in Section 2, there are two primary anti-stalking features: (i) unwanted tracking notifications that warn users of potential stalking and (ii) locating features to help users find, identify, and deactivate trackers. To understand how well these features work in practice, we approach the evaluation from the perspective of potential stalking victims who may be unfamiliar with these trackers. The following research questions guided our evaluation:

RQ1: How reliable are unwanted tracking notifications on iOS and Android?

RQ2: How do users understand and react to unwanted tracking notifications?

RQ3: How usable and useful are the available locating features to find a hidden AirTag, and how can they be improved?

As summarized in Figure 2, we used two studies to answer our research questions. Study A quantifies the reliability and latency of unwanted tracking notifications (RQ1) with fully informed expert participants from our institution. Study B investigates how users who unknowingly carry a tracker and unexpectedly receive a tracking notification react to it (RQ2) and how well the locating features work for them (RQ3).

4.1 Study A: Reliability of Unwanted Tracking Notifications

To test the reliability of unwanted tracking notifications, we gave $N_A = 50$ fully informed participants (employees from our institution) an AirTag. Participants kept the AirTag for two days or until they received an unwanted tracking notification. We chose the two-day time window to ensure a notification could be triggered for all participants due to the 24-hour detection window (see Background, Section 2). We ensured that participants' device settings allowed unwanted tracking notifications, i.e., having Bluetooth, location services, Find My network (iOS) or *unknown tracker alerts* (Android) enabled [3, 18].

Data Collection. We conducted an a priori power analysis with G*Power to determine the minimum sample size. Detecting a large effect ($d = 1.0$), at a significance criterion of $\alpha = .05$, requires a minimum of 23 participants in each group ($N = 46$) in an independent samples t-test. We collected the following data: the participants' smartphone model and operating system version, when they received the AirTag, whether and when they received an unwanted tracking notification, and the environment (e.g., at home) in which they received it. If participants were not notified, we double-checked their smartphone configuration to avoid false negatives.

Data Analysis. Based on the collected data, we calculated how long it took until participants received an unwanted tracking notification. In this experimental setup, we used descriptive statistics, i.e., median, average, and standard deviation, to describe the reliability of unwanted tracking notifications. Additionally, we used statistical hypothesis testing to understand which factors affected the reliability and latency of unwanted tracking notifications, e.g., we applied a Fisher's exact test to check if unwanted tracking notifications are triggered more consistently on Android or iOS, and we used a Student's t-test to compare the latency of the notifications on Android and iOS.

4.2 Study B: Users' Understanding of & Reactions to Unwanted Tracking Notifications & Locating Features

While Study A, with fully informed participants, helped quantify the notification's reliability, we also wanted to understand how users react to the notification when they are unaware of

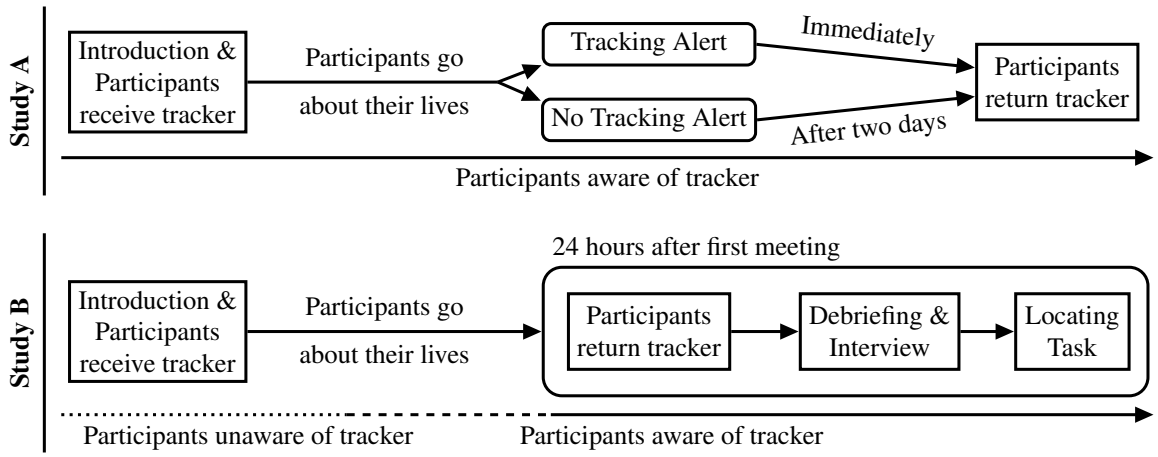

Figure 2: Overview of Study A, quantifying the tracking notification reliability with fully informed participants, and Study B, a deception study to understand people's reaction to an unexpected tracking notification.

carrying a tracker. To avoid the Hawthorne effect, we used a deception study [15]. During the recruitment stage and the initial phase of the study, we told participants that we were developing a novel activity monitor. The study comprised three parts: an introduction meeting to onboard participants to the deception study, a debriefing interview, and a locating task.

Figure 3: The blue 3D-printed case participants received in the deception study. It contains an AirTag and an explanation of the study's true purpose.

Introduction Meeting. In the first meeting, we introduced participants to the supposed purpose of the study and obtained their written consent. We gave the participants a 3D-printed box containing a hidden AirTag, shown in Figure 3, and told them we were developing a privacy-preserving method for measuring health data. In the context of the cover story, we instructed them to keep the 3D-printed box with them for activity measurement while logging their activities until the following meeting. We prepared a detailed story and answers to potential questions to ensure a credible study setup. Appendix B contains the detailed cover story. We scheduled a follow-up meeting the next day to inform participants of the study's true purpose as soon as possible.

Debriefing & Interview. In the second meeting on the next day, we started a semi-structured interview by establishing whether participants received an unwanted tracking notification and asked about their understanding of the situation and their reactions. We recorded the audio after obtaining consent. We debriefed all participants about the study's true nature and explained where they were deceived and why this deceptive setup was necessary. We gave all participants the option to opt out of the study and delete all their data. They all consented to continued participation and signed a second consent sheet describing the purpose of the actual study. We expected participants to associate the unwanted tracking notification with the study quickly, so we focused on their initial thoughts and reactions. We included speculative questions in the interview guideline (see Appendix C) for the participants who connected the notification too quickly to their study participation to react naturally.

Locating Task. In addition to investigating participants' reactions to the tracking notification, we wanted to understand how well the locating features worked for them. We gave them a locating task embedded in a simulated scenario to

ensure that all participants had experience with these features and could discuss their effectiveness. Since AirTags are often hidden in cars, we chose a car for our locating task. We hid an AirTag in the trunk of a company car (a sedan), sat with the participants in the front seats, and asked them to locate the AirTag.

Participants could not use their own iPhones for this simulated scenario because iOS currently does not support locating an unknown AirTag without first receiving a tracking notification. If participants previously received a notification from the hidden AirTag, the identifier could change prior to the task, rendering their phones unable to locate it. Additionally, we wanted to avoid the logistical difficulties of disassembling the enclosure, hiding the AirTag, and testing compatibility mid-interview. Since it was not feasible to wait for the notification, we provided participants with an iPhone already associated with the hidden AirTag, which they could use to locate it. We gave participants an iPhone that was feature-compatible with their own. Hence, we gave participants who owned an iPhone that supports the UWB-based direction-finding feature an iPhone 12 Pro and participants who owned an older version an iPhone 6, which does not support UWB. The Find Nearby feature is supported on iPhone 11 models and later, excluding iPhone SE (2nd and 3rd generation) [1] and available to people who received an unwanted tracking notification [7]. Giving participants phones instead of waiting for the tracking notification results in a slightly different audio that AirTags play when participants search for them with the audible sound.[1] However, we do not think the difference is significant enough to limit the applicability of our results.

