Can't Keep Them Away: The Failures of Anti-Stalking Protocols in Personal Item Tracking Devices

Kieron Ivy Turk[1][0000−0002−4705−4749], Alice Hutchings[1][0000−0003−3037−2684], and Alastair R. Beresford[1][0000−0003−0818−6535]

University of Cambridge, Cambridge, UK
{kst36, ah793, arb33}@cam.ac.uk

Abstract. A number of technology companies have introduced personal item tracking devices to allow people to locate and keep track of items such as keys and phones. However, these devices are not always used for their intended purpose: they have been used in cases of domestic abuse and stalking to track others without their consent. In response, manufacturers introduced a range of anti-stalking features designed to detect and mitigate misuse of their products. In this paper, we explore common implementations of these anti-stalking features and analyse their limitations. In other research, we identified that very few people use anti-stalking features, even when they know that someone might be tracking them and are incentivised to evade them. In this paper, we additionally identify several failures of the features that prevent them from performing their intended purpose even if they were in use. It is impossible for anti-stalking features to identify the difference between 'bad' tracking and 'good' tracking. Furthermore, some features work on some types of phones for some types of tracking devices, but not all work on all phones for all trackers. Some anti-stalking features are not enabled by default, and some require manual intervention to scan for devices. We provide suggestions for how these features could be improved, as well as ideas for additional anti-stalking features that could help mitigate the issues discussed in this paper.

Keywords: Domestic Abuse · Stalking · Tech Abuse

1 Introduction

Personal item tracking devices have recently surged in popularity with the introduction of Apple's AirTag. The intended use of these devices is to attach them to items such as keys, wallets, bags or luggage to be able to locate them quickly when misplaced. The devices can be located locally through Bluetooth and sound alerts, and remotely via devices owned by others.

Item trackers quickly began being used for malicious purposes, with news outlets starting to report the misuse of AirTags in 2021. In intimate relationships, abusers can set these devices up on their own phone, and then attach them to the

victim's possessions so that they can track them remotely [2]. In late 2022, Apple were sued by a pair of women who were stalked by partners using AirTags [10]. Some people have also used these devices for stalking strangers, and planted them on cars so they can see where they are parked later and steal them [3, 4, 11].

People then conducted informal experiments to test the ease of using different tracking devices for stalking. Hill [9] planted a large number of tracking devices on her husband to see how many he could find and how well she could track him throughout the day. Fowler allowed a colleague to stalk him to see the anti-stalking features in action and found them lacking in several respects [5]. Scott ran a game for an hour each in London and Nottingham to have one player attempt to complete tasks while another player tracked them, testing the real-time tracking effectiveness of the trackers [16, 17].

Manufacturers responded to these actions with the introduction of anti-stalking features: additions to their devices so that people would be able to identify if a tracker was tracking them without consent. These features centered around detecting trackers moving with a user while away from the owner, alerting them to the tracker's presence after a given period. The user can then make the tag play a sound or use Bluetooth to try and locate it in a similar fashion to the owner. There was some negative press around the ineffective implementations of these features [2, 9], so manufacturers later made improvements such as increasing the speaker's volume when playing an alert (e.g., [1]).

In response to the insufficient features provided by Apple, Heinrich et al. created their own AirGuard application to detect unwanted trackers [8]. Their app is able to detect trackers much faster than Apple's systems and is also able to detect trackers in scenarios where the provided anti-stalking features failed.

We argue these anti-stalking features are ineffective despite improvements to their design. In this paper, we discuss the different implementations of these features across a range of popular models of item tracking devices. We then identify issues across implementations of these devices in addition to issues unique to certain manufacturers which make the anti-stalking features insufficient for their intended purpose.

2 Threat Models

There are multiple important threat actors to consider for different misuses of item tracking devices. In §2.1, we discuss the different scenarios in which tracking devices have been used and the objectives of the offender in each case. We then explore the threat model of the offender in §2.2 and look at the capabilities and relevant information about the victims in §2.3.

2.1 Objectives of Stalking

One common scenario in which item trackers are misused is domestic abuse. In this case, the offender plants trackers on their partner to track them throughout

the day. They do not need to learn their home or work locations but will learn where they go during the day and their current location. In some cases, trackers may be used by abusers to detect where survivors have relocated to after leaving an abusive relationship. We are aware of cases where trackers have been planted on children's belongings during visitation in order to find their new home address. It is significantly easier to plant trackers in these cases due to the proximity to the victim and their possessions.

