




Poster: Will our Colleagues Detect the AirTag? Let’s Check (Consensually).

Dañiel Gerhardt 
CISPA Helmholtz Center
for Information Security
and Saarland University

Matthias Fassel 
CISPA Helmholtz Center
for Information Security

Katharina Krombholz 
CISPA Helmholtz Center
for Information Security

1 Introduction

Since their release, AirTags have been misused for stalking and other malicious purposes [2, 5, 9]. Their small size, affordability, availability, and precise tracking functionality facilitate the invasion of peoples’ privacy. To combat misuse, Apple implemented multiple anti-stalking features that inform potential victims and help them find and disable the location tracker.

One of the primary anti-stalking features is *unwanted tracking alerts*. These smartphone notifications – as shown in Figure 1 – alert users that they have been followed by an AirTag or other *Find My* device for some time.

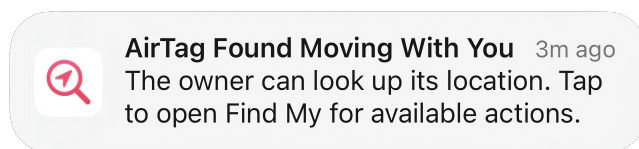


Figure 1: Unwanted Tracking Alert for AirTag on iOS 17.4

It is crucial to inform potential stalking victims quickly and in an easy-to-understand manner. Only then can they avoid further harm from a stalker who gains knowledge about their whereabouts and movement patterns. When AirTags were released, only selected Apple devices could send *unwanted tracking alerts*. To make the alerts platform-independent, Google introduced *unknown tracker alerts* for Android in August 2023 via Google Play services, followed by their own *Find My Device* network in April 2024.

Previous work has analyzed the AirTag’s hardware and the *Find My* network for a solid technical understanding of the technology [4, 6, 7]. However, verifying that currently available anti-stalking features effectively curb misuse is also necessary. Especially since the proposed best practices and protocols [3] imply that Google and Apple will use these anti-stalking features for their respective *Find My* networks going forward.

This preliminary work evaluates the reliability of *unwanted tracking alerts* across platforms. We performed an experiment

with $N = 50$ employees at our institution. We found that tracking alerts are very reliable on iOS devices and not as reliable on Android devices, indicating a different implementation of *unwanted tracking alerts* or hardware limitations.

2 Methodology

We investigate the reliability of *unwanted tracking alerts* as a first step towards evaluating existing anti-stalking features with the following research question: *How reliable are unwanted tracking alerts on iOS and Android?* Our findings could be used for recommendations and designing improved anti-stalking features.

Study procedure. We gave $N = 50$ participants (employees from our institution) an AirTag to take home and keep with them for two days or until they receive an *unwanted tracking alert* on their smartphone. We chose the two-day time window to ensure an alert could even be triggered when the trackers’ MAC address changes every 24 hours. We ensured that participants’ device settings allowed *unwanted tracking alerts*, i.e., having location services, *Find My iPhone* (iOS) or *Unknown tracker alerts* (Android), and Bluetooth enabled [1, 8].

Data collection. 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 alert*, and the environment in which they received it. Participants shared additional qualitative insights about their experience, which we partially report in the Discussion. If participants were not alerted, 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 alert. We used descriptive statistics, i.e., median, average, and standard deviation, to describe the reliability of

unwanted tracking alerts in this experimental setup. Additionally, we use statistical hypothesis testing to understand which factors affected the reliability of unwanted tracking alerts, e.g., we apply a Fisher’s exact test to check if unwanted tracking alerts trigger more consistently on Android or iOS.

Ethical considerations. We informed participants about the purpose of the study, the capabilities of AirTags, and our data handling procedures. All participants signed consent sheets that explained the details. We used the four-eye principle to prevent any single researcher from tracking the participants’ location. We could not compensate participants with money because they were employees at our institution. Our institution’s Ethical Review Board (ERB) approved this study, and we adhered to the GDPR and German privacy laws.

3 Results

We recruited $N = 50$ participants from our institution, 25 with iOS and 25 with Android. One potential participant had unsupported hardware and one declined to participate after we informed them about the study procedure.

iOS devices. Most participants ran iOS 17, with the latest being 17.2.1 and the oldest 16.5.1. The hardware ranged from iPhone 8 (2017) to iPhone 15 Pro (2023).