The simulated scenario started with participants sitting in the car's front seat with the provided phone in their hand. We asked participants to imagine they received an unwanted tracking notification just when they parked their car. The Find My app showed the item screen of the hidden AirTag. We started the audio recording, asked participants to describe everything they do while searching, and asked follow-up questions for clarification. When participants had difficulty finding the tracker, we provided hints. After they found the tracker, we asked them about their experience and suggestions for improvements. At the end, participants filled out a demographics form (see Appendix F).

Recruitment. The recruitment criteria for this study were that participants were over 18 years old, used an iPhone, spoke either English or German, and were available for an in-person meeting. We only included iPhone users for this part of the study since our preliminary results from Study A demonstrated that Android users do not reliably receive unknown tracker alerts. Hence, we studied the best-case scenario. Our recruitment flyer described the study's purpose as improving privacy technologies. We posted the flyers in university buildings and local cafés and handed them out to people directly on the streets. Additionally, we created postings on social media platforms and classified ads portals, e.g., LinkedIn, Instagram, and eBay Kleinanzeigen. We pre-screened interested participants to ensure diversity and the recruitment criteria. We stopped recruiting after 19 participants because we did not identify major new themes in the final four interviews.

Demographics. In total, we recruited $N_B = 19$ participants (see Appendix G for demographic details). Of these, 11 were women, eight men. No participant was non-binary or chose to self-describe their gender. Fifteen participants spoke German, and four spoke English. The participants' age ranged from 19 to 67 (M=30.5, SD=12.6). The average affinity for technology score was 4.20 (SD=0.77, α=0.84), indicating an above-average comfort with technology. Nine participants knew about AirTags and their functions, seven knew about AirTags but were unfamiliar with their functions, and three did not know about AirTags. Seven participants have used AirTags before; one had used a different tracker, and the others had not used location trackers before the study. Eleven participants knew about the problem of technology-mediated stalking before; eight did not. Two participants had been stalked by technology before, 16 had not, and one was unsure.

Data Analysis. We transcribed all audio recordings using a locally installed version of Whisper, an automatic speech recognition model (multilingual large-v3). The first author listened to all recordings and edited the transcripts for readability and correctness. We used a reflexive thematic analysis approach [11] to understand the underlying patterns of responses to tracking notifications and the technical and social factors associated with these responses.

The experience of the involved researchers influences the analysis [26]. In this case, three researchers conducted the analysis: a first-year doctoral researcher (DR), a fourth-year DR, and a postdoc. They all had experience with qualitative analysis, with at least one published paper using qualitative methods. The fourth-year DR and the postdoc coded two interviews collaboratively to create initial codebooks for RQ2 and RQ3. Afterward, all three researchers reviewed, discussed, and adapted the codebooks and code assignments. Using the resulting codebooks, the first-year DR and the postdoc independently coded seven more interviews, creating new codes and taking notes. The two met to discuss the code assignments, the relations between the codes, and the observed patterns in the data. Mismatching code assignments were usually not disagreements but rather missed details in the transcripts or unclear situations, e.g., reported technology failures that could also be misunderstood technology. We resolved the few genuine coding disagreements during extensive discussions until we reached a consensus on the interpretation and consistent application of codes. The first-year DR coded the rest of the interviews to identify gaps in the analysis. Finally, all three researchers discussed the analysis results and how to

[1] "Get to know AirTag sounds" by Apple Support: https://youtu.be/c0TVHPHRjXg?t=29

present them in the paper. The reproducability package (see Section Open Science) contains the final codebooks.

4.3 Limitations

We designed our studies in close collaboration with our ERB, following high ethical standards. Our priority was that participants of Study B were debriefed about the deception as soon as possible while still allowing us to collect their initial thoughts and reactions to receiving an unwanted tracking notification without feeling or being endangered. While we made an effort to recruit a diverse set of participants for Study B, our resulting participant pool trends to a young age group with an above-average affinity for technology, which might impact the results.

5 Results

We report the results in the order of the research questions, starting with the results of the quantitative reliability study and continuing with the results of the deception study.

5.1 Notification Reliability & Latency

For Study A, we recruited $N_A = 50$ participants from our institution, 25 with iOS and 25 with Android. This excludes one potential participant with unsupported hardware and one who declined to participate after we informed them about the study procedure. Figure 4 shows the reliability of the unwanted tracking notifications, and Figure 5 shows the latency for iOS and Android, respectively.

iOS Devices. Most participants ran iOS 17, with version 17.2.1 – the latest available at the time – being the most recent and 16.5.1 the oldest. The hardware ranged from iPhone 8 (2017) to iPhone 15 Pro (2023).

All 25 participants received one or multiple unwanted tracking notifications within the two-day window. It took between 1 and 24 hours for the notification to be triggered, with an average of 4 hours 58 minutes and a median of 4 hours. Most participants (23) received a notification after arriving home, while two received it at their workplace.

Android Devices. For Android users, we collected version information about Google Play services, as they implement the unknown tracker alerts. The Google Play services versions ranged from 23.42.12 to 23.49.14, and the Android versions ranged from 10 to 14, with 14 being the latest available version. The oldest hardware was a Samsung Galaxy J6 (2018), and the newest was a Google Pixel 7a (2023). The other phone manufacturers were Fairphone, Huawei, Xiaomi, and Redmi.

14 out of 25 participants (56%) received an unknown tracker alert within the two-day window. For the participants who received the alert, it took an average of 11 hours 51 minutes, with a median of 4 hours 30 minutes. Most participants (12) received it after arriving home, with two exceptions who received it on their way home or on a train.

Reliability of Tracking Notifications on iOS & Android. We used Fisher's exact test to compare the success rate of unwanted tracking notifications on iOS and Android. It resulted in a p-value $p < .001$ and odds ratio of $OR = 40.38$ (95% CI: 2.22 to 737.97) after Haldane correction. This suggests that iOS devices are more likely to trigger the notifications than Android devices. We used a Student's t-test to compare the latency of the unwanted tracking notification between iOS and Android devices. The results, $t(37) = -2.6191, p = .013$, indicate a significant difference. The effect size of Cohen's $d = -0.874$ suggests a large effect. This indicates that the latency of the notifications is significantly shorter for iOS than for Android devices. No discernible trend in Android hardware, OS, or Google Play services version contributed to whether an alert was triggered.

Takeaways

iOS devices were significantly more reliable and timely than Android devices in triggering unwanted tracking notifications for AirTags. Tracking notifications arrived significantly earlier on iOS than on Android. We found no discernible hardware or OS pattern affecting notification performance on Android.

5.2 Themes Associated with User Reactions to the Unwanted Tracking Notification

In Study B, the deception study, we provided participants with take-home tracking devices to understand how they react to unexpected tracking notifications in a naturalistic situation. Figure 6 provides an overview of participant response strategies and the factors influencing them.

Technology Understanding. Participants' understanding of the underlying technology was associated with their reactions to receiving an unwanted tracking notification. Participants with a higher self-reported affinity for technology demonstrated a deeper understanding of AirTags and the Find My network. In contrast, some participants with a lower affinity also showed more misconceptions about how the technology works. This difference in understanding is associated with the users' self-efficacy. Those with a high affinity mostly performed purposeful actions aligned with their desired result, whereas some participants with a lower affinity performed actions that did not help them achieve their goal, i.e., identifying or disabling the tracker.