A similar scenario involves stalkers tracking the locations of strangers. In addition to learning the victim's current location and daily activities, they will aim to uncover their home and possibly work locations, which are unlikely to be known before commencing tracking. On the other hand, it is more difficult to plant trackers on the victim, as the offender is only able to access the victim and their possessions during encounters in public spaces.

The final scenario in which tracking devices have been abused is for theft, most commonly of vehicles. In this case, offenders plant trackers on wealthy victims or their possessions (such as by targeting sports cars) and see where the tracker ends up at a later point in time. This provides opportunities to steal the vehicle when it has been parked in a less public space and also identifies the residence of people who are likely to have other valuable possessions to steal.

2.2 Modelling the Offender

Prior research on domestic abuse victims introduced the "UI-bound adversary" threat model [6]. Our first threat actor follows this model: they can only use an application or product through the user interface provided. Here the threat actor exploits the functionality of a device for their own benefit (and to the victim's detriment). In the case of item tracking devices, this translates to an offender who uses trackers and related applications without modification. The abuse of this technology occurs when the offender is the owner of a tracking device, and this device is placed on the victim or among their possessions without their knowledge.

The alternative threat actor in this case is an adversary who is capable of modifying the tracker after they have purchased it. There are online guides for modifications such as removing the Apple AirTag's speaker, which prevents one of the main methods of locating unwanted AirTags. These modified trackers are also sold online [14], more readily enabling the abuse of AirTags for stalking and theft.

2.3 Modelling the Victim

Domestic abuse victims and survivors often lack detailed technical understanding, which leads to the misconception that their abusers are "hackers" and that the victim has little control over their situation [12]. Victims can be modelled as "UI-bound" and limited to interactions available through the interfaces provided to them. Victims and survivors will own a variety of different devices, and safety tools need to cater to all of these. They may own iOS or various brands of

Tracker	Advertised Range	Measured Range	Location Updates Near	Background Scan	Alerts After	Manual Scan
Airtag	10m	25.8m	iPhones	iPhones	4-8 hours	Android
SmartTag	120m	73m	Galaxy	Galaxy	4 hours	✓
Tile Sticker	45m	65m	Tile User	✗	—	✓
Chipolo One	60m	56m	Chipolo User or iPhone	iPhones	4-8 hours	✗

Table 1. Mechanisms to Detect Each Type of Item Tracker

Android devices, and any anti-stalking interventions need to be easily accessible on all of these devices.

3 Existing Anti-Stalking Features

There is a wide range of consumer item tracking devices available. For our research, we focused on four brands of trackers which all have anti-stalking features: Apple AirTags, Samsung SmartTags, Tile trackers, and Chipolo trackers. AirTags and SmartTags are tied to their companies' phone brands, while Tile and Chipolo are instead associated with their own apps.

The main common anti-stalking features include background and manual scanning for trackers with alerts when an unknown tracker is following a user, using Bluetooth to see the distance and sometimes direction to a tracker, and making the device emit a sound to help locate it. In addition to features provided by manufacturers, there is also a third-party app called AirGuard which can be used to locate certain types of trackers.

3.1 Scanning for Trackers

Anti-stalking features most commonly allow a user to detect another user's tracker has been physically near them for an extended period. If such a tracker is detected, the device alerts the user and provides them with means to detect the tracker using similar functionalities as provided to the tracker's owner. An overview of the connection range of the devices and the types of scans available are shown in Table 1.

In many cases, potentially malicious trackers can be detected by a smartphone which uses Bluetooth to listen in the background for announcements from nearby trackers. Potential malicious trackers are detected by spotting the same tracker at different locations. The user is then notified that a tracker is following them. Most implementations will only do this when the tracker has been separated from its owner to avoid false positives. Galaxy phones and iPhones both integrate background scanning into the phone's OS, while Chipolo provides background scanning through their app. iPhones additionally provide background scanning for Find My-compatible devices such as Chipolo. The effectiveness of

Tracker	Advertised Volume (dB)	Maximum Measured Volume in... (dB)			
		Open Area	Coat Pocket	Bag (at 10cm)	Bag (at 5m)
AirTag	60	86	76	40	37
Galaxy SmartTag	85-96	89	84	68	54
Chipolo One	120	96	80	65	48
Tile Sticker	85-114	92	76	61	40

Table 2. Volume of Each Type of Tracker in Decibels. Background Volume is 34dB.

both of these approaches depends on the number of phone owners or app users in the area.

