Please Unstalk Me: Understanding Stalking with Bluetooth Trackers and Democratizing Anti-Stalking Protection

Alexander Heinrich
Secure Mobile Networking Lab
Department of Computer Science
TU Darmstadt, Germany
aheinrich@seemoo.de

Leon Würsching
Secure Mobile Networking Lab
Department of Computer Science
TU Darmstadt, Germany
lwuersching@seemoo.de

Matthias Hollick
Secure Mobile Networking Lab
Department of Computer Science
TU Darmstadt, Germany
mhollick@seemoo.de

ABSTRACT

While designed to locate lost items, Bluetooth trackers are increasingly exploited for malign purposes, such as unwanted location tracking. This study probes deeper into this issue, focusing on the widespread use of these devices for stalking. Following a dual approach, we analyzed user data from a widely used tracking detection app (over 200,000 active installations) and conducted a comprehensive online survey (N=5,253). Our data analysis reveals a significant prevalence of trackers from major brands such as Apple, Tile, and Samsung. The user data also shows that the app sends about 1,400 alarms daily for unwanted tracking. Survey insights reveal that 44.28% of stalking victims had been subjected to location tracking, with cars emerging as the most common hideout for misused trackers, followed by backpacks and purses. These findings underscore the urgency for more robust solutions. Despite ongoing efforts by manufacturers and researchers, the misuse of Bluetooth trackers remains a significant concern. We advocate for developing more effective tracking detection mechanisms integrated into smartphones by default and creating supportive measures for individuals without smartphone access.

KEYWORDS

Bluetooth Trackers, Stalking, Unwanted Tracking

1 INTRODUCTION

Bluetooth trackers are small, coin-size devices that can be attached to valuables to protect against loss and theft. Tracker owners can utilize crowd-sourced offline finding networks to locate their trackers precisely and, ideally, recover lost valuables, such as bags or keys [26]. However, Bluetooth trackers have been increasingly misused for unwanted tracking: Malicious actors can hide trackers to follow the location of their victim with a short delay of only 15 minutes [26], which has been classified as a method of stalking [19, 51]. Stalking incidents using unwanted tracking with Bluetooth trackers by intimate partners, parents, and criminals have been documented and reported in many news outlets [5, 13, 21, 34]. In at least three cases, this unwanted tracking resulted in the death of the tracked victim [8, 9, 38].

Our definition of stalking follows previous studies and includes episodes of harassment involving intrusive behavior and provoked fear [19, 51]. We did not set a minimum required time frame for the actions of a stalker and classify a single occasion of unwanted tracking as stalking.

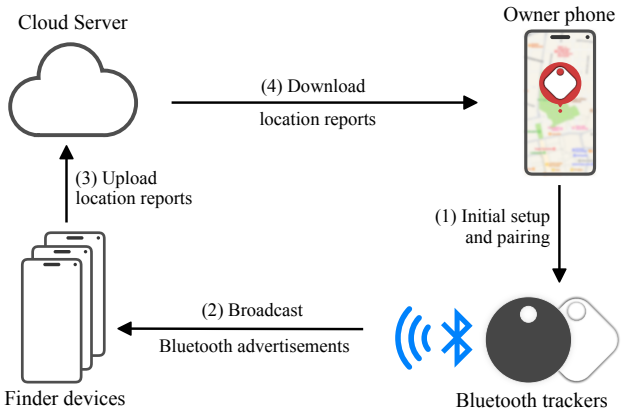

Figure 1: Offline finding network behavior; adapted from [26].

The manufacturers of Bluetooth trackers have acknowledged the misuse of their trackers, but so far, they have only delivered inadequate solutions. Almost all solutions require a victim to manually scan for a tracker on their phone while adding additional hurdles, like an artificial 10-minute delay or the requirement to walk while scanning [2, 56]. Fortunately, the research community developed several apps to identify trackers and warn users about stalking attempts [6, 24, 39].

In this work, we study the prevalence of Bluetooth trackers and how they are misused for unwanted tracking and stalking. We conduct a large-scale online survey to understand people's perceptions of Bluetooth trackers and connected them to general questions about prior stalking experiences. Additionally, we collect and evaluate user data of the tracking detection app AirGuard, which warns users when an unknown tracker is following them. Combining our studies, we aim to answer the following research questions:

- **RQ1:** How severe is the problem of tracker misuse for location stalking?
- **RQ2:** Which measures are considered effective stalking protection?
- **RQ3:** What are the privacy implications for benign tracker owners?

Proceedings on Privacy Enhancing Technologies 2024(3), 353–371

https://doi.org/XXXXXXX.XXXXXXX

Our user data analysis concluded that Apple AirTags were the most prevalent trackers, while Tile and Samsung trackers were also widespread. In the survey, we found that 19.13% of our respondents have previously experienced stalking, and that 8.47% were a victim to location tracking.

The contributions of our work are as follows:

(1) We analyze the user data of 14,739 AirGuard users, a tracking detection app with over 200,000 installations for Android and iOS (Section 5).
(2) We conduct and evaluate a large-scale online survey (N=5,253) about the misuse of Bluetooth trackers, stalking experience and anti-stalking protection (Section 6).
(3) We identify potential privacy risks for innocent tracker owners, allowing long-term identification of them based on the trackers they are using.
(4) We publish the results of the user data analysis in an accumulated manner, sharing insights with the research community while protecting the participants' privacy.[1]

2 BACKGROUND

This section introduces Bluetooth trackers, our threat model, an overview of laws concerning stalking, the tracking detection algorithm, and the app used for our user data collection.

2.1 Bluetooth Trackers

In this work, we concentrate on Bluetooth trackers, which are available from a range of manufacturers. Compared to GPS trackers, Bluetooth trackers are smaller and have a longer battery life. This allows them to be attached to many valuables but also increases the risk of misuse as they are easier to hide.

2.1.1 Offline Finding. All Bluetooth trackers in this work follow a similar behavior, as shown in Figure 1: When someone purchases a tracker, it first needs to be paired with the owner's phone. (1) This initial setup is performed by the manufacturer's app. (2) The tracker starts sending out Bluetooth Low Energy (BLE) advertisements, i.e., broadcast BLE packets containing data to identify the tracker. A Bluetooth tracker does not have a GPS sensor, so a network of *finder devices* is necessary to locate it. In most cases, *finder devices* are smartphones participating in the offline finding network of the tracker manufacturer. When a *finder device* scans for BLE advertisements and discovers a tracker, it will use its own GPS hardware to get its current location. (3) The *finder device* forwards this location with the data necessary to identify the tracker to the tracker manufacturer's server. (4) The owner can now use the tracker manufacturer's app to locate the tracker.

2.1.2 Apple Find My Trackers. Apple has offered the Apple AirTag since 2021, which is part of a vast offline finding network with close to one billion iPhones acting as finder devices [27]. Apple has opened the Find My network to third-party device manufacturers, which can offer trackers, headphones, and other devices locatable with Apple's finder devices. These trackers must follow a specification from Apple, which dictates how these trackers interact with the Find My network. Therefore, AirTags and third-party Find My trackers behave in the same way.

[1] https://github.com/seemoo-lab/Please-Unstalk-Me

The initial setup between the tracker and the iPhone ensures that a set of secret keys are exchanged. Based on these keys, the trackers generate rotating private-public key pairs, allowing the nearby finder devices to use end-to-end encryption for all uploaded locations to Apple's servers.

The life cycle of AirTags and Find My trackers follows an internal state machine: If the trackers are in Bluetooth range of their owner's iPhone, they will keep a BLE connection. In the connected state, they are not advertising their public key, making it impossible for finder devices to report the tracker's location. Following a predefined pattern, the tracker rotates its MAC address every 15 minutes to protect the owner's privacy. Only if the trackers disconnect, they advertise their public key and become findable. In this state, the tracker changes its BLE MAC address every 24 hours, allowing it to be discovered by anti-tracking technologies but preventing any long-term identification of the device itself [1].

2.1.3 Tile. Tile trackers have been sold since 2012, and they were the first to offer offline finding technology by utilizing crowdfinding [33, 55]. Finder devices are all smartphones with the Tile app installed. This method allows Tile trackers to work across operating systems, unlike Apple AirTags or Samsung SmartTags. The Tile tracker itself follows a simple life cycle: Once the user has set up the tracker using the Tile app, the tracker starts broadcasting BLE advertisements. These advertisements contain an identifier reserved for Tile (service UUID) and proprietary data that changes every 15 minutes. In contrast to the AirTags, Tile trackers are always findable and do not differentiate whether the owner's smartphone is nearby. The BLE MAC address of the Tile tracker is static and never changes, allowing identification over several years (see Section 7.1).

2.1.4 Samsung SmartTag. Samsung SmartTags are part of Samsung's *Find My Device* offline finding network with about 200 million active finder devices (i.e., Samsung smartphones) [63]. Upon initial pairing, each Samsung SmartTag receives 1,000 privacy IDs from the owner's phone. The owner and Samsung know these privacy IDs and allow identification of the SmartTag while it employs BLE MAC address randomization.

Samsung trackers follow a similar life cycle to Apple's Find My trackers: If the tracker is connected to the owner's smartphone, it is findable, but the tracker announces its connection state in the BLE advertisement. After disconnecting, the tracker progresses through three different modes: It starts in the *prematurely lost mode*, indicating that it has lost the connection to the owner's device. After 15 minutes, it switches to the *lost mode*. After another eight hours, it changes to the *overmature lost mode* and stays in this mode until it can reconnect to the owner's device. In the connected state and *(prematurely) lost modes*, the device keeps changing its privacy ID and BLE MAC address every 15 minutes, making it hard for tracking detection software to identify the device as the same tracker following the user. In the *overmature lost mode*, the tracker keeps one privacy ID for 24 hours, allowing robust tracking detection [63].

2.1.5 Chipolo. The Chipolo tracker manufacturer offers a variety of trackers that can operate in different offline finding networks. Their Chipolo Spot and Chipolo Card trackers work across different operating systems and use their offline finding network, like Tile.

Table 1: Classification when a tracker is findable and when it is recognized as a potential stalking threat.

Tracker	Findable	Potential stalking threat
AirTag	⚷×	⚷×
Tile	∞	∞
SmartTag	∞	⚷× ≥ 15 min
Chipolo	⚷×	⚷×

⚷× = Tracker is not connected to an owner's device
∞ = At all times

This work focuses on the original Chipolo tracker using a custom offline finding network. The tracker has two states: Connected to its owner's device and disconnected from the owner's device. Only during the disconnected state the tracker advertises a custom service UUID which makes it findable. The tracker has a static BLE MAC address that also serves as the identifier used for finder devices to report the location of a lost tracker. As iOS does not allow third-party apps to read BLE MAC addresses, the tracker also advertises a service data packet that contains the device's BLE MAC address. This behavior allows for the same long-term identification that is also possible with Tile trackers (see Section 7.1)

2.1.6 Trackers used for stalking. All presented trackers have the potential to be misused for stalking. Table 1 summarizes when each tracker is becoming a potential stalking threat based on their Bluetooth advertising behavior. While a tracker is connected to its owner's device, we do not classify it as a stalking threat because it indicates that the tracker is used for benign purposes.

2.2 Threat Model

In contrast to a classical threat model, which takes a system's perspective, we focus on the security and privacy of individuals. We follow the threat modeling framework for intimate partner violence by Slupska and Tanczer [48].