> *"You said you would switch off your phone, can you think of anything else that you could perhaps change on your phone?"* – Interviewer
>
> *"Yes, maybe switch off the Bluetooth and maybe switch off the Internet."* – P13

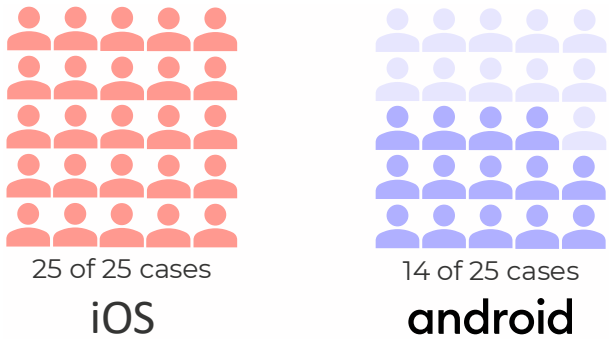

Figure 4: Number of successfully triggered unwanted tracking notifications on iOS and Android.

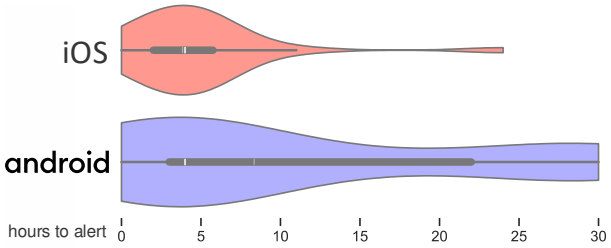

Figure 5: Probability distribution of the time it took to trigger the tracking notification on iOS and Android.

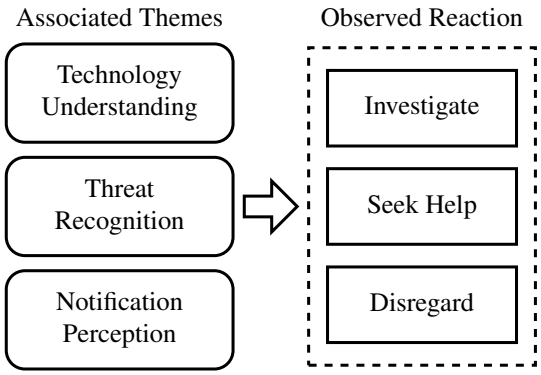

Figure 6: Participants' reactions observed to the unwanted tracking notification and their associated themes.

All participants were unaware of how system settings, such as Bluetooth and location services, influence unwanted tracking notifications. Some participants disabled Bluetooth temporarily for various reasons, such as disconnecting a Bluetooth device or preserving battery life. Even when they knew about the notification, they did not know they would not receive tracking notifications when Bluetooth was turned off.

Some participants who had a general understanding of a technology they deemed similar, such as location sharing via messaging or navigation apps, applied this understanding to AirTags. An analogical transfer is difficult in this case, as most other tracking technologies work differently. Hence, reasoning based on analogical transfer was associated with wrong conclusions.

Threat Recognition. Most participants considered stalking a serious issue. However, this stated concern was not reflected in their actions, and few took protective measures in a potential stalking scenario. This inaction can be explained for the eight participants who immediately associated the notification with the study. The remaining seven participants who received the notification gave various reasons, such as not considering themselves a potential target for stalking. Notably, all participants who shared this attitude were men.

> *"So I have to be honest, I personally don't mind. [...] I also think to myself, what are they going to do with my location now? They're not going to send a killer after me."* – P10

Since unwanted tracking notifications do not mention a concrete threat, potential victims must infer the threat themselves. Participants who knew and understood the technology from previous contact with Find My devices or personal or anecdotal exposure to technology-facilitated abuse could easily identify the threat. Participants who had not known that AirTags are misused for stalking did not pay much attention to the notification or recognize the potential threat, increasing the potential for prolonged surveillance. Understanding the unwanted tracking notification and recognizing the threat is an essential first step in protecting oneself. However, many participants who received and saw the notification decided not to investigate further. This was done for various reasons: One participant assumed the notification was triggered by a device from someone in their friend group. Another was busy when they saw the notification and postponed their inquiry. In both cases, the participants received the notification a second time and investigated it then. In a real stalking scenario, the time between the two notifications provides attackers with additional information about their victim.

Notification Perception. The presentation of the unwanted tracking notification in iOS (see Figure 1) was associated with our participants' reactions. Depending on the context a given participant was in when they saw the notification, they chose to disregard it. Some explained that the notification did not appear important, as it looked similar to other notifications. In iOS, unwanted tracking notifications are delivered as active notifications – the default on iOS, meaning they are shown like any other notification and not prioritized in any way [6]. Some participants were busy or in a rush when they saw the notification, so the combination of these factors led them to disregard it.

"Then I read 'You know this AirTag' and... 'You don't know it'. But then I was at work and I couldn't mess with it. I probably should have continued, I suppose." – P13

The heading of an unwanted tracking notification reads "AirTag Found Moving With You," below it states in smaller font "The owner can look up its location." Fully understanding this notification requires prior knowledge about the mentioned item, in this case an AirTag. Three participants did not know what AirTags are and initially did not understand the notification content. After investigating the situation further, they realized what the notification tried to warn them about. However, whether participants knew AirTags before the study or not, everyone was uncertain about the potential threat. Neither the notification nor the Find My app UI explicitly mentions a threat such as stalking, and they remain vague about possible consequences. One participant described how they scan notifications by looking at the associated icons and judging their importance when they have many notifications. They recalled seeing the notification icon triggered by our study, thinking it looked similar to another icon they had seen before and did not consider important, thus disregarding it until later in the day.

"Why I was less worried is that this icon, this white magnifying glass or what it actually is [...] looked like [an icon] with the AirPods back then. And I think if another icon would show up, which I haven't really seen before, then that would have triggered something more in my head." – P2

Scanning notifications roughly instead of examining each one in detail is a strategy mentioned by multiple participants to handle a large number of notifications. Most participants who did examine the notification more closely tried to find a benign explanation for receiving it instead of assuming it was a threat. The benign explanations included a bystander on a bus being responsible for triggering the alert and someone else accidentally putting the tracker on a participant without bad intentions.

"At first, I honestly thought that someone had accidentally put it in my pocket, I didn't intuitively think that someone had somehow put it in my pocket with negative intentions." – P10

Takeaways

Participants' reactions to unwanted tracking notifications varied. They appeared to be associated with their understanding of technology, threat perception, and how they perceived the tracking notifications. Those with high technology affinity generally took more effective actions, while others, especially those who viewed stalking as unlikely or misinterpreted the notifications, often dismissed them.

5.3 User Reactions to the Notification

The technology understanding, threat recognition, and notification perception were related to how participants reacted to the unwanted tracking notification. We divide the reactions into three groups: those who investigated the situation themselves, those who sought help from others, and those who disregarded the notification (see Appendix D for a summary of participant responses).

Investigate. Participants familiar with AirTags or other Find My devices mostly tapped on the notification and used the functions to identify and find the device within the Find My app. The participants examined the map that shows the tracker movements, and, in most cases, used the Play Sound function on the found AirTag. Most realized then that the "activity monitor" from our study contained the detected AirTag. Two participants tried to identify who the AirTag belonged to by holding it close to their phone's NFC receiver, but they could not get the function to work.

"I first took my phone and held [the tracker] up to it. You should hold it relatively close to it to find out who it's from. You should be redirected to an Apple website. But that wasn't the case." – P17

Some participants did not know about AirTags and searched online for more information about the device and its uses. Even without prior knowledge or experience with AirTags, some participants who opened the Find My app still used the available features to investigate the situation.