Several anti-stalking features also provide manual scanning capabilities, where the user initiates a scan to identify nearby trackers. Users have to initiate a manual scan from multiple locations to identify which trackers have moved with them to the new location. Samsung and Chipolo provide this feature through their respective apps, and Apple provide a dedicated Tracker Detect app as the mechanism for Android users to be able to detect unwanted Find My-compatible trackers such as AirTags and Chipolo trackers.

An improvement over the industry-led anti-stalking features is Heinrich et al.'s [8] AirGuard app. This was developed in response to Apple's limited anti-stalking features. By reverse-engineering how the Find My network identifies and reports the location of AirTags, they can detect when a tracker is following a person. Their application allows both background and manual scanning and has been updated since the original paper to also allow detection of Tile trackers. They are able to detect trackers in approximately 30 minutes, additionally identifying trackers in scenarios that the Apple detection failed to find.

3.2 Sound Alerts

All tracking devices have a built in speaker to play an alert sound and help locate the tracker. This allows the owner to quickly find the device when they are close to it. When AirTags have been separated from the owner for over 3 days, the device will start playing a sound to notify tracking victims of its presence.

3.3 Bluetooth Location

All trackers allow the owner to use Bluetooth to help them locate their tracker. Bluetooth provides the distance from the tracker once it is in connection range, allowing users to find the tracker. AirTags additionally provide a proprietary means to determine the direction of the tracker. When a user is alerted to an unwanted tracker, they can use this feature to help locate it.

4 Failures of Anti-Stalking Features

4.1 Scanning Mechanisms

Background scanning via manufacturer-produced anti-tracking features has a long time to alert users to detected trackers. Apple originally used a random period between 8-24 hours[1], though have since updated this to 4-8 hours[2]. In the worst case for the trackers we examined, it can take up to a day for users to be alerted to unwanted trackers; in the best case, it takes approximately 2 hours. This provides the owner of the tracker updates on the tracker's location for an extended period without concern of it being found. AirGuard significantly improves upon this with approximately half an hour to detect a tracker, which manufacturers should aim towards.

Furthermore, background scanning is disabled by default for some brands of tracker, including the Samsung SmartTags. Detecting these trackers requires installing their app and going through settings to enable the background scanning. This is problematic as some users will assume that by downloading the app they are safe from unwanted trackers, however in reality they need to complete further steps to be able to detect trackers.

Manual scanning for unwanted trackers is difficult to use effectively. Users have to suspect they are being tracked, know which brand(s) of trackers may be following them, and run manual scans in different locations to identify that they are being tracked. Our recent work found that even users who knew they were being tracked did not use anti-stalking features, so it is even more unlikely that the average user will perform these extra steps to identify trackers. In addition, Apple's Tracker Detect App does not have background scanning, forcing Android users to use manual scanning. This makes it significantly harder for a victim to identify trackers placed on them compared to background scanning.

There are distinct applications for different types of tracker. Users who are attempting to locate trackers have to install a different app for each type of tracker they are trying to detect (with the exception of iPhone users being able to detect all Find My-compatible trackers by default). This requires awareness of the different possible ways that the user may be tracked, in addition to being concerned enough about being tracked to install these apps. The exception is the AirGuard app which can detect both Find My compatible trackers and Tile trackers, however this does not cover all possible devices.

4.2 Locating Detected Trackers

There are two primary mechanisms for locating a detected unwanted tracker: sound alerts and Bluetooth. Bluetooth detection is limited by the range of the tracker being used, and many systems will simply provide the distance to the

[1] https://www.theverge.com/2022/2/10/22927374/apple-airtag-safety-update-stalking

[2] https://www.macworld.com/article/606934/apple-airtag-problem-notifications-android-sound.html

tracker in meters. This makes it difficult to locate the tracker in circumstances where the Bluetooth location will simply state "$\leq$ 1m away" or "Nearby".

The small size of the different trackers makes it hard to produce a loud sound, as shown in Table 2. Most trackers produce a sound between 90–100dB in an open environment, but are easily muffled down to 40–65dB, and make the sound alert feature largely ineffective. There are also step-by-step guides published online which describe how to disable the speaker[3]. Furthermore, Heinrich et al. [8] found that AirTags only ring out for 15 seconds every 6 hours, giving a very brief window for the sound alerts to be noticed. This makes it incredibly difficult for this feature to be effective.

4.3 Distinguishing Misuse from Intended Use

One underlying issue with the effectiveness of anti-stalking features is identifying when a tracker is being used maliciously rather than intentionally. False positives are relatively common, with family members and people travelling together receiving alerts about other's tracker devices. The existing workarounds for this are allow-listing certain devices and avoiding notifications when the owner is near to their tracker.