The main threat is unwanted location tracking, where an adversary hides a Bluetooth tracker in their victim's belongings to monitor their location. Unwanted tracking results in a privacy invasion and a potential for physical involvement of the adversary. Additional threats exist, e.g., adversaries have been using trackers to find the parking location of valuable cars to steal them [34].

The goal is continued access to the victim's location without interference or detection by the victim. The adversary possesses technical knowledge and has can purchase, install, and operate Bluetooth trackers. We do not take into account adversaries with the technical ability to bypass tracking detection systems by modifying trackers or building a custom tracker. Multiple threat actors with various motivations exist in our model: A (prior) intimate partner can use location tracking to coerce, harass, or to gain control over their victim, or a stranger attempting to find out the home location of a celebrity or politician [42, 45].

2.3 Laws on Stalking and Location Tracking

Many countries and states have laws against stalking and location tracking. In this section, we briefly describe laws in Europe and North America, focusing on what they have in common and how they define stalking. Stalking is generally defined as a repeated or continuous act of following the victim, physically approaching the victim, unwanted communication with the victim through means of text messages, mail, or other digital communication means, or threatening the victim or their family with physical harm or death [14, 15, 47, 52, 53, 61].

The U.S. federal law covers only cases of stalking in which the stalker has crossed state borders to pursue the victim [31]. In any other case, the state where the victim or the perpetrator live are legally responsible. In response to the rise in stalking attempts, using AirTags and other trackers, several US states have proposed bills punishing unwanted tracking of a person. For example, in Texas, it is explicitly disallowed to mount a GPS tracking device on a motor vehicle without the owner's consent [20].

In Europe, we have reviewed laws concerning stalking and harassment in Austria, Belgium, France, Germany, and the UK. Only France explicitly forbids tracking someone's location and fines this behavior with a fine of up to 45.000€ and up to one year of prison [32] .

2.4 Tracking Detection App

Our tracking detection app AirGuard is available for both major mobile operating systems (OSs), Android [46] and iOS [54]. We developed the apps focusing on detecting Bluetooth trackers from Apple, Tile, Samsung, Chipolo, and other trackers compatible with the Find My network. Both apps identify tracking attempts while the app is running in the background. This section explains AirGuard and how it identifies trackers potentially used for stalking. Moreover, since both OSs follow different design paradigms regarding background execution and Bluetooth scanning, we explain how this affects the implementation and data collection of the apps.

2.4.1 Tracking detection algorithm. Whenever a tracker is detected that is in a state that denotes it as a potential stalking threat (see Table 1), the detection event is stored in a database alongside the current location of the phone.

The basic algorithm to classify a tracker as a stalking threat is based on the reverse-engineered algorithm of Apple [24]. Two conditions need to be fulfilled:

(1) Was the tracker seen at three distinct locations?
(2) Did the tracker follow the user for at least 60 minutes?

Users can define their security level, switching between low, medium, and high. The default level is set to medium, following the conditions described above. In the low security level, five locations and 120 minutes are required for a classification as a stalking threat. In the high level, only two locations and 30 minutes are necessary. The classification algorithm uses clustered locations with a radius of 150 m each. This method reduces false positives caused by a neighbor's device, which would be seen many times at almost the same location.

2.4.2 False positives. A false positive is a misclassification of a benign tracker as a stalking threat. Every false positive also results in a notification sent to the app's user, which we term a *false alarm*. A typical scenario for a false positive is in an airplane: The owner of a tracker activates flight mode and disables Bluetooth and Wi-Fi during the flight. Their tracker is then disconnected from the

owner's device for the entire flight. AirGuard will start identifying a tracker that is following the user since multiple locations are registered during the flight. As a result, AirGuard misclassifies the tracker as a stalking threat, resulting in a *false alarm*, i.e., a notification is sent to the user.

2.4.3 Android. AirGuard has been programmed to perform BLE scans for trackers nearby every 15 minutes. The OS can also delay these scan windows to once an hour for power saving constraints since Android 13. Therefore, the app can only follow irregular scan intervals, which may lead to delayed detection of trackers. The app can identify various types of trackers, including AirTags, Find My trackers, Tile trackers, Chipolo trackers, and Samsung SmartTags, even when running in the background without any user interaction. For SmartTags, the app can only warn users if these trackers are in the *overmature lost mode*, i.e., disconnected from the owner's device for more than eight hours.

2.4.4 iOS. iOS handles the background execution of apps entirely differently, leaving BLE background scans in the hands of the OS. An app can specify a list of BLE service UUIDs and let iOS scan for these devices. The OS then performs all BLE scans automatically and wakes the app (1) immediately when a new tracker is detected, (2) when a known tracker changes its Bluetooth advertisement, or (3) periodically when a tracker remains nearby. Thus, the iOS background scan is close to a continuous scan mechanism, ensuring that AirGuard for iOS immediately detects all Tile, Samsung, and Chipolo trackers. One limitation of iOS is that Apple does not support background scans for Find My devices (i.e., AirTags). To close this gap, AirGuard enables users to detect these trackers when opening the app and performing a manual scan. While iOS does not automatically limit background scans for power saving, activating the iPhone's low-power mode can influence the scanning behavior.

The iOS scan capabilities enable us to create advanced tracking detection for Samsung SmartTags. The SmartTag tries to evade identification by rotating its BLE MAC address when it is not in the *overmature lost mode*. Since the iOS app detects any new device almost instantly, we developed a matching algorithm identifying a SmartTag across BLE MAC address and privacy ID changes. The algorithm performs SmartTag tracking detection as soon as the SmartTag has entered the *lost mode*.

3 RELATED WORK

To the best of our knowledge, our work is the first to analyze the stalking problem with Bluetooth trackers with research results from an online survey and user data from a tracking detection app. This section covers related work in the analysis of Bluetooth trackers, the misuse of these, tracking detection apps, and stalking and abuse.

3.1 Bluetooth Tracker Analysis

Researchers have looked at Bluetooth trackers and related offline finding networks from many angles. This section summarizes the existing body of research.

Weller et al. performed the first security and privacy analysis of Bluetooth trackers covering a variety of manufacturers, including Tile. They focused on the security of server components and mobile applications and found severe issues with most manufacturers [62]. A follow-up study by Garg et al. defined a set of security properties to which crowd-sourced tracking systems should adhere [22]. A new design for a secure, crowd-sourced offline finding network was proposed by both authors [22, 62].

Apple's offline finding and crowd-sourced Find My network has been evaluated for security and privacy properties by Heinrich et al. [26]. The BLE protocol of Apple's Find My devices was uncovered, and a framework to build custom, AirTag-like Bluetooth trackers have been published [7, 25].

Roth et al. analyzed the hardware and software of the AirTag and found a voltage glitch that allows access to the AirTag firmware and subsequent manipulation, including cloning an AirTag, manipulating the serial number, and modifying the firmware [43].

Yu et al. did the first privacy analysis of Samsung's crowd-sourced offline finding system [63]. They revealed the BLE protocol used to enable offline finding and found several security and privacy issues. Samsung fixed some of the issues subsequently through firmware and software updates.

Pace et al. performed a forensic analysis on the Tile tracker apps for Android, iOS, and Windows. Each app revealed the private location data of the user and would allow investigators to analyze the user's movement patterns [40].

3.2 Tracking Detection

The tracker manufacturers' reaction to stalking and unwanted tracking was delayed. This lack of tracking protection resulted in the development of a range of tracking detection apps and scientific research on the topic.

3.2.1 Tracking Detection Apps. First, this section presents all tracking detection apps linked to academic research, followed by the solutions presented by tracker manufacturers. The order is based on the release date or publication date.

Our previous publication presented the first Android version of our open-source tracking detection app, AirGuard [24]. The evaluation showed little impact on the phone's battery life and reliable tracking detection within 30 minutes and for a minimum distance of 400 m moved with the tracker. The initial user-data analysis with only AirTags was conducted, concluding that the tracking detection worked. However, false positives were often caused by GPS drifts. We designed the updated algorithm in Section 2.4 to handle GPS drifts and false alarms caused by neighbor's tracker.

Another tracking detection app for Android, BLE-Doubt, has been presented by Briggs and Geeng [6]. Their app uses trajectory classification to identify trackers from Apple, Tile, and Chipolo in 10 minutes and a minimum distance of 300 m traveled. The novel detection method allows faster detection and a reduction of false positives but requires ongoing BLE scans, which quickly drain the smartphone's battery. The authors did not release this app to the public. Therefore, no user data analysis was conducted.

Müller et al. have developed HomeScout for Android, promising an improved detection speed of a malicious tracker in 1 minute and 200 m distance traveled [39]. The app starts tracking detection when the user starts moving using a novel technique of motion activation to identify any trackers following the user quickly. In comparison with prior research, this saves battery life compared to BLE-Doubt, and it enables faster tracking detection than AirGuard.

The app supports Apple AirTags, Samsung SmartTags, and Tile Trackers. Reducing the number of false positives when traveling with friends is still an active area of research [39]. No user data analysis was performed because the authors did not release the app to the general public.

Besides developments in academia, most tracker manufacturers have offered custom solutions to detect nearby trackers. Apple integrated a background tracking detection for AirTags and other Find My trackers into iOS. For Android, they offer an artificially limited application that allows users to scan for AirTags manually: as soon as they open the app, they need to wait for 10 min before a scan can be performed [2].

Tile has integrated a manual scan, allowing users of the Tile app to scan for nearby Tile trackers. The scan mechanism is also artificially limited and requires a user to walk while performing a scan [56].

Samsung provides a manual scan and background detection option for their trackers on Samsung smartphones based on the SmartThings app [44].

At the time of writing, Google has not launched its trackers, but they have integrated background detection and manual scan method to find AirTags in the Android OS [23].

3.2.2 Analyzing and Improving Tracking Detection. Several analyses of manufacturer-provided tracking detection mechanisms have yielded inadequate protection. Doyle and Kajzer have found that people are not sufficiently protected against Apple AirTags [18]. Most issues in Apple's tracking detection have been remedied [28]. In addition, Turk et al. have analyzed the anti-stalking features of Tile and Samsung, coming to a similar conclusion [59].

Mayberry et al. have demonstrated that slightly modifying a tracker can bypass most tracking detection schemes [37]. For example, a custom tracker could employ a faster BLE MAC address and key rotation scheme as AirTags, masking the detected tracker as a new tracker in every BLE scan. A follow-up study presented an updated Find My protocol, disallowing any unknown or modified trackers and protecting against the previously demonstrated attacks [36]. Despres et al. have developed a novel algorithm to link rotating BLE MAC addresses of nearby devices, helping tracking detection software to identify trackers that would otherwise be hard to detect [16]. To detect stalking attempts more reliably and to improve the privacy of users, Beck et al. have created an improved offline finding protocol [4].

At last, Apple and Google have partnered to develop a common standard for trackers, ensuring a united tracking detection strategy across mobile OSs [30]. The specification was finalized in December 2023, but it has not yet been integrated into any operating system at the time of writing.. All trackers, including GPS trackers, should announce their presence using BLE advertisements. Smartphones use these advertisements nearby to detect if a tracker is following the user. Users can then act against any identified trackers and look up the serial number using their smartphone.

3.3 Stalking and Abuse

The misuse of Bluetooth trackers quickly became a relevant topic to the research community. These devices added to the already existing variety of Internet of Things (IoT) devices used for surveillance and abuse [10, 50].