One of our participants reported that they had been a victim of stalking with an AirTag previously and shared information about their experience, in which this participant performed multiple steps after receiving an unwanted tracking notification: They turned off location services, changed all of their passwords, and sought help from a friend who attempted to find a hidden tracker but failed. However, even after these measures, an AirTag moving with them could reveal their location as long as another device on the Find My network is nearby. While the protective measures the participant took are helpful in some contexts, they are insufficient in a stalking scenario with an AirTag, indicating an incomplete understanding of the technology.

Multiple participants mentioned they would throw away or disable a foreign AirTag they found. No participant did so in the study, as all associated the notification with the study shortly after receiving it.

Seek Help. Participants who were less familiar with AirTags or uncertain about the situation sought help from people in their social circle, such as family, friends, and colleagues. Typically, participants referred to people they deemed more knowledgeable in technology.

Some participants asked their friends or family members if the notification could be caused by one of their devices, seeking a benign explanation. One participant received the

notification while with a friend group and investigated the situation within the group to determine if one of them could be responsible. They considered a reason outside their group only after receiving the notification again later.

> *"I got the notification on the way there and just thought, okay, one of [my friends] will have an AirTag. At some point later I asked [...] 'Do either of you have an AirTag'? And they were both like 'Nope'. But then we didn't question it any further and just thought, okay."* – P9

Other participants who needed clarification about the notification and what to do in the app or with the tracker would ask someone they deem knowledgeable and trustworthy for help and advice. One participant mentioned that their teen child likely knows better what the notification means and how to deal with it. They would have asked them if they had received it outside the study setting.

Multiple participants would contact the tracker manufacturer or local law enforcement in a real stalking scenario. Two participants opened the 3D-printed case we gave them and read the note, which provided the first author's contact information (see Figure 3). However, they did not contact them because they were unconcerned and could wait until the follow-up meeting for an explanation.

Disregard. Participants who neither investigated the threat nor sought help disregarded the notification for various reasons. As expected, some participants reacted this way because they immediately associated the notification with their study participation.

However, others disregarded the notification, citing benign causes beyond the study, such as erroneously receiving the notification from a bystander. One participant mentioned having received a false positive before and thus being desensitized to the notification.

> *"The first time, I probably wouldn't think too much about it, I would just think, okay, maybe someone walked around me or something. I think if it happened a second time, I'd get a bit paranoid."* – P9

Participants also disregarded the notification because the presentation of the unwanted tracking notification in iOS does not appear important or urgent, making it a low priority for some, especially if they are focused on other notifications. Several participants did not react to the notification because they did not consider themselves a potential stalking target. Notably, all participants who shared this attitude identified as men.

Takeaways

We identified three primary ways participants reacted to unwanted tracking notifications: investigate the notification, seek help, or disregard it. Those familiar with AirTags or suspicious of a threat often used the app to investigate, sometimes seeking information or support online. Others sought help from knowledgeable friends or family. Some participants, especially those who did not consider themselves likely stalking targets or saw the alert as low priority, disregarded the notification.

5.4 Locating the Tracker

In the second part of Study B, we asked participants to locate a hidden AirTag in a car while describing their thoughts and actions. We observed them during the process and asked them about their experience and suggestions for improvement after finding the tracker (see Appendix D for a summary of participant responses and behavior).

Finding Process. Most participants were able to find the hidden tracker within ten minutes and concluded that the locating features helped them do so.

During the finding process, some participants were confused about the map in the Find My app. The map is not precise enough to locate the tracker's exact location, but it is always displayed even if the tracker is close. This prompted some participants to interact with the map first, realizing it was not helpful before moving on to another method.

> *"As I said, I also criticize the fact that it was simply on a map, which is rather large, I'd say, so you can't zoom in that much. It is simply not really feasible. Especially when it's supposed to be in a car."* – P10

The function descriptions in the UI were unclear to many participants. We observed a trial-and-error exploration approach where participants kept using the first option that worked for them.

This approach was especially apparent with the Find Nearby feature, which many participants never used despite having it available. When asked, most replied that they did not know what it does and that the Play Sound function worked well enough. One participant who used the Find Nearby function outside the car in the rain (which impacts the function) was confused by the incorrect distances shown on the phone, which made it harder to find the tracker.

Participants without prior experience with location trackers were confused by the chirping sound they could play on the AirTag. Multiple participants were uncertain about whether the sound originated from the phone they were holding or the tracker they were searching. In multiple instances, participants attempted to increase the volume of the chirping sound using the phone's physical volume buttons, which is not possible.

Some participants could not hear the dampened sound the tracker played in the trunk while sitting in the front seat.

Overall, the majority of our participants mainly used the Play Sound feature during the finding process. Only a few participants who had it available used the Find Nearby feature, but those who did found it helpful. Two participants initially searched for the tracker without technical means but changed their approach after being unsuccessful.

Improvements. Our participants consistently mentioned that the sound played by the AirTag should be louder, though some acknowledged that this might be a technical limitation of the form factor. One participant added that there should be an option to play the sound continuously so they would not have to keep tapping the button. Some participants who showed difficulty locating the tracker from the sound asked for a different sound that was easier to pinpoint by ear.

While participants who had tried the Find Nearby feature mostly praised it, they criticized the UI as unintuitive and confusing. The finding interface usually displays an arrow pointing toward the tracker, but this arrow disappears if the technology cannot determine the direction with high confidence. Some participants asked for more straightforward descriptions of what happens while using the Find Nearby feature.

In a few cases, the technology was unreliable, not connecting to the hidden AirTag, making the locating features unavailable. In those cases, participants did not know how to proceed and had to wait for the connection, asking for higher reliability.

Participants wished for improvements like visual alerts, i.e., blinking lights, to help locate the tracker more quickly, especially for those who are hard of hearing. Some asked for a streamlined and easy-to-find feature to identify the owner of a tracker after finding it.

Takeaways

Most participants found the hidden AirTag using the Play Sound feature but encountered challenges with the UI. Many considered the sound too faint and suggested a louder, continuous option for easier tracking. The Find Nearby feature was underused due to unclear function labels, though helpful when used. Participants recommended improved UI guidance, visual locating aids, and more reliable connections to make the locating process smoother and more accessible.

6 Discussion

Crowd-sourced location tracking networks like Apple's Find My and compatible trackers like AirTags are powerful stalking tools. They are easy to obtain, perceived as a positive technology, and their functionality enables precise location tracking. While we highlight the shortcomings of AirTags' anti-stalking features, the literature considers them a benchmark [30]. Most other location trackers omit implementing anti-stalking features entirely or only do so to a lesser extent. In many cases, the existing features will notify potential stalking victims within a few hours. They can then find the device using the locating features or manually search before disabling or disposing of it.

6.1 Disparities Across User Groups

Unwanted tracking notifications are only available to people with a supported Apple or Android device, the latter of which is much less effective. People without such a device need to rely on the chirping sound emitted by AirTags in motion or have to spot them visually without any technical support.

Marginalized populations, such as those hard of hearing or deaf, may not benefit from sound-based features in trackers. This highlights a critical issue: Anyone can be a victim of stalking independent of their abilities or resources. Thus, not everyone is equally and sufficiently protected from the misuse of Bluetooth location trackers.

Further, potential victims have minimal control over the stalking situation. Stalkers control critical aspects, such as selecting and modifying the tracking device, which affects the availability and reliability of anti-stalking features for the victim. For example, a stalker can remove the speaker or use a tracker without UWB functionality, preventing victims from finding it with the Find Nearby feature.

These tracking devices expand the capabilities of traditional stalkers and allow for opportunistic stalking in situations where a tracker previously obtained with good intentions starts to be misused. Related work describes abuse facilitated by Bluetooth location trackers, often in the context of intimate relationships [13, 17]. Abuse scenarios such as stalking can be a severe threat and cause lasting harm to victims.