All 25 participants received one or multiple *unwanted tracking alerts* within the two-day window. It took between 1 and 24 hours for the alert to trigger, with an average of 4 hours 58 minutes and a median of 4 hours. Most participants received an alert after arriving at home, while two received the alert at their place of work.

Android devices. As *unknown tracker alerts* are part of Google Play services, we also collected version information about it. The Google Play services versions ranged from 23.42.12¹ to 23.49.14², and the Android versions from 10 to 14. The oldest hardware was a Samsung Galaxy J6 (2018) and the newest 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 that received an alert, it took 11 hours 51 minutes on average, with a median of 4 hours 30 minutes. Most participants received an alert after arriving home, with two exceptions receiving the alert outside their homes.

Reliability difference. We used a Fisher’s exact test to compare the success rate of unwanted tracking alerts on iOS and Android. It resulted in a p-value $p < .001$, meaning that the observed reliability difference is likely not random. On An-

droid, no discernible trend in hardware, OS, or Google Play services version contributed to whether an alert was triggered.

4 Discussion

Unreliable tracking alerts put Android users at risk. The iOS and Android implementations are proprietary, so we cannot explain the reliability differences. Google’s approach is likely more challenging to implement since, compared to Apple, it needs to work for a broader set of devices.

Our data suggests that Android users cannot rely on receiving a notification about potential stalking events. Hence, the much lower reliability of *unknown tracker alerts* on Android puts these users at an increased risk. They must either discover unknown trackers by the sound they emit or stumble upon them by accident. Time is of the essence when a stalker collects as much data as possible because early detection gives victim more chances to protect themselves and seek support. The responsibility of discovering a tracking device should not lie solely on the victim.

Triggering alerts at home is too late. *Unwanted tracking alerts* were often triggered after a participant arrived home. This is an intended behavior built on the *significant locations* feature on iOS. Our data suggests that Android uses a similar approach. While this helps avoid false positives, it also means that victim will only be notified after the tracking device makes their home location known to the stalker.

Users unintentionally limit unwanted tracking alerts through unrelated changes in the settings. In this experiment, we ensured the correct settings on participants’ smartphones. Many participants would otherwise not have received the notification because they disabled Bluetooth and Location Services, regularly enabled airplane mode, opted out of the *Find My* network, or turned off seemingly unnecessary notifications. Participants mostly changed these settings for unrelated reasons and were unaware how this impacts *unwanted tracking alerts*.

Other (non-)users are also at increased stalking risks because unwanted tracking alerts are not available on all devices. Potential stalking targets also include people that either do not have an iPhone or an Android device without Google Play services. That could be users with another phone or no phone. Their device might not support iOS 14.5 or Android 6.0 and later, which is required for the alerts feature.

Even when the *unwanted tracking alerts* work as intended, users need to be able to understand them and act accordingly. The provided information should help protect them from further harm, even without technical knowledge or prior experience with AirTags. Further research is necessary to investigate users’ understanding and reactions when using the current anti-stalking features.

¹(190400-574052649)

²(190400-590296185)

References

- [1] Google. Find unknown trackers - Android Help, April 2024. <https://support.google.com/android/answer/13658562?hl=en>.
- [2] The Guardian. '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>.
- [3] Brent Ledvina, Zachary Eddinger, Ben Detwiler, and Siddika Parlak Polatkan. Detecting Unwanted Location Trackers. Internet Draft, Internet Engineering Task Force, December 2023.
- [4] Jeremy Martin, Douglas Alpuche, Kristina Bodeman, Lamont Brown, Ellis Fenske, Lucas Foppe, Travis Mayberry, Erik Rye, Brandon Sipes, and Sam Teplov. Handoff All Your Privacy – A Review of Apple’s Bluetooth Low Energy Continuity Protocol. In *Proceedings on Privacy Enhancing Technologies*, PETS '19. PoPETS, October 2019.
- [5] BBC News. Apple sued by women over AirTag stalking, December 2022. <https://www.bbc.com/news/technology-63880969>.
- [6] Thomas Roth, Fabian Freyer, Matthias Hollick, and Jiska Classen. AirTag of the Clones: Shenanigans with Liberated Item Finders. In *IEEE Security and Privacy Workshops (SPW)*. IEEE, May 2022.
- [7] 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*, July 2023.
- [8] Apple Support. What to do if you get an alert that an AirTag, Find My network accessory, or set of AirPods is with you, April 2024. <https://support.apple.com/en-us/HT212227>.
- [9] The New York Times. 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>.