Stephenson et al. interviewed victims of intimate partner abuse based on IoT devices [49]. 70% of all victim-survivors reported attempts on location tracking using GPS trackers, AirTags, or Bluetooth earbuds like AirPods. Multiple respondents explicitly mentioned the misuse of an AirTag to monitor their location. Interestingly, some refrained from disabling the AirTag and placed the AirTag in a known location to let the perpetrator believe the tracker is still on the victim.

A study by Mavoa et al. found that many parents (in Australia) use family activity tracking and location tracking apps to monitor their children [35]. The usage is justified with safety improvements for their children, and 95% stated that their children know about it. Nevertheless, the authors demand privacy as a right for children to develop themselves without constant supervision.

The lifetime prevalence of stalking in two European cities has been researched by Dressing et al. [19] and Stieger et al. [51]. They performed two independent surveys demonstrating who the victims were, how their stalkers acted, and in which relation the stalker and victim were. In a large-scale data study, Diette et al. revealed that the experience of stalking leaves a "psychological footprint" on female victims in the age of 18-45 [17].

4 METHODOLOGY

To understand the prevalence of stalking and location tracking with Bluetooth trackers, we ran two studies: A user data analysis of the stalking protection app AirGuard and an online survey. In this section, we describe the design of our studies and their evaluation.

4.1 Ethics

The ethics commission, representing our institutional review board (IRB), reviewed and accepted both studies. In the case of our user data analysis, participants were informed which data would be collected and how it would be processed. Only after giving consent is data collected. We did not hinder participants who denied participation from using our Bluetooth tracker detection app. Furthermore, we collected no personally identifiable information (PII) during our data collection. We store all research data on servers locally hosted at our institute, minimizing third-party access to sensitive research data. The online survey also started with a consent form, which the IRB reviewed. Only participants giving consent filled out the questionnaire. We designed the questions to collect minimal PII to protect the privacy of the participants. The entire survey was hosted at our institute, ensuring that no third party gained access to sensitive user data.

4.2 User Data Analysis

The goal of the user data analysis was to (1) identify the prevalence of Bluetooth-based personal item trackers in use, (2) determine how many users are warned of a potential stalking attempt, and (3) discover how the currently available trackers behave. These insights allow us to develop improved stalking protection and a better user experience.

All participants of this study were required to have our application installed. During the application's setup, the app asks each

person to choose if they want to participate in our user data analysis and voluntarily share data with us. Participating app users can always decide to stop their participation in the data collection or request to delete their collected data through the app. It is also possible to join the data analysis later from the app's settings. The minimum age for participants is 18 years. Our Android application has 130,000 active installations, and the iOS application has 152,000 downloads and about 80,000 active installations as of November 23, 2023. Our apps grew organically and were boosted by online blogs/magazines and mentions on social media. However, on iOS about 98,400 downloads are *institutional purchases*, i.e., companies or agencies installing the app on employees' iPhones. From this user base, 47,715 users participated in the data collection. For this work, we focus on the analysis of data collected in 14 days between November 13 and November 26, 2023, i.e., the user data of 14,739 AirGuard users from Android and iOS.

For each participant, the following data was uploaded to our collection server:

- A record for each participant in the data analysis.
- A record of each tracking device the participant's app had detected.
- The timestamp and RSSI for every advertisement the participant's app had received.
- A record of each tracking notification AirGuard had sent to the user and which device had triggered it.
- The participant's user input about the hideout where a tracker was placed.

Our data collection followed a privacy-first design since all the collected user data is susceptible. Therefore, we removed all PII from the uploaded data, including location information where the app has detected a tracker, BLE MAC addresses, and data of BLE advertisements. As a result, the dataset is fully anonymous and cannot be used to identify individual AirGuard users. Each device contains a random identifier generated by the app, which allows subsequent uploads to be matched. Therefore, if the same tracker is detected by two participants, two records will be created in our database. Figure 11 in the Appendix contains the database schema.

4.2.1 Analysis Plan. We created an analysis plan to reduce the number of Type I errors in our analysis.

We inferred the prevalence of each tracker type, i.e., Tile, AirTag, and Samsung, by the number of times our app detected it. We analyzed both sets separately since iOS and Android use different background detection mechanisms. In addition, we identified how trackers behave and bring this into context with our user data. We deeply analyzed the number of tracking detection notifications sent by the app, focusing on how many users are notified and which devices trigger notifications the most. We also evaluated the number of false positives, i.e., trackers that were classified as a stalking threat but are, in fact, not used for malicious purposes. Users can mark trackers as false positives by marking the notification as a false alarm in the app.

4.3 Online Survey

The online survey aimed to (1) identify the prevalence of stalking and location-tracking attacks utilizing Bluetooth trackers and (2) understand what protection measures people are looking for.

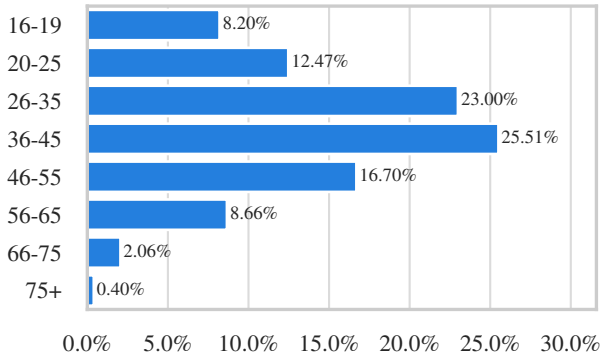

Figure 2: Age distribution of all survey participants.

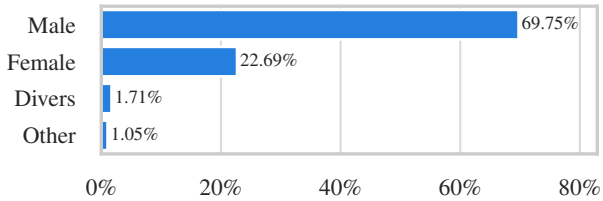

Figure 3: Gender distribution of all survey participants.

The survey mostly contained 22 single-choice questions and eight multiple-choice questions. Nine of these questions featured an option to add an alternative answer. Additionally, the questionnaire contained two open-ended questions.

In this study, we also wanted to include minors who might be threatened through location tracking attacks, e.g., by their guardians. The IRB allowed the inclusion of minors from the age of 16. We shared the link to our online survey on social media (Twitter/X), SurveyCircle, and directly in AirGuard. Most participants were recruited from AirGuard users (Android, N=4,790; iOS, N=408). Of the 20,692 people who started our survey, 5,263 finished it, and 5,253 were selected for the final dataset. We did not compensate participants.

Figures 2 and 3 show the age and gender distribution of the respondents. Most respondents reside in North America (38.76%) and Western Europe (38.47%). Our study sample is not representative. We mainly recruited respondents using AirGuard, resulting in a biased group that is familiar to the threat of stalking attempts with Bluetooth trackers. Also, previous studies about stalking reported 11.6% of respondents had experienced stalking [19], while our group consists of 19.13% of people with stalking experience.

The survey consists of five parts:

(1) Misuse of Bluetooth trackers: general knowledge, potential malicious actors, government regulation.
(2) Stalking: stalking prevalence, a question set adapted from [19, 51], targeting prior stalking victims (N=1,005).
(3) Stalking Protection: Preferences for anti-stalking and anti-tracking solutions.
(4) AirGuard App: successful tracker detection, false positives, general user experience.
(5) Demographics: gender, age groups, and world regions where they reside.

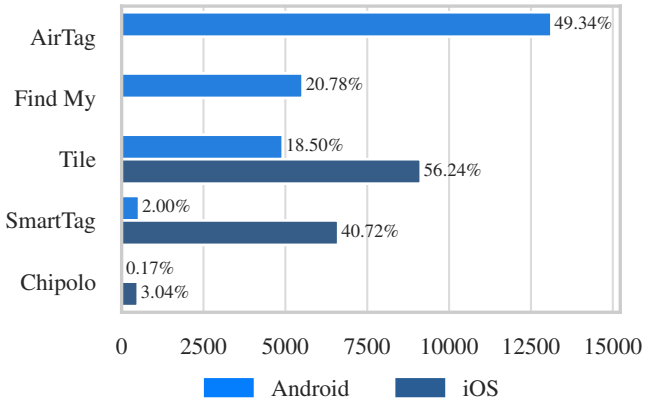

Figure 4: Number of Bluetooth trackers detected during background scans, separated by tracker type and mobile OS.

As in our first study, we aimed for a high privacy standard for all participants. Therefore, we only collected minimal PII. All survey questions were optional, and participants could skip questions that made them feel uncomfortable. We list the entire questionnaire in the Appendix.

4.3.1 Analysis Plan. We followed our previously created analysis plan to limit any false positives (Type I errors) during our analysis. For single-choice and multiple-choice questions, we consider proportions from all responses. Then, we analyze the responses based on affiliation to a specific group, e.g., gender, age, or stalking victim. If the group affiliation influences the responses given, we present these. For answers following a Likert scale, we transformed the answers to numerical scales and then reported the average values of all replies and the distribution of replies.

Nine questions featured an option to indicate an alternative answer, and two questions were open-ended and required a text answer. We selected and coded five of these questions to answer our research questions. Two independent researchers performed the coding by creating individual codebooks for each question. Then, they agreed on a master codebook and coded all questions individually. Finally, they reviewed both resulting codebooks and solved any differences through discussions.

5 USER DATA ANALYSIS

A total of 14,739 app users (iOS, N= 5,490; Android, N=9,249) shared data with us for this analysis during our data collection from November 13, 2023, to November 26, 2023. These users discovered 1.9 million Bluetooth trackers, which sent out 3.9 million Bluetooth advertisements. In this section, we analyze the resulting dataset to identify the dissemination of trackers and evaluate how often trackers led to a warning.

5.1 Tracker Prevalence

Figure 4 visualizes the distribution of Bluetooth trackers detectable during background scans in the AirGuard user dataset. As Apple limits the iOS app in background scanning for their own trackers, AirTags and Find My trackers found by the iOS version are omitted. They can only be detected when the user opens the app to scan for an unknown device. This required user interaction complicates the comparison with the number of trackers found during background scans. In the following sections, we will analyze the distribution of each tracker type and comment on the specifics of each tracker to bring the numbers into perspective.

5.1.1 Apple AirTag & Find My Tracker. Advertisements from Apple AirTags and other Find My trackers rank first and second in the tracker distribution among Android users, accounting for 70.08% of all detected trackers. The numbers reported here only include AirTags and Find My trackers that are **not connected** to their owner device. Indicating that this device is either lost, the owner is out of reach, the connection failed for other reasons, or it is used for malicious purposes. Although Find My trackers were released just over two years ago, they massively influenced the market [27, 29]. AirTags are now seen more than twice as often as Tile trackers, representing 49.34% of all trackers. Since Apple does not disclose sales figures, it is not possible to make a direct comparison of their market share. However, we can estimate that the total number of AirTags in use is even higher if we consider that only disconnected trackers are detectable by the app.

5.1.2 Tile Tracker. With over 40 million trackers sold worldwide [40], Tile trackers are the most common trackers discovered by AirGuard for iOS, accounting for 55.01% of all devices. Among Android users, Tile trackers rank in third place with 18.42%. Comparing the total number of Tile tracker detections, it is remarkable that Tile trackers are more often detected by iOS users even though there are less iOS users than Android users. This observation is explainable as Android limits AirGuard's background scans to four scans an hour while the nearly continuous scanning of iOS ensures that AirGuard detects all Tile trackers near them.