6.2 Product Design & Support

The technological capabilities of Bluetooth location trackers and crowd-sourced tracking networks make them useful for stalking. For example, Apple's Find My servers do not appear to rate-limit location requests [24], which enables near real-time location tracking. The Find My app shows the AirTag's location precisely, enabling the identification of the specific building in which the tracker is located. Together with a high frequency of location updates from nearby devices, AirTags allow for precise real-time tracking. We are convinced that location trackers can still fulfill their intended purpose even with less precision and lower update frequency. Manufacturers' desire to be competitive and build the best product they can for their targeted use cases seems detrimental to protecting people from stalking.

Significant Locations. Tracking notifications are often triggered when victims arrive home, which is likely too late to

prevent harm. This is a deliberate design decision. Apple's iOS, by default, tracks frequently visited locations and remembers them as significant. To avoid premature tracking notifications, iOS uses these significant locations to determine when to deliver tracking notifications [7]. Study A showed that an unwanted tracking notification is more likely to be delivered after a device arrives at a significant location, such as a home. Thus, it is too late to hide valuable location information from a stalker. To avoid revealing the home location by design, providing an alternative way of reducing false positives is crucial.

Notification & Application Design. Tracking notifications are easily dismissed and disregarded. By default on iOS, they are treated as regular active notifications [6]. This means that they behave like most notifications from apps such as messengers, i.e., they do not break through settings that silence notifications or play sounds when the phone is silent. The behavior of tracking notifications on Android is similar. Study B revealed that users easily overlook tracking notifications or disregard them because they get lost among other notifications. Delivering tracking notifications at a higher interruption level, such as *time sensitive*, could improve the situation by always notifying users immediately.

Notification Phrasing. The notification itself is challenging to understand without further information. The phrasing of tracking notifications on iOS uses the product name of the identified tracker in the heading. As the participants who had to search for information on AirTags underline, fully understanding this notification requires knowledge about the mentioned item. Android's version of this notification, "Tracker traveling with you," uses a more widely understood generic term to explain the situation. However, both platforms avoid mentioning a potential threat, only explaining that the tracker's owner can look up its location. While false positives are possible, users should receive all necessary information to assess a personal threat. Study B showed that users who are new to this technology or those with a low affinity for technology have difficulties understanding the full extent of the situation with the limited information and description provided. Some users searching for resources online will find helpful information on Apple's and Google's support pages [3, 18]. However, those websites also lack concrete threat models, and both vendors omit negative-associated wording such as "stalking." Notably, in October 2024, Apple further softened their language by renaming "unwanted tracking alerts" to "unwanted tracking notifications" on their *detecting unwanted trackers* support page [4].

Support Documentation. The online support resources are not kept up to date for all regions where the Find My network is available. During our work on this project, we realized that Apple's *Personal Safety User Guide* is kept up to date in US English. However, the documentation for other languages (including other variations of English) lags behind. Technology safety resources linked by Apple only cover three English-speaking countries, while their Find My network and AirTags are available in many more. Many parts of the support documentation shift the burden of dealing with a tracker or associated problems to local law enforcement. From anecdotal stories and our research, success with law enforcement regarding issues involving technology-facilitated abuse can vary considerably. We could not find an extensive personal safety guide for Google's Android, which is also rolling out its Find My Device network at the time of writing.

6.3 Transfer to Other Trackers

While we used AirTags as a showcase example for a Bluetooth location tracker in this project, other trackers exist within the Find My network and other tracking networks, such as Google's Find My Device. We kept the extensive landscape of location trackers in mind while developing our methodology. Most results and discussion points are transferable to other trackers and tracking networks because they work similarly.

At the time of writing, the Find My network and AirTags are the biggest and most capable of their kind [8]. While other tracking networks might become more important in the future, it is unlikely that crowd-sourced location tracking will cease to exist. Therefore, we must develop and deploy comprehensive and effective tools to detect and mitigate misuse for all current and future locating devices. Apple and Google were the main contributors to an industry specification for detecting unwanted location trackers [21]. It lists best practices and protocols for location tracker manufacturers but falls short of the actual detection mechanism or enforceable technical or algorithmic provisions. The specification does not go beyond the capabilities we evaluated in this project, which we showed to be insufficient.

6.4 Recommendations

We provide actionable recommendations (AR), in order of urgency, for platform operators of crowd-sourced location tracking networks such as Apple's Find My.

AR1: Notifications must use clear language & convey urgency. Unwanted tracking notifications are easily missed or disregarded due to their current presentation. They should be delivered with urgency and presented with priority, getting a user's immediate attention and remaining visible until interacted with. The wording of the notification should be clear to everyone, using generally understood terminology. The visual presentation of the notification should convey the potential importance of the situation by distinguishing it from other notifications.

AR2: UI must guide users to safe responses. The current UIs for interacting with location trackers on iOS and Android are minimal. They must provide guidance and explanations.

The interface must explain the possible situation, including threats, and actively support users with identifying and disabling a tracker. Based on our findings, a guided interface should offer an option to contact people in a person's social circle, the tracker's manufacturer, victim support organizations, such as the cyber helpline,[2] and local law enforcement.

Manual scans for unknown trackers should be an option, and previously delivered tracking notifications should remain accessible in case they are accidentally dismissed. Supporting documentation should be linked to as part of the user experience and kept up to date without delay for all regions where a tracking network is deployed.

AR3: Create different protection levels corresponding to users' risk profiles. Anti-stalking features must be proactive when possible and technically reliable on all platforms. Platform operators should consider higher protection levels that concerned users can manually enable. Higher protection levels could, e.g., deliver unwanted tracking notifications more quickly and with higher urgency. Lower protection levels could increase the threshold for delivering warnings to avoid warning fatigue. Where possible, the capabilities of a tracking network should be reduced to a minimum to make it less appealing to misuse. An example is reducing the number of possible location requests per hour, which would make stalking less convenient while maintaining the ability to find personal items.

7 Conclusion

The currently available anti-stalking features for Bluetooth-based location trackers, such as AirTags, are a first step in the right direction, but they are still highly insufficient to protect from stalking. Unwanted tracking notifications do not convey the potential threat because they use unclear terminology and lack a sense of urgency. Sound-based features discriminate against hard-of-hearing and deaf people and do not necessarily lead to finding trackers, even for people with good hearing. Furthermore, up-to-date and usually expensive smartphones are needed to use the full spectrum of available anti-stalking features. This promotes forward compatibility, and people who do not update their hardware regularly are left alone when dealing with potential threats. Minor changes to the user experience will already improve stalking protection significantly. First and foremost, tracking notifications must convey the potential severity of the situation while offering more resources to handle it. Presenting the notifications with urgency and making interaction necessary would make them stand out. Anti-stalking features need a guided user experience with an explicitly stated potential threat and the necessary information as central points to support a safe response. More research is necessary to identify anti-stalking measures for marginalized populations, and enable backward compatibility, but overall, these improvements will provide all users with increased protection.

[2] https://www.thecyberhelpline.com

Acknowledgments

This work would not have been possible without the enthusiastic participants who contributed their time and insights. We thoroughly appreciated the fruitful discussions about the methodology and ethical considerations with Sven Bugiel and the members of CISPA's Empirical Research Support team. We thank Avian Krämer from CISPA's Scientific Writing and Presentation team for proofreading this paper. Lastly, we thank the anonymous reviewers and the shepherd for their valuable and constructive feedback that substantially improved our paper.