Another possible type of false positive is theft. If an item with a tracker on is stolen, the owner can use the device to locate the thief — however, anti-stalking features will alert the thief to the tracker and make it easier for them to remove it. In this case, the tracker is being used as intended, but it will appear as though it is being used to stalk someone else. We note, however, that research shows stolen items are usually disposed of quickly, often within the hour [15].

Furthermore, in abusive relationships the owner is frequently close to the device making it appear as a legitimate use. An abusive partner can also take advantage of allow-list features through the victim's phone (as they commonly will get access to their partner's technology during the relationship [7]) to make it appear as a legitimate use of the device. In all of these scenarios, it is not possible to accurately determine legitimate use from misuse due to overlap with the other scenarios.

5 Possible Improvements

We have identified a wide range of existing issues in the anti-stalking features of item tracking devices. In this section, we discuss our suggestions for how the features can be improved in the future.

5.1 Improving Scanning

Scanning for unwanted trackers is the primary anti-stalking feature currently in use. Despite this, our prior work identified that almost no users download and use

[3] `https://mashtips.com/remove-airtag-speaker/`

these features, even in the extreme case where they know they will be tracked. To improve on this, the anti-stalking features need to be enabled by default wherever possible, and should be available to users of all devices regardless of platform. The ideal case would be to integrate the anti-stalking features into mobile phone operating systems, as Apple currently does for detecting AirTags in iOS.

Furthermore, all applications offering anti-stalking features should provide background scanning as the primary mechanism for detecting trackers. Currently, the Tile and Tracker Detect apps only provide manual scanning, which we find to be too difficult to use effectively. It would be beneficial for these to be supplemented or replaced with background scanning for unwanted trackers.

There are some artificial limitations on alerts to users that an unknown tracker has been identified. For example, Apple waits for the user to either return to their home location or for many hours to pass before notifying users that a tracker is following them, despite often identifying the unwanted devices several hours earlier. These restrictions slightly reduce the false positive rate but have a severe impact on the tracked user, as the person tracking them will be able to follow them throughout the day and discover their home address if not already known before the user is made aware of the tracker's presence. These artificial restrictions should be removed in the interest of user's safety and privacy.

5.2 Improving Alerts

After identifying that an unwanted tracker is present, the user is reliant on a small selection of features to locate it: making the tracker play a sound, and using Bluetooth to see the distance from the tracker. Not all applications provide both of these features to users who have identified an unwanted tracker; the Tile application specifically provides neither, and just reports on the quantity and models of trackers found. The sound alerts and Bluetooth location need to be universally available to enable users to find these devices after they become aware of their presence.

The sound alerts produced by the trackers are easily muffled by coats, bags, and other objects they may be placed in. This is an issue as these are common hiding places for trackers, and if the sounds are inaudible when the tracker has been hidden then they are of no use to the stalking victims. Improving the volume is a necessary step to locating the trackers. Alternatively, manufacturers may consider adding some hardware to the trackers to make them easier to locate, such as LEDs so the trackers are more easily spotted visually, or vibration as an alternative way to cause noise.

The alerts produced by Apple's AirTags after they have been separated from their owner are an excellent idea with poor execution. Forcing trackers to play sounds when they are not being used as intended provides a useful backup mechanism for noticing unwanted trackers when scanning fails. However, Apple's implementation of this feature only makes trackers play a sound for 15 seconds every 6 hours after the device has been separated from the owner for at least 3 days. These alerts need to ring out for a longer period and with higher frequency,

ideally with a shorter wait time after the tracker is separated from its owner. Otherwise, this is a useful feature and should be implemented for other brands of item tracking devices.

Apple additionally provides directed location to the trackers as an additional improvement over the standard anti-stalking feature set provided by other devices. This makes use of the Ultra-WideBand (UWB) antennae present in both the AirTag and modern Apple phones. This is a significant improvement on the simple distance estimate provided by other devices using Bluetooth, as it allows users to move directly towards the device instead of having to play "hot or cold" with the tracker. Adding this feature to non-Apple trackers would be beneficial for locating the tracking devices.

5.3 Reducing Accuracy of Tracking Devices

While improvements on existing anti-stalking features would significantly benefit users, there are additional possible features that could impede the use of tracking devices for stalking. One possibility would be to limit the accuracy of the tracker's current location once it has been detected as potentially malicious. This would prevent the owner of the tracker from having accurate location data of the victim when they are stalking them, reducing the impact of this malicious use of trackers.