5.1.3 Samsung SmartTag. Looking at the Samsung SmartTags, Android users report only 8.48% of the number of SmartTags found with iOS users. For SmartTags, both apps follow a different approach: The iOS app discovers SmartTags in every state, while the Android app explicitly filters for SmartTags in the *overmature lost mode* (see Section 2.4). The reported amount by iOS users is, therefore, better for estimating the distribution of SmartTags. Hence, the numbers from Android users show us how many trackers are disconnected from the owner's smartphone for at least 8 hours. These trackers are most likely attached to a lost item that has not been retrieved or are used for (unwanted) location tracking. Comparing these numbers with AirTags in a disconnected state is not straightforward, while an AirTag moves directly from the connected state to a findable state, a SmartTag needs at least 8 hours.

5.1.4 Chipolo Tracker. In this section, we focus on the original Chipolo trackers since their Find My compatible version is already covered by Section 5.1.1. The user data analysis shows that the Chipolo trackers only cover between 0.17% (Android) and 2.94% (iOS) of the available trackers. This, in return, also means that the offline finding network is likely minimal and may not yield regular location updates for the owner. Hence, a Chipolo may be used for unwanted location tracking, but the small offline finding network will likely result in close to zero location updates. However, compared to Apple's Find My network, previous work found that

Table 2: Notifications sent out during the two weeks of the user data analysis.

Device	All	User-tagged false alarms
Tile	14,331	77
AirTag	2230	55
Find My	1442	25
SmartTag	520	18
AirPods	396	13
Chipolo	241	6
Total	19584	194
Users involved	1986	105

the network results in sufficient updates to reconstruct the path a person has travelled [26].

5.2 Notifications

As described in Section 2.4, AirGuard is designed to send users an alarm (i.e., a notification) when a tracker follows them. This section discusses the alarms sent out by the two apps, delving into the number of users warned and potential false positives, i.e., users receiving a notification for a benign tracker.

5.2.1 Daily Notification Load. Table 2 shows the number of unwanted tracking notifications sent out by our apps during the two weeks of the user data analysis. AirGuard sent 19,584 warning notifications to users about devices potentially following them. Tile trackers caused most notifications (73.18%), even though AirTags and Find My trackers are more widespread. The number of notifications (over 14,000) and the prevalence of Tile trackers compared to other trackers is excessive. One Tile tracker causes, on average, 4.7 notifications, pointing towards the observation that users who own a Tile tracker or interact regularly with Tile owners get used to the false alarms and ignore them. If these trackers were used for stalking, we would expect a tracker to be found and removed after receiving several notifications.

There are two possible explanations for such false alarms:

(1) Tile trackers do not indicate if the owner of the tracker is nearby. Therefore, our apps cannot differentiate between malicious and genuine Tile trackers close to the user.
(2) Since Tile trackers do not change their BLE MAC address, encountering the same Tile tracker multiple times can lead to tracking notifications even weeks later. For example, when a user meets a colleague who owns a Tile tracker while grocery shopping, the app recognizes a tracker that has followed the user from the office to the shop.

Both reasons can independently lead to false alarms. Future work will require an adapted tracking detection algorithm for trackers with static BLE MAC addresses, i.e., Tile and Chipolo, that balances false positives with accurate unwanted tracking notifications.

Figure 5 compares the time until a notification is sent for all tracker types. Tile trackers have a median notification delay of 4,413 minutes, which is more than three days. In contrast, all other trackers have a median below 1,000 minutes, with Samsung SmartTags having the lowest at 70 minutes. Tile trackers do not use BLE MAC address randomization, which can cause the app to send a notification weeks after the initial detection of the tracker. If a tracker is not identified as a potential tracker for weeks, it is probable that the tracker is not being used to follow the user but rather is owned and used by someone the user knows. This observation supports the explanations for false alarms mentioned above. Similarly, Chipolo trackers also do not implement BLE MAC address randomization. However, since they are not as widespread, we do not detect as many of these potential false positives and highly delayed alarms.

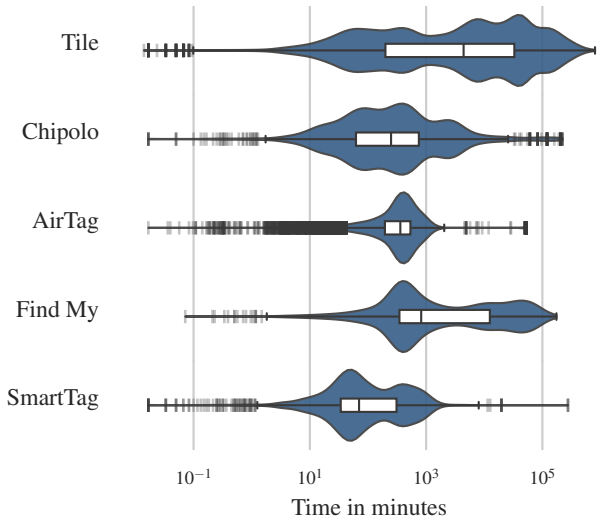

Figure 5: Comparison of the time to notification for all tracker types. Shown is the time it takes to send a notification from the first discovery of a tracker.

5.3 Interaction and Feedback

We observe if the user has tapped on a notification to inspect if a potential stalking attempt caused it. In the two-week data collection period, AirGuard sent out 19,584 notifications, out of which users tapped on 799. Table 2 shows 196 notifications were marked as false alarms by app users. Further, 770 notifications belong to trackers that were later marked as *ignored*. Users can ignore trackers from which they do not want to receive further notifications. We equally categorize them as false alarms. Only 1.02% of trackers in total (3.46% of SmartTag, 2.49% of Chipolo, 2.46% of AirTag, 1.73% of Find My, and 0.53% of Tile) are marked as false alarms. We expect that more false alarms are caused, but users disregard the notifications. Especially when comparing the high number of notifications for Tile trackers, and the small percentage marked as false alarms.

In addition, users can give feedback on where they found a tracker (only in the Android version) and select from these categories: Backpack, Bike, Car, or Clothes. During the two-week user data analysis, ten trackers were found in a car and two in a backpack. Five of these trackers were Tile trackers and seven were AirTags. Figure 6 shows the tracker locations selected for one year from December 2022 to November 2023, removing every notification that has been marked as a false alarm. The figure shows that most trackers are hidden in cars or attached to cars.

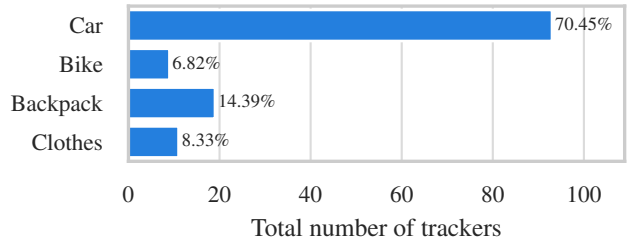

Figure 6: Hideouts of trackers that triggered AirGuard notifications.

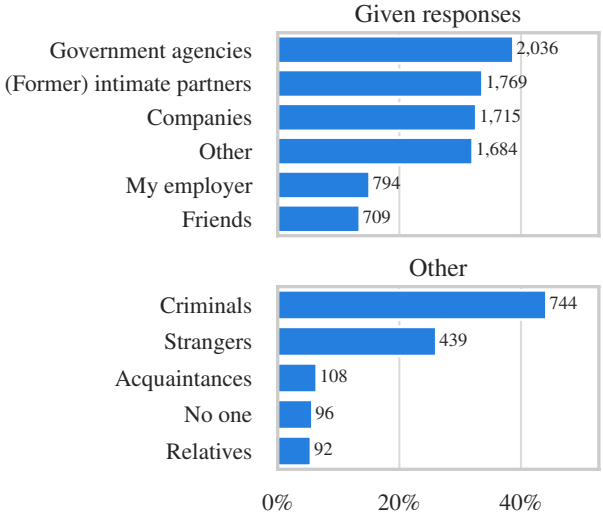

Figure 7: Actors that our survey participants expected to act as stalkers.

6 SURVEY RESULTS

In this section, we present the results of our online survey, turning to each survey part individually: Misuse of Bluetooth trackers (Section 6.1), stalking experience (Section 6.2), stalking protection (Section 6.3), and AirGuard user experience (Section 6.4). For each part, we focus on the questions that align the most with our research questions. 20,692 participants commenced the online survey. Out of the 5,263 completed surveys, we had to remove 10, resulting in a study sample of **N=5,553**. These participants joined the online survey from AirGuard for Android (4,781), AirGuard for iOS (411) or other sources, e.g., social media (61).

6.1 Misuse of Bluetooth Trackers

6.1.1 Potential Stalkers. We asked our participants which potential actors they expected as stalkers in a multiple-choice question with an option to provide alternative answers. Figure 7 shows the most commonly named actors. Government agencies rank first, followed by (former) intimate partners, companies, and other actors. Other frequently named actors are employers, criminals, and friends. Potential stalkers can be classified into two categories: Actors close to the victim and distant obscure groups. On the one hand, participants expect stalkers close to them (3,364), including their partners, friends, and family, as well as people from their work environment.

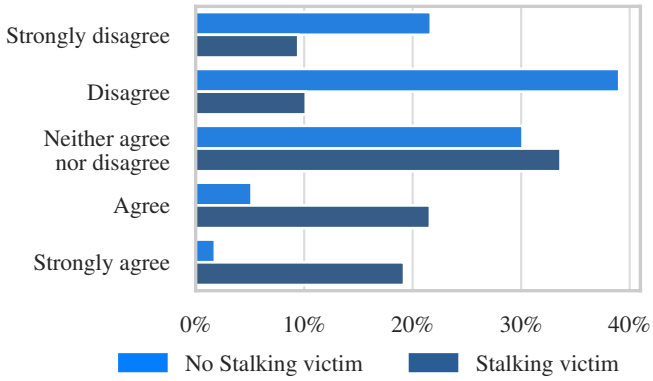

Figure 8: Comparison of the participants' expectations to be tracked depending on their stalking background. Depicted is the agreement with the statement "During the next 12 months, somebody will try to track me using a key finder". The bar colors indicate whether participants identify as stalking victims (dark blue) or not (light blue).

These are familiar faces the victim meets regularly. On the other hand, our participants name distant, hard-to-grasp organizations (4,525), including government agencies, companies, and criminal organizations. The common denominator of these groups is distance and uncertainty, as there is no representative to associate with these organizations, so any stranger on the street could be a member. Additionally, the motives of these groups are uncertain, suggesting that everyone can be a potential victim.

6.1.2 Future Stalking Attempts. We asked the participants if they expected to be tracked in the next 12 months. Figure 8 compares the participants' agreement depending on their background as stalking victims. Participants reporting stalking experience were more likely to agree with the statement (mean value 3.33) than participants without stalking experience (mean value 2.25). As stalking has already been an issue in the participants' lives, they likely want to add protection mechanisms since stalking with Bluetooth trackers is a potential risk in their lives.

6.1.3 Regulation and Responsibility. When asked if easy accessibility to Bluetooth trackers favored stalking, 4,156 participants (79.11%) agreed. More than half of the participants (54.21%) agree that governments should intervene and explicitly disallow and punish unwanted location tracking. Many governments worldwide have been moving forward in that direction since the release of AirTags in 2021 [45, 58, 60]. We asked participants if the intended function of these devices (finding lost items) is more important to them than the potential misuse of trackers. People were on both sides of this question, showing an almost equal 50% distribution.