The first and third authors contributed to this work as part of the Saarbrücken Graduate School of Computer Science. This work was partially funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – 521601028.

8 Ethics Considerations

Before our quantitative and qualitative user studies on location tracking, we intensively discussed ethical issues around consent, deception, handling personal data, and appropriate compensation. Our institution's ethical review board (ERB) approved this study, and we adhered to the GDPR and German privacy laws.

Consent and Deception. We ensured that participants felt comfortable and had room to ask questions and raise concerns throughout the project. We informed all participants about the study's purpose and our data handling procedures. All participants signed consent sheets that explained the details.

Before Study A, we fully informed the participants from our institution about the study purpose and explained how AirTags work and how we protect their privacy, including location data. This study has little harm potential as participants are fully informed about the experiment and only report non-personal data from and about their smartphones.

Study B investigated users' reactions to unwanted (and unexpected) tracking notifications. Hence, we could not fully inform participants about the study purpose – the notification would no longer have been unexpected. Instead, the onboarding procedure included a cover story. Deception can cause distress, confusion, or other affective responses in participants. To avoid harm and maintain ecological validity, we designed the study in line with ethical guidelines and in collaboration with experts and our institution's ERB.

While developing the methodology, we considered approaches that do not require deception or carrying an AirTag. However, these would have led to low ecological validity or introduced biases and uncertainties, resulting in low-quality data. Carefully weighing the risks and benefits of a deception study, we decided that a cover story was the best approach to exploring participants' reactions to unwanted tracking notifications with ecological validity. The cover story kept statements about data handling and hardware properties as accurate as possible while withholding knowledge about the real device. Participants knew they carried a motion sensor and Bluetooth device that sent data to a server we could not access.

We took multiple precautions to minimize distress and confusion during the deceptive study. In the onboarding interview, we gave participants our contact details and told them they could reach out in case of any questions or concerns. Our supposed "activity monitor" contained a hidden explanation about the study and provided contact details (see Figure 3). Furthermore, we advised our institution's front desk on how to respond to distressed participants or the police if they inquired about the research. Before conducting the study, we asked psychology and sociology experts to identify potential concerns. Thus, we were ready to handle distressed or angered participants.

Following ethical guidelines, we debriefed all participants about the study's purpose within 24 hours. We gave participants a second consent form containing the full study details without deception and asked for their consent again. All participants agreed to continue participating in the study, i.e., no one dropped out. Until then, we only had participants' contact information.

The societal benefits – for people at risk of stalking – outweigh the risks, as this work informs technical and policy safeguards to better protect potential victims.

Data Handling. In Study A, we collected relevant smartphone details from our participants. Additionally, we recorded the time we gave out the AirTag and the self-reported time participants received an unwanted tracking notification. In Study B, we collected two audio recordings: an interview after the debriefing when participants consented to the actual study purpose and one during the locating task. Additionally, we collected demographic information in our exit survey.

In neither study did we collect location information. However, to use AirTags, they must be paired with an Apple Account. This Apple Account then has access to the AirTags' location. So, we created an Apple Account solely for this project and used the four-eye principle to prevent any single researcher from accessing it. After configuring the AirTags, we logged out of the Apple Account, making it impossible to retrieve the location of the AirTags without colluding. We informed participants that their end-to-end encrypted location data goes through Apple servers and can only be decrypted using the Apple Account we created for the study. After finishing data collection, we deleted this Apple Account and the associated key material–making it impossible for Apple or us to access the AirTags' location.

Compensation. All Study A participants were employees at our institution. Legally, we can not compensate them for their participation. We are confident this does not decrease our finding's validity as our study focused on the technical reliability of tracking notifications and not the participants' behavior. We compensated Study B participants – the deception study and the locating task – with 50 EUR wire transfers.

9 Open Science

To improve this work's reproducibility, we published[3] the demographics questionnaire, the interview guidelines, codebooks, and the 3D model of the AirTag case we used for Study B. We also published the detailed anonymized data we collected for Study A in machine-readable format. We do not publish interview transcripts because (i) it is hard to remove all identifiable information from them, and (ii) we do not have the participants' consent to publish them.

[3] Open science archive DOI: 10.5281/zenodo.15527227

References

[1] Apple. Ultra Wideband availability, December 2023. https://support.apple.com/en-us/109512.

[2] Apple. Apple Platform Security Guide - Using Find My to locate missing Apple devices, November 2024. https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf#page=204.

[3] Apple. Detecting unwanted trackers, 2024. https://support.apple.com/guide/personal-safety/detecting-unwanted-trackers-ips139b15fd9/web.

[4] Apple. Detecting unwanted trackers (Web Archive), September 2024. http://web.archive.org/web/20240905211036/https://support.apple.com/guide/personal-safety/detecting-unwanted-trackers-ips139b15fd9/web.

[5] Apple. Find the precise location of an AirTag, March 2024. https://support.apple.com/en-me/guide/iphone/ipha779f0c10/ios#iph44bb32c36.

[6] Apple. Managing notifications, 2024. https://developer.apple.com/design/human-interface-guidelines/managing-notifications.

[7] Apple. What to do if you get an alert that an AirTag, set of AirPods, Find My network accessory, or compatible Bluetooth location-tracking device is with you, December 2024. https://support.apple.com/en-us/119874#unwantedtracking.

[8] AppleInsider. Apple has more than 2.35 billion active devices, up 550 million since 2022, January 2025. https://appleinsider.com/articles/25/01/30/apple-has-more-than-235-billion-active-devices-up-550-million-since-2022.

[9] Rosanna Bellini, Emily Tseng, Nora McDonald, Rachel Greenstadt, Damon McCoy, Thomas Ristenpart, and Nicola Dell. So-Called Privacy Breeds Evil": Narrative Justifications for Intimate Partner Surveillance in Online Forums. *Proceedings of the ACM on Human-Computer Interaction*, 4(CSCW3), December 2020.

[10] Alex Bellon, Alex Yen, and Pat Pannuto. TagAlong: A Free, Wide-Area Data-Muling Service Built on the AirTag Protocol. In *Proceedings of the 20th ACM Conference on Embedded Networked Sensor Systems*, SenSys '22, pages 782–783. ACM, January 2023.

[11] Virginia Braun and Victoria Clarke. *Thematic Analysis: A Practical Guide*. Sage Publications, October 2021.

[12] Rose Ceccio, Sophie Stephenson, Varun Chadha, Danny Yuxing Huang, and Rahul Chatterjee. Sneaky Spy Devices and Defective Detectors: The Ecosystem of Intimate Partner Surveillance with Covert Devices. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 123–140. USENIX Association, August 2023.

[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)*, pages 441–458. IEEE, May 2018.

[14] James Clayton. Apple sued by women over AirTag stalking, December 2022. https://www.bbc.com/news/technology-63880969.

[15] Verena Distler, Matthias Fassl, Hana Habib, Katharina Krombholz, Gabriele Lenzini, Carine Lallemand, Lorrie Faith Cranor, and Vincent Koenig. A Systematic Literature Review of Empirical Methods and Risk Representation in Usable Privacy and Security Research. *ACM Transactions on Computer-Human Interaction*, 28(6):1–50, December 2021.

[16] Matthias Fassl, Simon Anell, Sabine Houy, Martina Lindorfer, and Katharina Krombholz. Comparing User Perceptions of Anti-Stalkerware Apps with the Technical Reality. In *Proceedings of the Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, pages 135–154. USENIX Association, 2022.

[17] 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*, CHI '18, pages 1–13. ACM, April 2018.

[18] Google. Find unknown trackers, 2024. https://support.google.com/android/answer/13658562?hl=en.