An alternative to limiting the accuracy of the location provided would be to broadcast false locations for the tracker after it has been identified as following a user who does not own it. This could be implemented by providing a broad range of possible locations for the tracker instead of a precise location, or by providing previous locations for the tracker so that up-to-date locations are not available. These would both interfere with the stalker directly rather than relying on users to find the tracker and intervene.

A third possibility would be to restrict the availability of remote location tracking for items until users prove their identity to the platform. This would add a barrier to remote tracking for stalkers, and would also ensure that the platform has access to the stalker's identity to pass on to law enforcement if required. Tile recently announced an approach which overlaps with this, which is their "anti-theft mode" [13]. This mode prevents the tracking device from being detected by Tile's "Scan and Secure" manual scanning feature to avoid thieves learning about the presence of a tracker on a stolen item, however it requires the user to register with 2FA including biometric data, provide government ID, and agree to additional terms to use the feature. These terms allow Tile to provide this information to law enforcement at its discretion, and Tile are additionally threatening to sue anyone who abuses the feature.

6 Conclusions

In this paper, we have detailed the implementations and failures of anti-stalking features in a range of different personal item tracking devices. Some of these

issues are shared across different devices, such as the limitations of manual scanning, while others are specific to certain manufacturers, such as the absence of background scanning on Android for AirTags or disable background scanning in the Samsung SmartThings app. The limitations of these features, in combination with our study showing that they are rarely used even in extreme cases where people know they are being tracked, show that there is a need for these existing features to be improved and additional features to be added to prevent the malicious use of item tracking devices.

References

1. Apple: An update on airtag and unwanted tracking. https://www.apple.com/uk/newsroom/2022/02/an-update-on-airtag-and-unwanted-tracking/ (2022)
2. Cahn, A.F.: Apple's AirTags are a gift to stalkers. Wired (2021)
3. Charlton, H.: Apple's AirTag item trackers increasingly linked to criminal activity. MacRumors (2021)
4. Cole, S.: Police records show women are being stalked with Apple AirTags across the country. Motherboard (2022)
5. Fowler, G.A.: Apple's AirTag trackers made it frighteningly easy to 'stalk' me in a test. Washington Post (2021)
6. Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T., Dell, N.: "A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology. In: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. p. 1–13. CHI '18, Association for Computing Machinery, New York, NY, USA (2018). https://doi.org/10.1145/3173574.3174241, https://doi.org/10.1145/3173574.3174241
7. Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T., Dell, N.: "A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology. In: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. p. 1–13. CHI '18, Association for Computing Machinery, New York, NY, USA (2018). https://doi.org/10.1145/3173574.3174241, https://doi.org/10.1145/3173574.3174241
8. Heinrich, A., Bittner, N., Hollick, M.: AirGuard – Protecting Android users from stalking attacks by Apple Find My devices (2022). https://doi.org/10.48550/ARXIV.2202.11813, https://arxiv.org/abs/2202.11813
9. Hill, K.: I used Apple AirTags, Tiles and a GPS tracker to watch my husband's every move. New York Times (2022)
10. Holpuch, A.: Two women sue Apple over AirTag stalking. The New York Times (2022)
11. Mac, R., Hill, K.: Are Apple AirTags being used to track people and steal cars? The New York Times (2021)
12. Maher, J., McCulloch, J., Fitz-Gibbon, K.: New forms of gendered surveillance?: Intersections of technology and family violence, pp. 14–27. Routledge Studies in Crime and Society, Routledge, United Kingdom, 1st edn. (2017). https://doi.org/10.4324/9781315441160-2
13. Perez, S.: Tile takes extreme steps to limit stalkers and thieves from using its bluetooth trackers. TechCrunch (2023)

14. Piper, D.: These custom Apple AirTags are causing serious alarm. Creative Bloq (2022)
15. Stevenson, R.J., Forsythe, L.M., Weatherburn, D.: The stolen goods market in New South Wales, Australia: An analysis of disposal avenues and tactics. British Journal of Criminology **41**(1), 101–118 (2001)
16. Tom Scott plus: Can you stalk someone with an Apple AirTag? `https://www.youtube.com/watch?v=GmC05wOc5Dw` (2022)
17. Tom Scott plus: He tracked me with an AirTag. now it's my turn. `https://www.youtube.com/watch?v=NuEgjAMfdIY` (2022)