6.2 Stalking Experience

We tailored this part of the online survey towards prior stalking victims to uncover the stalking prevalence and its effect on people, adapting questions from previous surveys on stalking [19, 51]. This

Table 3: Contingency table of the stalker's gender depending on the victim's gender.

		Stalker			
		Male	**Female**	**Diverse**	**Other**
Victim	**Male**	141	172	56	4
	Female	399	48	24	2
	Diverse	9	7	6	0
	Other	13	4	1	0
	Total	58.40%	23.68%	8.85%	0.59%

set of general stalking-related questions allows us to compare our results with previous works and to understand how stalking victims specifically feel about the threat of Bluetooth trackers. The answers presented in this section are not directly related to Bluetooth trackers besides that most respondents are users of the AirGuard app and thus aware of the misuse. We included a filter so that only participants with stalking experience replied to this part of the survey. In our study sample, 1,005 participants (19.13%) report having been a victim of stalking. Out of these, 41% identify as male, 49% identify as female, 4% as other or divers, and 6% do not disclose their gender. Further responses are in the Appendix.

6.2.1 Victim-Stalker Gender Dependency. Our participants identify the gender of stalkers as follows: Most stalkers were male (58.40%), 23.68% of stalkers were female, and 8.85% were diverse. Compared to previous research [19], we report fewer male stalkers (-30 p.p.) and a higher share of female stalkers (+11 p.p.). Considering the participants' gender, our data suggests that female victims are pursued primarily by male stalkers (81%), while male victims are pursued by male and female stalkers alike (41% and 48%, respectively).

6.2.2 Victim-Stalker Relationship. We asked stalking victims about their current relationship with the perpetrator. The highest percentage of perpetrators (26.07%) were identified as prior intimate partners. Previous studies have shown an even higher proportion of 32% for this group. 23.18% reported that their stalker is unknown to them, supporting the findings of previous studies (21% - 24%) [19]. These findings can be combined with the actors expected to be stalkers (Section 6.1): Victims of stalking more often expect stalkers close to them, while people without stalking experience more often expect stalkers from unknown, distant organizations. A summary of all results is presented in the Appendix in Table 6.

6.2.3 Stalking Motives. The motivations of a stalker can be manifold. Our respondents claimed that jealousy, envy, distrust, and revenge were the most common reasons for their perpetrators to act. These numbers align with previous research [19] and show that stalking is often performed by a (former) intimate partner who either has trust issues, wants to revive a past relationship, or strives for revenge after the breakup. All responses are summarized in the Appendix in Table 7.

6.2.4 Stalking Patterns. Most of the stalking victims report being stalked for more than one year (49%), either irregularly (36%) or daily (25%). Such long-term stalking can cause severe psychological issues for victims [17] and require vast investments to stop the perpetrator.

Most victims stated that four or more different methods of stalking have been used against them, indicating that stalkers, on average, use 6.6 different methods to pursue their victims. The most frequently mentioned stalking methods are physically following the victim (66.17%) and unwanted digital communication (61.49%). Location tracking (44.28%) is also a commonly used tactic of stalkers. We see that a stalker, in most cases, uses at least one method, which is illegal in many countries (see Section 2.3). Table 8 in the Appendix gives the full list of all responses.

Our digital society offers a variety of methods to track the location of a stalking victim. Besides Bluetooth trackers, perpetrators may install stalkerware apps [41] on the victim's phone or configure existing apps, e.g., Google Maps, to permanently access the victim's location. Such stalking apps require access to the victim's phone, which is predominantly given when the stalker and victim are in an intimate relationship or otherwise close.

6.2.5 Impact on Victim's Life. The impact of stalking cannot be dismissed. What is striking is that most participants with stalking experience had to take additional security measures (66.37%), a much higher number than previous research found (17%). 63% of stalking victims in our study had to change their current lifestyle as a direct result of stalking, supporting the findings of previous studies (73%). Many victims had to change their phone numbers or email addresses to avoid unwanted communication (46%). Others had to change their residence, change their workplace, or seek help from a lawyer. On average, victims reported 2.7 factors in which their life was impacted or where they had to change.Table 9 in the Appendix lists all answers to this question.

6.3 Stalking Protection

We asked the participants which measures they expected to be applicable against stalking and unwanted location tracking with Bluetooth trackers.

6.3.1 Anti-Stalking Apps. 68% agreed that an app-based solution that detects trackers from all manufacturers will improve the current situation. At the time of the survey, AirGuard for Android could only detect Find My (e.g., AirTags) and Tile trackers, explaining the frequent requests for further tracker types. As explained in Section 2.4, AirGuard for Android and iOS now detects trackers of Apple, Samsung, Tile and Chipolo.

6.3.2 Smartphone-Based Stalking Protection. Two-thirds (66%) of participants demand tracking detection integrated into their smartphone's OS. An integration would solve an integral problem of anti-stalking apps, i.e., victims need to know about Bluetooth trackers and manually install the anti-stalking app before they are protected.

6.3.3 Privacy-by-Design for Trackers. 53% of participants agree that trackers should gain attention by making sound or emitting light. These features are also part of the new standard developed by Apple and Google [30]. Other participants propose bright coloring of tracking devices, larger trackers that cannot be hidden easily, and tamper-proof trackers for which the speaker could not be disabled without destroying the tracker. Furthermore, 46% believe

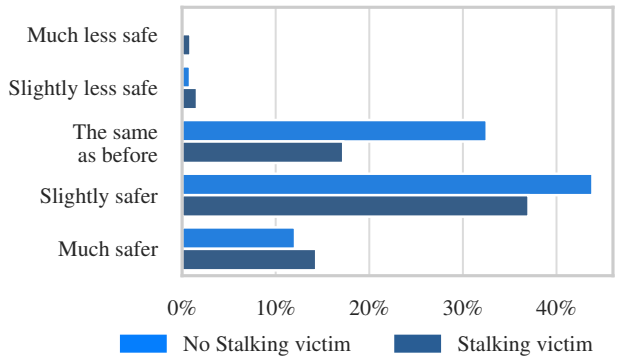

Figure 9: Change of the user's perceived safety level after installing AirGuard.

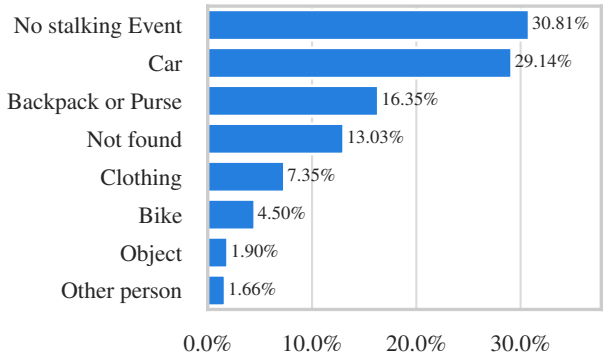

Figure 10: Hideouts at which participants found a Bluetooth tracker with AirGuard.

manufacturers should be responsible for preventing stalking with their trackers. We are unaware of any solutions from a manufacturer that would prevent misuse of their Bluetooth tracker. All solutions require the victim to act, like AirTags emitting sound or the tracking detection implemented in iOS and Android. There is no solution impeding the stalker as long as the victim does not actively act against it.

Multiple participants suggest an identification procedure that links the tracker's serial number to the owner's identity. Tile provides a similar system in their anti-theft mode: Owners of a tracker have to provide a copy of their national ID card and then sign a document agreeing to pay a fee of one million US dollars if they use their tracker to involuntarily track a person. If agreed, all trackers from the owner are hidden from Tile's tracking detection feature [57]. This approach allows Tile to combine theft protection with anti-stalking mechanisms.

Finally, 30 participants suggested that more public information and technology education would help people to know about the misuse and how to act if an unknown tracker is found.

6.4 App Behavior and Interaction

We asked all participants familiar with AirGuard app-specific questions to evaluate if AirGuard provides sufficient protection for the users. To this end, we filtered for participants who are current or prior AirGuard users. Only those filled in the questions addressed in this section.

6.4.1 Perceived Safety. When asked if they felt less safe or safer since discovering AirGuard, users indicated they felt safer overall. Figure 9 depicts the level of perceived safety. Only 1.5% of participants feel less safe than before.

6.4.2 False Alarms. We asked users if AirGuard had found more trackers than expected, but most participants denied it: About 55% of users reported that they have never received a false alarm, 15% stated that crowded places, e.g., concerts or public events, increased false positives and 12% indicated false alarms in public transport. Additionally, in an open-answer question 19.69% of all respondents and 27.72% of prior stalking victims stated that false alarms would cause anxiety or let them feel unsafe. 65.02% responded that they would not be affected by false alarms. It is relevant to say that 14.41% stated that a notification would show them the app works and they would risk more false alarms than missing an actual tracker.

6.4.3 Stalking Attempts. In the survey, 8% of app users indicated they received a notification from a tracker following them. These 422 people were asked to specify where the tracker had been hidden. 30.81% of all responses described an event that did not include any stalking attempts, e.g., a fellow passenger in public transport (10%), another person owning a tracker (18%), or their own Tile trackers. Figure 10 shows all responses, identifying the car as the most prominent place to hide a tracker. Additionally, these locations were indicated in the *other* responses: Eight trackers were hidden inside or attached to objects, like suitcases, briefcases, and purses. Seven trackers were found on another person, potentially indicating a tracker that was used to track a friend's location. One tracker was found on an e-scooter.

Unfortunately, we can see that many misunderstood the question about the tracking device used for stalking — many stated a non-stalking related event. Therefore, we cannot be sure that the remaining replies refer to an occasion of unwanted tracking.

7 DISCUSSION

7.1 Privacy Implications for Tracker Owners

Focusing on the intended use of trackers, they are primarily used to track personal items. Apart from the malicious use of trackers to stalk other people, Bluetooth trackers also pose a privacy risk to their genuine users. As some trackers never change their BLE MAC address, they can be detected and linked over an extended period, allowing the long-term tracking of a tracker and, therefore, its owner. This potentially causes grave privacy implications for users: For example, even years later, authorities could identify protesters based on the Bluetooth trackers they carried.

We analyze the user data to determine the maximum duration for which a tracker has been identified as the same device. Even though our data set is limited to two weeks, each database entry contains the date when the user first discovered a tracker.

Table 4 compares the maximum observed tracker re-identification periods of different trackers, i.e., the maximum duration for how long AirGuard has re-identified a specific tracker of that brand.

Table 4: Observed maximum tracker re-identification periods.

Tracker	Re-identification period
Tile	602 days
SmartTag	226 days
Chipolo	221 days
Find My	220 days
AirTag	172 days
AirPods	141 days

For example, the app re-identified one Tile tracker 602 days after the first detection. This tracker was first discovered one day after the app update, adding support for Tile trackers. **An observation caused by the static, non-randomized BLE MAC addresses of Tile trackers**. Chipolo trackers suffer from the same issue: The tracker in Table 4 was first detected when support for these trackers was added and has been re-identified since then.