[19] Alexander Heinrich, Milan Stute, and Matthias Hollick. OpenHaystack: a Framework for Tracking Personal Bluetooth Devices via Apple's Massive Find My Network. In *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, WiSec '21, pages 374–376. ACM, June 2021.

[20] Alexander Heinrich, Leon Würsching, and Matthias Hollick. Please Unstalk Me: Understanding Stalking with Bluetooth Trackers and Democratizing Anti-Stalking Protection. *Proceedings on Privacy Enhancing Technologies*, 2024(3):353–371, July 2024.

[21] IETF Datatracker. Detecting Unwanted Location Trackers, 2024. https://datatracker.ietf.org/doc/draft-detecting-unwanted-location-trackers/01/.

[22] Ryan Mac and Kashmir Hill. Are Apple AirTags Being Used to Track People and Steal Cars?, December 2021. https://www.nytimes.com/2021/12/30/technology/apple-airtags-tracking-stalking.html.

[23] Adrienne Matei. 'I was just really scared': Apple AirTags lead to stalking complaints, January 2022. https://www.theguardian.com/technology/2022/jan/20/apple-airtags-stalking-complaints-technology.

[24] Travis Mayberry, Ellis Fenske, Dane Brown, Jeremy Martin, Christine Fossaceca, Erik C. Rye, Sam Teplov, and Lucas Foppe. Who Tracks the Trackers? Circumventing Apple's Anti-Tracking Alerts in the Find My Network. In *Proceedings of the 20th Workshop on Workshop on Privacy in the Electronic Society*, WPES '21, pages 181–186. ACM, November 2021.

[25] Paul E. Mullen and Michele Pathé. Stalking. *Crime and Justice*, 29:273–318, January 2002.

[26] Anna-Marie Ortloff, Matthias Fassl, Alexander Ponticello, Florin Martius, Anne Mertens, Katharina Krombholz, and Matthew Smith. Different Researchers, Different Results? Analyzing the Influence of Researcher Experience and Data Type During Qualitative Analysis of an Interview and Survey Study on Security Advice. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, CHI '23, page 21. ACM, 2023.

[27] Thomas Roth, Fabian Freyer, Matthias Hollick, and Jiska Classen. AirTag of the Clones: Shenanigans with Liberated Item Finders. In *2022 IEEE Security and Privacy Workshops (SPW)*, pages 301–311. IEEE, May 2022.

[28] Narmeen Shafqat, Nicole Gerzon, Maggie Van Nortwick, Victor Sun, Alan Mislove, and Aanjhan Ranganathan. Track You: A Deep Dive into Safety Alerts for Apple AirTags. *Proceedings on Privacy Enhancing Technologies*, (4), 2023.

[29] Sophie Stephenson, Majed Almansoori, Pardis Emami-Naeini, and Rahul Chatterjee. "It's the Equivalent of Feeling Like You're in Jail": Lessons from Firsthand and Secondhand Accounts of IoT-Enabled Intimate Partner Abuse. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 105–122. USENIX Association, August 2023.

[30] Sophie Stephenson, Majed Almansoori, Pardis Emami-Naeini, Danny Yuxing Huang, and Rahul Chatterjee. Abuse vectors: A framework for conceptualizing IoT-enabled interpersonal abuse. In *32nd USENIX Security Symposium (USENIX Security 23)*, volume 3. USENIX Association, 2023.

[31] Leonardo Tonetto, Andrea Carrara, Aaron Yi Ding, and Jorg Ott. Where Is My Tag? Unveiling Alternative Uses of the Apple FindMy Service. In *2022 IEEE 23rd International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, pages 396–405. IEEE, June 2022.

[32] 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 *Proceedings of the 29th USENIX Conference on Security Symposium*, pages 1893–1909. USENIX Association, 2020.

[33] Kieron Ivy Turk and Alice Hutchings. Stop Following Me! Evaluating the Effectiveness of Anti-Stalking Features of Personal Item Tracking Devices. In *Proceedings of the 2024 European Symposium on Usable Security*, EuroUSEC '24, pages 1–21. ACM, 2024.

A Phone Settings Required for Unwanted Tracking Notifications

Unwanted tracking notifications on iOS and Android phones only work if all necessary settings are enabled. During the study, we developed the following checklist to verify that an unwanted tracking notifications could be triggered.

Android.

- Google Play services on Android 6.0+
- Bluetooth (on)
- Location services (on)
- Notifications for Google Play Services (on)
- Unknown tracker alerts (on) at *Settings* $\longrightarrow$ *Safety & Emergency* $\longrightarrow$ *Unknown tracker alerts*

iOS and iPadOS.

- iOS or iPadOS 14.5 or later
- Bluetooth (on)
- Airplane mode (off)
- Location Services (on)
- Find My network (on)
- Tracking notifications (on)

B Onboarding Information (RQ2)

Greet participant, introduce myself and introduce topic:
"Hello, thank you for participating in this study about private activity monitors."

Purpose and Consent. Hand out consent sheet, explaining purpose of study and how data is going to be used:
"In this study, we want to test an activity monitor that measures movement, sleep, and stress data with its sensors and analyzes it to create a picture of trends in the data without allowing the collecting entity to identify an individual. An example would be health insurance companies that started giving out activity monitors in recent years but usually do so by collecting data on an individual level. The goal is to develop solutions for private activity monitoring that companies can then use without invading the privacy of customers. While we ask you to carry this activity monitoring device with you for about one day, we want to stress that no one will have access to your raw data, location data, or any other personal data. The data will only be fed to an algorithm after being fully anonymized and the raw data including all of your personal details will be deleted."

Hand Out Tracker. After the consent sheet has been read and signed, hand out activity monitor, and ask participant to carry it around with them as much as possible for the next day.

"To get a picture for our data analysis later and whether it works as expected we would also like you to keep track of the types of activity you perform during the next 24 hours and write it down here."
Give out sheet for activity.

Schedule Next Meeting. *"To ensure that everything works as expected and make sure the collected data so far is usable, I would like to schedule a meeting tomorrow between morning and noon. We can do this either online or in-person — what you prefer."*
Schedule meeting for early next day. Inform them of time and place.
"That is everything. Thank you so far and talk to you tomorrow!"

C Guideline for Interview & Debriefing (RQ2)

Participant should have received unwanted tracking alert. Typically scheduled one day after onboarding. If at any point, participant shows that they immediately made the connection between the unwanted tracking alert and this study, include question from next page.

Greet participant, start audio recording and inform them about this. Ask about unusual experience without hinting at unwanted tracking alert:
"Hello, thank you for taking the time today. Before we get started, did everything go alright on your end?" If they do not mention an unwanted tracking alert, ask more specifically:

1. *"Did anything unusual happen?"*
2. *"Did you receive an unexpected notification?"*
3. *"Anything on your phone?"*
4. *"Did you receive a notification about a tracking device?"*
5. *"Did you receive a notification about an Apple AirTag moving with you on your personal smartphone?"*

As soon as unwanted tracking alert is mentioned, make sure participant explains their thoughts and reactions in as much detail as possible and keep asking follow-up questions when necessary:

- *"What were your first thoughts when receiving the alert?"*
- *"Was it clear what the notification was trying to tell you?"*
- *"How did you feel right after seeing the notification?"*
- *"How did you respond when receiving the alert?"*
- *"(How) did you interact with notification?"*
- *"Did you look for or change any settings?"*
  - If yes: *"Which ones, how, and why?"*
- *"Did you change anything about your device or another device in response?"*