Even though AirTags and other Find My trackers use rotating BLE MAC addresses, AirGuard was able to re-identify them over an extended period. The AirTag's low-battery mode causes this long-term identification. A note in the Find My App states: "When AirTag battery is low, privacy protections are temporarily adjusted and AirTag may be trackable over Bluetooth." [3] These adjustments stop the rotation of the BLE MAC address and the private key of the AirTag, keeping the offline finding features available at the cost of long-term identification and potential tracking. For AirTags, we observed that they can continue to operate in low-battery mode for almost a year. **AirTags, Apple AirPods, and Find My trackers in low-battery mode allow long-term identification a person.**

Fortunately, a simple battery replacement restores the rotation of BLE MAC addresses, mitigating this privacy issue. Normal behavior disallows long-term identification since the BLE MAC address changes every 15 minutes in the connected state. A daily BLE MAC address change prohibits long-term identification, even in the disconnected state.

According to the AirGuard user dataset, some Samsung SmartTags could also be re-identified for over seven months. Long-term identification is likely caused by repeating privacy IDs. As a SmartTag contains only 1,000 privacy IDs, they repeat every 10.42 days [63]. Therefore, one can re-identify a SmartTag based on one equal privacy ID. However, there could also be an existing bug or an unknown low battery mode that stops the SmartTag from rotating its privacy ID at least every 15 minutes to 24 hours. We can only confirm that long-term identification of a SmartTag is possible.

7.2 Limitations and Future Work

While our online survey provides essential insights into the misuse of Bluetooth trackers for stalking, it is crucial to fully acknowledge its limitations to understand the context and scope of the findings.

Firstly, the participants in the online survey and the user data analysis only partially represent a broader population. Participants had to install and use AirGuard for the user data analysis. Online survey participants were recruited mainly through AirGuard. We acknowledge that both studies contain a biased group that has prior knowledge about the potential misuse of Bluetooth trackers and a higher percentage of people with stalking experiences, 19.18% compared to 11.6% in [19]. To address this issue, an independent study with user data from the iOS and Android tracking detection should be performed. Such a study would provide valuable insights for most of the global population but would also require the cooperation of these companies.

Another limitation lies in the multiple-choice questions of the online survey: We did not rotate answers, potentially causing an influence of order.

We intentionally chose a privacy-first approach with all user data collected, limiting the scope of our analysis. For example, we opted against uploading location information of where trackers had been discovered. While this would have allowed us to classify false alarms better, it would have violated the participants' privacy. Our limitation on four tracker manufacturers, Apple, Chipolo, Tile, and Samsung, also limits the scope. However, since these brands are the most commonly used, we cover the majority of the market.

In future work, it will be relevant to expand the current research into different areas: Tracking detection algorithms for static BLE MAC addresses could be adapted to balance false alarms while maintaining the detection of trackers used for stalking. This is especially relevant since a false alarm can cause anxiety as 19.69% of respondents stated. Finally, manufacturers should enhance their research into privacy-by-design trackers to limit the opportunities for stalkers to use Bluetooth trackers.

7.3 Answers to our Research Questions

In the introduction of this paper, we formulated three research questions, which we aimed to answer with two studies: The AirGuard user data analysis and the online survey. In this section, we combine the results of both studies to answer our research questions.

7.3.1 RQ1: How severe is the problem of tracker misuse for location stalking? It is not possible to provide a comprehensive quantification of the misuse of Bluetooth trackers for location stalking due to the biased population represented in the survey. This bias affects the findings, as we are likely to observe a higher percentage of people affected by location stalking than in the general population. However, the group consists of individuals with valid experiences and needs, which led to valuable insights in user data analysis and the online survey:

- **Prevalence:** Trackers were prevalent, with the average user discovering 2.9 trackers daily.
- **Stalking experience:** 19.18% of our survey participants report being a stalking victim, and 8.49% of all respondents have been affected by a form of location tracking. 222 (4.22%) participants of the online survey mentioned that a tracker had been used to stalk them.[2]
- **Warnings:** AirGuard warns about 400 people daily from our dataset of a potential tracking attempt. We cannot precisely state the rate of false positives, but we have understood from the online survey that users prefer false positives over missing an actual tracker.

[2]We removed participants that stated a false alarm

- **Tracker hideouts:** We have received specific feedback on where participants found hidden trackers. Participants of the online survey and feedback in AirGuard show that trackers were mainly hidden in their cars or a backpack or purse.

While the participants of our studies are not representative of a specific population, we report insights from 14,739 AirGuard users and 5,253 survey participants, hinting towards a widespread stalking problem concerning people worldwide.

7.3.2 RQ2: Which measures are considered effective stalking protection? Our results show that there is no one-size-fits-all solution against stalking:

- **Anti-stalking apps:** Our survey participants favored apps integrating tracking detection for all tracker devices. The AirGuard user data analysis found that AirGuard provides working tracking detection mechanisms across all participating users. However, anti-stalking apps require the victim to know about trackers and proactively install the app.
- **OS-integrated stalking protection:** Previous research showed that many users do not take appropriate measures by themselves [59]. Tracking detection integrated into the smartphone's OS is a favorable solution for most users. We are pleased that Apple and Google are working on a common standard [30]. However, updating AirTags, Tile, SmartTags, and third-party Find My trackers to comply with the standard could take years. We would appreciate a solution that is not limited to the detection of standard-conforming trackers.
- **Privacy-by-design:** We advocate for a solution that limits the tracking capabilities of stalkers with Bluetooth trackers and thus makes stalking harder. One approach proposed by related work [59] is to reduce trackers' accuracy after it has not been near its owner for some time. Another idea is stalking detection on the manufacturer's side, e.g., disallowing the use of trackers for unwanted tracking.

We anticipate more concrete future work in this direction.

7.3.3 RQ3: What are the privacy implications for genuine tracker owners? In Section 7.1, we have shown that no tracker device sufficiently protects the privacy of genuine tracker owners.

- **Static BLE MAC address:** The most concerning trackers use a static BLE MAC address for the entire lifetime of the tracker. This allows long-term tracking and re-identification for months and years. Researchers have demanded to improve MAC address randomization for years [4, 11, 12, 62].
- **Trackers in low power mode:** Even trackers with BLE MAC address randomization, i.e., AirTags, Find My trackers, and SmartTags, have been identifiable by AirGuard for over five to seven months due to non-rotating BLE MAC addresses in low power mode. Trackers should perform BLE MAC address randomization at least once daily.
- **Buggy Implementations:** Bugs may cause the issue of long-term tracking in some trackers. Tracker owners should know this issue, regularly change their tracker's battery, and update the firmware.

AirGuard could re-identify trackers of all manufacturers, allowing long-term identification and long-term tracking of the owner. We can, therefore, conclude that **owning a Bluetooth tracker is a privacy risk even for genuine users**.

8 CONCLUSION

In this work, we performed two studies shedding light on the widespread stalking problem with Bluetooth trackers. In a user data analysis study of AirGuard, a tracking detection app with over 200,000 installations on iOS and Android, we found details about the prevalence of trackers from different manufacturers. In detail, we saw that the AirTag and other Find My trackers have surpassed the number of Tile trackers deployed. Still, Tile trackers caused most tracking alarms. We identified many of these as likely false alarms, exaggerated by the missing BLE MAC address randomization of Tile trackers. In addition, we found that trackers from all manufacturers suffered from privacy issues. AirGuard users have identified the same trackers over several months.

In our second study, we performed a large-scale online survey (N=5,253) to identify measures to improve tracking detection and to quantify the stalking problem with Bluetooth trackers further. The results revealed that 19.18% of participants have experienced stalking and that location tracking has been a typical method that stalkers applied (44.28%). Most participants also agreed that the easy accessibility of trackers increased stalking issues (79.11%). At last, we found that AirGuard successfully identified malicious trackers for 222 respondents.

Overall, our results suggest that unwanted tracking performed with Bluetooth trackers is a widespread problem that needs to be addressed thoroughly. The recently started standardization for unified Bluetooth tracking detection by Apple and Google is a step in the right direction. We also advocate for manufacturers to think about victims without a smartphone, requiring a solution that hinders stalkers from misusing trackers in the first place.

ACKNOWLEDGMENTS

We thank the anonymous reviewers and our shepherd, for their constructive feedback. We thank the participants of our two studies. We also thank Dennis Arndt and Leon Böttger for their support in developing the AirGuard apps for iOS and Android. We express our gratitude to Momo Matern for her feedback on our online survey design and our analysis plan. This work has been co-funded by the German Federal Ministry of Education and Research and the Hessian State Ministry for Higher Education, Research, and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE and by the German Federal Ministry of Education and Research in the Open6GHub project.

REFERENCES

[1] Apple Inc. 2020. Find My Network Accessory Specification - Release R1. https://images.frandroid.com/wp-content/uploads/2020/06/Find_My_network_accessory_protocol_specification.pdf
[2] Apple Inc. 2021. Tracker Detect - Apps on Google Play. https://play.google.com/store/apps/details?id=com.apple.trackerdetect&hl=en&gl=US
[3] Apple Inc. 2023. iCloud+ - Find My. https://www.apple.com/icloud/find-my/
[4] Gabrielle Beck, Harry Eldridge, Matthew Green, Nadia Heninger, and Abhishek Jain. 2023. Abuse-Resistant Location Tracking: Balancing Privacy and Safety in the Offline Finding Ecosystem. Cryptology ePrint Archive, Paper 2023/1332. https://eprint.iacr.org/2023/1332 https://eprint.iacr.org/2023/1332.
[5] Thomas Brewster. 2023. Criminals Are Allegedly Using Apple AirTags To Track Illegal Weapons. https://www.forbes.com/sites/thomasbrewster/2023/09/12/apple-airtags-used-to-track-illegal-weapons-dhs-says/

[6] Jimmy Briggs and Christine Geeng. 2022. BLE-Doubt: Smartphone-Based Detection of Malicious Bluetooth Trackers. In *2022 IEEE Security and Privacy Workshops (SPW)*. IEE, San Francisco, CA, USA, 208–214. https://doi.org/10.1109/SPW54247.2022.9833870

[7] Lukas Burg, Max Granzow, Alexander Heinrich, and Matthias Hollick. 2022. OpenHaystack Mobile - Tracking Custom Find My Accessories on Smartphones. In *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '22)*. Association for Computing Machinery, New York, NY, USA, 277–279. https://doi.org/10.1145/3507657.3529655

[8] Andrea Cavallier. 2023. Texas Man Uses Apple AirTag to Find Man Who Stole His Truck, Kills Him. https://www.dailymail.co.uk/news/article-11930083/Texas-man-uses-30-Apple-AirTag-track-thief-stole-Chevy-truck.html

[9] CBS Chicago. 2023. Prosecutors: Man Killed Girlfriend for Removing AirTag He'd Put in Her Car - CBS Chicago. https://www.cbsnews.com/chicago/news/armoni-henry-charged-murder-jailene-flowers-marianos-evergreen-park/

[10] Rose Ceccio, Sophie Stephenson, Varun Chadha, Danny Yuxing Huang, and Rahul Chatterjee. 2023. Sneaky Spy Devices and Defective Detectors: The Ecosystem of Intimate Partner Surveillance with Covert Devices. In *32nd USENIX Security Symposium (USENIX Security 23)*. USENIX Association, Anaheim, CA, 123–140. https://www.usenix.org/conference/usenixsecurity23/presentation/ceccio

[11] Guillaume Celosia and Mathieu Cunche. 2020. Discontinued Privacy: Personal Data Leaks in Apple Bluetooth-Low-Energy Continuity Protocols. *Proceedings on Privacy Enhancing Technologies* 2020, 1 (Jan. 2020), 26–46. https://doi.org/10.2478/popets-2020-0003

[12] Guillaume Celosia and Mathieu Cunche. 2020. Valkyrie: A Generic Framework for Verifying Privacy Provisions in Wireless Networks. In *'WiSec '20: Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. ACM, Online, 6.

[13] Hartley Charlton. 2021. Apple's AirTag Item Trackers Increasingly Linked to Criminal Activity. https://www.macrumors.com/2021/12/31/airtag-increasingly-linked-to-crime/

[14] Code Penal Legifrance 2018. Article 222-33 - Code Pénal - Légifrance. https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000037289662

[15] Criminal Code Canada 1985. Criminal Code (R.S.C., 1985, c. C-46) | Criminal Harassment. https://laws-lois.justice.gc.ca/eng/acts/c-46/section-264.html

[16] Tess Despres, Noelle Davis, Prabal Dutta, and David Wagner. 2023. DeTagTive: Linking MACs to Protect Against Malicious BLE Trackers. In *Proceedings of the Second Workshop on Situating Network Infrastructure with People, Practices, and Beyond (SNIP2+ '23)*. Association for Computing Machinery, New York, NY, USA, 1–7. https://doi.org/10.1145/3609396.3610544

[17] Timothy M. Diette, Arthur H. Goldsmith, Darrick Hamilton, William Darity Jr., and Katherine McFarland. 2014. Stalking: Does It Leave a Psychological Footprint? *Social Science Quarterly* 95, 2 (2014), 563–580. https://doi.org/10.1111/ssqu.12058

[18] Molly Doyle and Mitchell Kajzer. 2021. Exploring the Criminal Use and Data Collection of Apple AirTags. (2021).

[19] Harald Dressing, Christine Kuehner, and Peter Gass. 2005. Lifetime Prevalence and Impact of Stalking in a European Population: Epidemiological Data from a Middle-Sized German City. *The British Journal of Psychiatry* 187, 2 (Aug. 2005), 168–172. https://doi.org/10.1192/bjp.187.2.168

[20] Find Law 2021. Texas Penal Code - PENAL § 16.06. https://codes.findlaw.com/tx/penal-code/penal-sect-16-06/

[21] Geoffrey A. Fowler. 2021. Review | Apple's AirTag Trackers Made It Frighteningly Easy to 'Stalk' Me in a Test. https://www.washingtonpost.com/technology/2021/05/05/apple-airtags-stalking/

[22] Chinmay Garg, Aravind Machiry, Andrea Continella, Christopher Kruegel, and Giovanni Vigna. 2021. Toward a Secure Crowdsourced Location Tracking System, In WiSec '21: Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks. *arXiv:2106.00217 [cs]*. https://doi.org/10.1145/3448300.3467821 arXiv:2106.00217 [cs]

[23] Google Inc. 2023. 3 Ways Unknown Tracker Alerts on Android Help Keep You Safe. https://blog.google/products/android/unknown-tracker-alert-google-android/

[24] Alexander Heinrich, Niklas Bittner, and Matthias Hollick. 2022. AirGuard - Protecting Android Users from Stalking Attacks by Apple Find My Devices. In *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '22)*. Association for Computing Machinery, New York, NY, USA, 26–38. https://doi.org/10.1145/3507657.3528546

[25] Alexander Heinrich, Milan Stute, and Matthias Hollick. 2021. 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)*. Association for Computing Machinery, New York, NY, USA, 374–376. https://doi.org/10.1145/3448300.3468251

[26] Alexander Heinrich, Milan Stute, Tim Kornhuber, and Matthias Hollick. 2021. Who Can Find My Devices? Security and Privacy of Apple's Crowd-Sourced Bluetooth Location Tracking System. *Proceedings on Privacy Enhancing Technologies* 2021, 3 (July 2021), 227–245. https://doi.org/10.2478/popets-2021-0045

[27] Alex Kirschner. 2021. Apple Introduces AirTag. https://www.apple.com/newsroom/2021/04/apple-introduces-airtag/

[28] Alex Kirschner and Apple Inc. 2022. An Update on AirTag and Unwanted Tracking. https://www.apple.com/newsroom/2022/02/an-update-on-airtag-and-unwanted-tracking/

[29] Alex Kirschner and Lindsay Shanahan. 2021. Apple's Find My Network Now Offers New Third-Party Finding Experiences. https://www.apple.com/newsroom/2021/04/apples-find-my-network-now-offers-new-third-party-finding-experiences/

[30] Brent Ledvina, Zachary Eddinger, Ben Detwiler, and Siddika Parlak Polatkan. 2023. *Detecting Unwanted Location Trackers*. Internet Draft draft-detecting-unwanted-location-trackers-00. Internet Engineering Task Force. https://datatracker.ietf.org/doc/draft-detecting-unwanted-location-trackers

[31] Legal Information Institute 1996. 18 U.S. Code § 2261A - Stalking. https://www.law.cornell.edu/uscode/text/18/2261A

[32] Legifrance 2020. Chapitre VI : Des Atteintes à La Personnalité (Articles 226-1 à 226-32) - Légifrance. https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006070719/LEGISCTA000006149831/#LEGISCTA000006149831

[33] Natasha Lomas. 2013. Tile Grabs $2.6M Via Selfstarter For Its Lost Property-Finding Bluetooth Tags Plus App. https://social.techcrunch.com/2013/07/24/tile-grabs-2-6m-via-selfstarter-for-its-lost-property-finding-bluetooth-tags-plus-app/

[34] Ryan Mac and Kashmir Hill. 2021. Are Apple AirTags Being Used to Track People and Steal Cars? *The New York Times* (Dec. 2021). https://www.nytimes.com/2021/12/30/technology/apple-airtags-tracking-stalking.html

[35] Jane Mavoa, Simon Coghlan, and Bjørn Nansen. 2023. "It's About Safety Not Snooping": Parental Attitudes to Child Tracking Technologies and Geolocation Data. *Surveillance & Society* 21, 1 (March 2023), 45–60. https://doi.org/10.24908/ss.v21i1.15719

[36] Travis Mayberry, Erik-Oliver Blass, and Ellis Fenske. 2023. Blind My - An Improved Cryptographic Protocol to Prevent Stalking in Apple's Find My Network. *Proceedings on Privacy Enhancing Technologies* 2023, 1 (Jan. 2023), 85–97. https://doi.org/10.56553/popets-2023-0006

[37] Travis Mayberry, Ellis Fenske, Dane Brown, Jeremy Martin, Christine Fossaceca, Erik C. Rye, Sam Teplov, and Lucas Foppe. 2021. 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)*. Association for Computing Machinery, New York, NY, USA, 181–186. https://doi.org/10.1145/3463676.3485616

[38] A. J. McDougall. 2022. Woman Used Apple AirTag to Track and Kill Boyfriend With Her Car: Cops. https://www.thedailybeast.com/indiana-woman-gaylyn-morris-murders-boyfriend-after-using-apple-airtag-to-track-him-cops

[39] Katharina O. E. Müller, Louis Bienz, Bruno Rodrigues, Chao Feng, and Burkhard Stiller. 2023. HomeScout: Anti-Stalking Mobile App for Bluetooth Low Energy Devices. In *2023 IEEE 48th Conference on Local Computer Networks (LCN)*. IEEE, 1–9. https://doi.org/10.1109/LCN58197.2023.10223406

[40] Lauren R. Pace, LaSean A. Salmon, Christopher J. Bowen, Ibrahim Baggili, and Golden G. Richard. 2023. Every Step You Take, I'll Be Tracking You: Forensic Analysis of the Tile Tracker Application. *Forensic Science International: Digital Investigation* 45 (July 2023), 301559. https://doi.org/10.1016/j.fsidi.2023.301559

[41] Christopher Parsons, Adam Molnar, Jakub Dalek, Miles Kenyon, Bennett Haselton, Cynthia Khoo, and Ronald Deibert. 2019. *The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry*. Technical Report.

[42] Kieran Press-Reynolds. 2022. An Influencer and Sports Model Alleged That a Stranger Slipped an Apple AirTag into Her Coat to Track Her in New York. https://www.businessinsider.com/brooks-nader-instagram-model-apple-airtag-stalking-tracked-2022-1

[43] Thomas Roth, Fabian Freyer, Matthias Hollick, and Jiska Classen. 2022. AirTag of the Clones: Shenanigans with Liberated Item Finders. In *2022 IEEE Security and Privacy Workshops (SPW)*. 301–311. https://doi.org/10.1109/SPW54247.2022.9833881

[44] Samsung Electronics Inc. 2022. SmartThings Find. https://support.smartthings.com/hc/en-us/articles/10863369660052-SmartThings-Find

[45] Pauline Schinkels. 2023. AirTags: Ich finde dich. *Die Zeit* (Nov. 2023). https://www.zeit.de/digital/2023-11/airtags-stalking-deutschland-tracker-strafbar

[46] Secure Mobile Networking. 2023. AirGuard - AirTag Protection. https://play.google.com/store/apps/details?id=de.seemoo.at_tracking_detection.release&hl=en

[47] Sentencing Council UK 1997. Harassment and Stalking – Sentencing. https://www.sentencingcouncil.org.uk/outlines/harassment-and-stalking/

[48] Julia Slupska and Leonie Maria Tanczer. 2021. Threat Modeling Intimate Partner Violence: Tech Abuse as a Cybersecurity Challenge in the Internet of Things. In *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*, Jane Bailey, Asher Flynn, and Nicola Henry (Eds.). Emerald Publishing Limited, 663–688. https://doi.org/10.1108/978-1-83982-848-520211049

[49] Sophie Stephenson, Majed Almansoori, Pardis Emami-Naeini, and Rahul Chatterjee. 2023. "It's the Equivalent of Feeling Like You're in Jail": Lessons from Firsthand and Secondhand Accounts of IoT-Enabled Intimate Partner Abuse. *Usenix Security 2023* (2023).