- *"Did you contact anyone in response to receiving the alert?"*
- *"Did you investigate further by navigating through the UI, or researching online/asking people?"*
- *"Did you try to locate the device that was mentioned in the alert? If yes, did you succeed and how?"*
- *"Is there anything else you would like to share about this situation?"*

In case the participant immediately made the mental connection to the study setup ask:

- *"What made it clear to you that the notification must be related to the study?"*
- *"How would you have reacted if you were not participating in this study?"*

If participant never received notification investigate why they did not receive the alert:

- Inquire (or check with them) if either Bluetooth, location services, notifications or Find My had been turned off?
- If one of those is turned off: *"Why have you turned off this setting?"*
- *"Were you aware of the impact in terms of your protections from stalking by changing these settings, i.e., that you would not receive a tracking alert?"*
- *"If you received an alert telling you, an unknown AirTag was moving with you, what would you do and how would you react?"*

Inform participant about true nature of study, explain why deception was necessary. Inform them of their right to withdraw and ask for consent in ongoing study:

"We have not informed you about the true purpose of this study in order to trigger a so-called unwanted tracking alert on your phone and get your thoughts and reactions without you being prepared. If you do not want to continue with this study after receiving this information, you can always withdraw and we will immediately delete all collected information so far. If you choose to continue, you need to sign this consent form and we will move on."

Let them know that they were never being tracked and they can ask questions for clarification. If they agree and sign consent form, continue with next part of the study. Otherwise end interview and delete data, ask for device back.

D Participant Behavior (Study B)

Table 1 reports a summary of participant characteristics and responses to receiving an unwanted tracking notification and locating a hidden AirTag in Study B.

Table 1: Summary of our $N_B = 19$ participants' responses in Study B.

Category	Participants (%)
Participant Overview	
Received Tracking Notification	15 (79%)
Attributed Notification to Study	8 (42%)
Observed Reaction (non-exclusive)	
Investigated	11 (58%)
Sought Help	4 (21%)
Disregarded	7 (37%)
Locating Task (non-exclusive)	
Used Play Sound Feature	17 (89%)
Used Find Nearby Feature ⋆	9 (60%)
Reported Difficulty Hearing Sound	14 (74%)
Reported Confusion with UI	11 (58%)

⋆ if supported

E Guideline for Locating Task (RQ3)

Greet participant, ask to have device returned:
"Hello, thank you for taking the time today. Before we get started, can you please return the device to me?"
Explain locating task and demographics data collection:
"Today, I want to perform a quick locating task with you and then collect some demographic information about you for later data analysis."

Locating Task. Move to the prepared car with the hidden AirTag, only then inform the participant of task:
"Now, I want to perform a quick locating task. For this, imagine the following scenario: You are driving around with your car and when you park the car after arriving at home, you notice an unwanted tracking alert on your phone."
Show picture of unwanted tracking alert.
"You are sitting in your car and want to find the hidden AirTag. Now, use your personal smartphone to locate the AirTag. You can use all features available to you, open anything, and generally nothing is prohibited as long as you don't cause damage."
Start audio recording and inform them about this. Ask them to think aloud and explain everything they do. Remind them of the think-aloud protocol by asking them to explain what they do and nudge them to talk.

After concluding locating task, ask participants for their thoughts:

- *"In a context like this, do you consider the features you used helpful?"*
- *"How did you feel during this experience?"*
- *"How would you rate the anti-stalking features when considering an actual stalking scenario? Consider the*

unwanted tracking alerts, and the features to find an AirTag."

F Demographics Questionnaire

This form collects demographic data as part of your participation in the AirTags study. All your data will remain anonymous and will only be processed for the purpose of this study and then deleted.
Please answer truthfully.

- How old are you?
  free response
- What is your gender?
  Woman, Man, Non-binary, Do not wish to disclose, Other (free response)
- What is your highest educational qualification?
  Secondary school, University entrance qualification, Bachelor (or comparable), Master (or comparable), Other (free response)
- What is your monthly net income?
  Net income is the income that remains after deducting certain expenses from your gross income.
  Under 1000 EUR, 1000-2000 EUR, 2001-3000 EUR, More than 3000 EUR
- What is your relationship status?
  Single, Engaged, Married, Divorced, Widowed, In a relationship/partnership, In an open relationship, Living separately, Other (free response)
- What type of environment do you currently live in?
  Please select the answer that best suits your living situation.
  In a (big) city, In a small town, In a suburb, In a village, Other (free response)
- Which answer best describes your current dating activity or relationship search?
  Active on dating apps/websites, Active dating or relationship search without dating apps/websites, In a new relationship, Not actively looking for dates or relationships but open to them, No current dating activities/Not applicable
- The following image shows an Apple AirTag. This is a location tracker. [Picture of an Apple AirTag]
  Were you familiar with Apple AirTags before participating in this study?
  Yes, I knew them and their functions; Yes, I knew them, but I'm not familiar with them; No, I was not familiar with them
- The following two images show tracking notifications as they are displayed on a smartphone. [Tracking notification Android] [Tracking notification iPhone]
  Did you ever receive a tracking notification before participating in this study?
  Yes, No
- There are reports of AirTags being used for unwanted purposes. One of these unwanted purposes is stalking. In this case, people use AirTags to determine and track the location of other people.
  Stalking is the deliberate and repeated following or harassment of a person whose physical or psychological integrity may be threatened and harmed as a result.
  Were you aware of the problem described above before this survey?
  Yes, I knew about it already; No, I didn't know about it
- Are you currently or have you ever been a victim of stalking using technology?
  Technologies include, for example: location trackers (e.g. AirTags), social media, hidden cameras/microphones.
  Yes, I am currently or have been affected in the past; I have a suspicion, but have not (yet) been able to confirm it; No, I am not and have never been affected; I don't know or am unsure
- *Affinity for Technology (ATI)* scale

G Participant Demographics (Study B)

Table 2 reports aggregated demographic details for participants in Study B. The full questionnaire is available in Appendix F.

Table 2: Aggregated demographic data of our $N_B = 19$ participants in Study B.

Demographics	Category	Participants (%)
Age	18 to 29	13 (68%)
	30 to 49	4 (21%)
	50 and above	2 (11%)
Gender	Man	8 (42%)
	Woman	11 (58%)
Interview Language	German	15 (79%)
	English	4 (21%)
Highest Education	Secondary school	1 (5%)
	High school	6 (32%)
	Bachelor's degree (or equivalent)	9 (47%)
	Master's degree (or equivalent)	3 (16%)
Monthly Net Income	Below 1,000€	11 (58%)
	1,000€ to 2,000€	2 (11%)
	2,001€ to 3,000€	5 (26%)
	Above 3,000€	1 (5%)
Relationship Status	Single	7 (37%)
	In a relationship	8 (42%)
	Married	4 (21%)
Dating Activity	Actively dating	1 (5%)
	In a new relationship	1 (5%)
	Open but not actively dating	6 (32%)
	Not dating/applicable	11 (58%)
Type of Residence Area	Big city	13 (68%)
	Small city	4 (21%)
	Suburb	1 (5%)
	Countryside	1 (5%)
AirTags Familiarity	Familiar with AirTags	9 (47%)
	Heard about AirTags	7 (37%)
	Unfamiliar with AirTags	3 (16%)
Location Tracker Usage (*not collected from all participants*)	Used AirTags	7 (37%)
	Used other trackers	1 (5%)
	Does not use trackers	8 (42%)
Previously received tracking notification	Yes	4 (21%)
	No	15 (79%)
Knew about AirTag misuse for stalking	Yes	11 (58%)
	No	8 (42%)
Previously affected by technology-aided stalking	Yes	2 (11%)
	No	16 (84%)
	Unsure	1 (5%)