[50] Sophie Stephenson, Majed Almansoori, Pardis Emami-Naeini, Danny Yuxing Huang, and Rahul Chatterjee. 2023. Abuse Vectors: A Framework for Conceptualizing IoT-Enabled Interpersonal Abuse. In *32nd USENIX Security Symposium (USENIX Security 23)*. USENIX Association, 69–86.
[51] Stefan Stieger, Christoph Burger, and Anne Schild. 2008. Lifetime Prevalence and Impact of Stalking: Epidemiological Data from Eastern Austria. *The European Journal of Psychiatry* 22, 4 (Dec. 2008), 235–241. https://scielo.isciii.es/scielo.php?script=sci_abstract&pid=S0213-61632008000400006&lng=es&nrm=iso&tlng=en
[52] Strafgesetzbuch der BRD 2021. § 238 StGB - Einzelnorm. https://www.gesetze-im-internet.de/stgb/__238.html
[53] Strafgesetzbuch der Republik Österreich 2022. RIS - Strafgesetzbuch § 107a - Bundesrecht Konsolidiert, Tagesaktuelle Fassung. https://www.ris.bka.gv.at/NormDokument.wxe
[54] Technische Universität Darmstadt. 2023. AirGuard - Tracking Protection. https://apps.apple.com/app/id1659427454
[55] Tile Inc. 2020. How Does the Tile Network Work? | Tile. https://www.thetileapp.com/en-eu/blog/what-is-tile-network-community-find-lost-stolen-far-away
[56] Tile Inc. 2023. Tile Scan and Secure Overview. https://support.thetileapp.com/hc/en-us/articles/4563823537431-Tile-Scan-and-Secure-Overview
[57] Tile Inc. 2023. What Is Anti-Theft Mode? https://www.tile.com/blog/tile-anti-theft-mode
[58] Morgan Trau, Ohio Capital Journal October 24, and 2023. 2023. Airtag Stalking Would Become Illegal under Proposed Ohio Bill. https://ohiocapitaljournal.com/2023/10/24/airtag-stalking-would-become-illegal-under-proposed-ohio-bill/
[59] K. Turk, Alice Hutchings, and A. Beresford. 2023. Can't Keep Them Away: The Failures of Anti-Stalking Protocols in Personal Item Tracking Devices.
[60] Samantha Valentino. 2023. New Ky. Law Cracks down on AirTag Stalking. https://www.wkyt.com/2023/06/29/new-ky-law-cracks-down-airtag-stalking/
[61] Wanted Law 2020. Depuis quand es-tu harcelé ? https://www.wanted.law/fr/Most-Wanted/Wanted-Facts/Article/Id/24049/Depuis-quand-es-tu-harcelé
[62] Mira Weller, Jiska Classen, Fabian Ullrich, Denis Waßmann, and Erik Tews. 2020. Lost and Found: Stopping Bluetooth Finders from Leaking Private Information. In *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. ACM, Linz Austria, 184–194. https://doi.org/10.1145/3395351.3399422
[63] Tingfeng Yu, James Henderson, Alwen Tiu, and Thomas Haines. 2022. Privacy Analysis of Samsung's Crowd-Sourced Bluetooth Location Tracking System. arXiv:2210.14702 [cs] http://arxiv.org/abs/2210.14702

A APPENDIX

A.1 Collected User Data

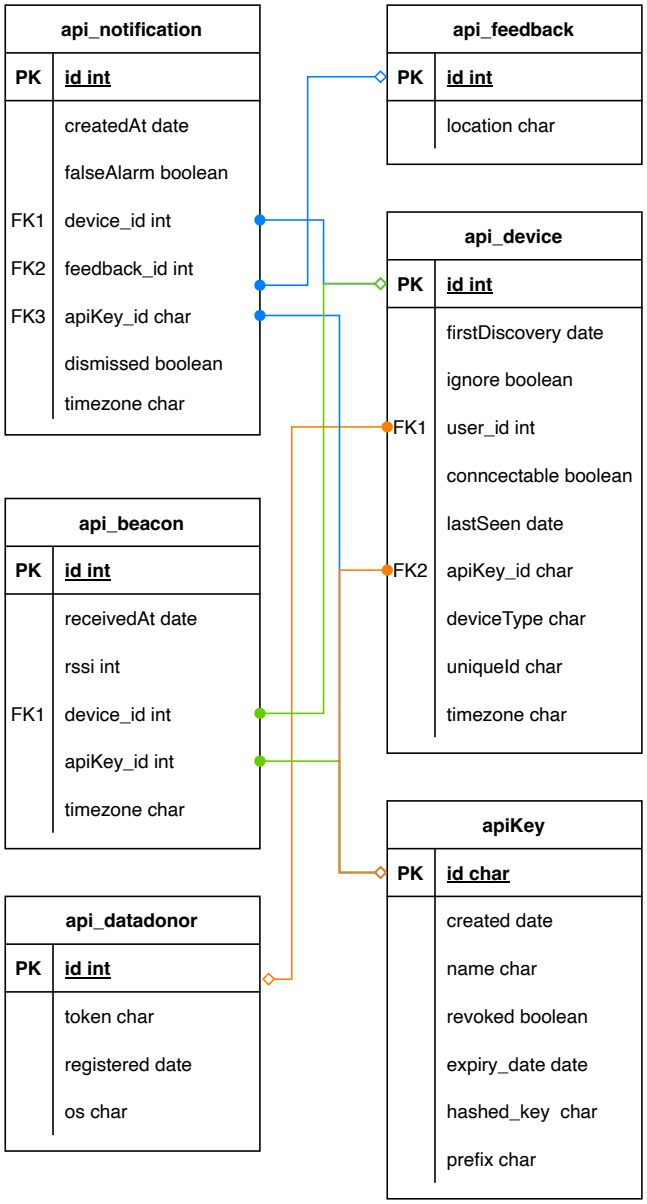

Figure 11: The database scheme for all tables containing user data.

A.2 Survey Responses

Table 5: Regional distribution of participants.

Region	Percentage
North America	38.76%
Western Europe	38.47%
Northern Europe	8.81%
Southern Europe	2.25%
Oceania	2.04%
Eastern Europe (including Northern Asia)	1.87%
South-eastern Asia	0.84%
Latin America and the Caribbean	0.69%
Eastern Asia	0.51%
Northern Africa	0.40%
Southern Asia	0.34%
Sub-Sahara Africa	0.25%
Western Asia	0.23%
Central Asia	0.19%
Northern Asia	0.04%

Table 6: Relationship of stalker and victim.

Relation	Percentage
Prior intimate partner	26.07%
Unknown	23.18%
Known, but I don't want to specify	15.32%
Friend or acquaintance	9.15%
Family member	6.27%
Ex-partner of the current partner	6.07%
Colleague at work	4.08%
Client or customer	2.09%
Boss or supervisor	0.10%

Table 7: Stalker motives.

Motivation	Percentage
Jealousy, envy or distrust	49.35%
Revenge	37.31%
Feeling hurt by rejection	36.72%
Desire for a loving relationship	26.47%
Other	24.38%
Resumption of a former relationship	20.30%

Table 8: Applied stalking methods.

Stalking Method	Percentage
Following	66.17%
Unwanted digital communication: email, messages, Audio/Video messages, etc	61.49%
Loitering nearby	56.52%
Unwanted telephone calls	52.14%
Defamation or spread of personal information	47.66%
Approach via a third party	44.38%
Location tracking (through Bluetooth tracker or other means)	44.28%
Verbal violence	41.89%
Threats	40.70%
Damage of property	30.05%
Invading at home	27.46%
Physical contact	26.76%
Physical violence	19.90%
Sexual harassment	17.61%
Placing orders under your name	15.42%
Sexual assaults	12.14
Other	11.64%

Table 9: Impact on stalking victims' lives

Impact	Percentage
Additional security measures	66.37%
Change of lifestyle	61.00%
Change of phone number, email address, etc	46.07%
Change of residence	32.64%
Filing a report at the police	32.04%
Seeking help from a lawyer	20.40%
Change of workplace	20.20%
Other	17.61%

A.3 Survey Questions

A.3.1 Misuse of Key finders and Bluetooth trackers.

(1) Which potential misuse of key finders / Bluetooth trackers (e.g. AirTags) has been known to you before you started this survey? (multiple-choice)
- Stalking
- Car theft (tracking a valuable car to its parking location)
- Espionage
- Absence tracking (detecting when someone is not at home)
- Other (open-ended answer)

(2) Do you agree with the statement:"During the next 12 months, somebody will try to track me using a key finder" (single choice)
- strongly disagree
- disagree
- neither agree nor disagree
- agree
- strongly agree

(3) Which potential actors do concern you in the case of location tracking? (multiple-choice)
- My employer
- Friends
- Government agencies Companies
- (Former) intimate partners
- Other (open-ended answer)

(4) Do you think the easy accessibility of Apple AirTags, Tile trackers and Samsung Smart Tags has led to more stalking? (single-choice)
- Yes
- No

(5) Do you think there is need for a government regulation that disallows the misuse of key finders such that they can be used for stalking? E.g. forbid tracking of moving targets, delay location updates by several hours (single-choice)
- Yes
- No

(6) Is the intended function of these devices (finding lost items) more important to you than the potential misuse of them? (single-choice)
- Yes
- No

A.3.2 Stalking.

(1) Have you been a victim to stalking in general? (single-choice) *The following questions in this section could only be answered if the respondent answered "Yes" here.*
- Yes
- No

(2) Which gender did your stalker have? (single-choice)
- Male
- Female
- Divers[3]

(3) How long did the stalking continue? (single-choice)
- Less than 1 month
- 1 month up to 1 year
- More than 1 year

(4) How often have you been pursued? (single-choice)
- A few times (irregularly)
- Several times a month
- Several times a week
- Daily

(5) Have you been a victim to ongoing harassment? (single-choice)
- Yes
- No

(6) How is your current relation to the stalker? (single-choice)
- Unknown
- Known, but I don't want to specify
- Prior intimate partner
- Ex-partner of the current partner
- Friend or acquaintance
- Colleague at work
- Client or customer
- Family member

(7) What do you think has been the motivation of the stalker? (multiple-choice)
- Desire for a loving relationship
- Resumption of a former relationship
- Jealousy, envy or distrust
- Revenge
- Feeling hurt by rejection
- Other (open-ended answer)

(8) What methods of stalking have been used? (multiple-choice)
- Unwanted telephone calls
- Loitering nearby
- Unwanted digital communication: email, messages, Audio/Video messages, etc
- Location tracking (through Bluetooth tracker or other means)
- Following
- Approach via a third party
- Damage of property
- Invading at home
- Placing orders under your name
- Defamation or spread of personal information
- Threats
- Physical contact
- Physical violence
- Verbal violence
- Sexual harassment
- Sexual assaults
- Other (open-ended answer)

(9) How has stalking impacted your life? (multiple-choice)
- Change of lifestyle
- Change of phone number, email address, etc Additional security measures
- Change of residence
- Change of workplace
- Seeking help from a lawyer
- Filing a report at the police
- Other (open-ended answer)

A.3.3 Stalking Protection.

(1) Anti-tracking solutions in a Smartphone or based on an app ... (single-choice)
- can cause more harm (due to anxiety) than do good
- might cause some harm
- do not affect users in general
- might give some protection against misusing Bluetooth tracker are the best solution protect against misusing Bluetooth tracker

(2) How do you think stalking protection can be enhanced? (multiple-choice)
- It should be integrated into Smartphones by default
- An-app based solution should be able to find all kinds of key finder devices (from Apple, Samsung, Tile, etc)
- All manufacturers of key finders should publish their own apps that detect stalking attempts
- Governments should provide solutions (can be an app or legislation)

[3]The third gender, if one cannot not be determined to be male or female defined by German law.

- Manufacturers of key finders should prevent using the device for location tracking through technical measures
- Bluetooth Tracker should draw attention to theirselves after some time (Light/Sound signals)
- Other (open-ended answer)

A.3.4 AirGuard.

(1) Are you a user of AirGuard or have you used AirGuard in the past? (single-choice)
The following questions in this section could only be answered if the respondent answered "Yes" here.
- Yes
- No

(2) Since I discovered AirGuard I feel ...
- much less safe
- slightly less safe
- the same as before
- slightly more safe
- much more safe

(3) How would you rate the onboarding of the app? That is the first view you see when opening the app and where you need to permit Bluetooth, Location, and Battery scheduling.
*Participants were rating if the onboarding was **easy to understand**, **helpful**, and **if the app needed to many permissions***

(4) Which version of the dashboard do you prefer? (single-choice)
Participants were seeing two screenshots from a dashboard. One was showing a risk scale and the other was showing a more detailed view on the number of trackers found during the last scans.
- The left/top one with the cards showing a user the current risk status
- The right/bottom one showing a graph and detailed information about trackers found

(5) Chose the statement that fits best concerning the discovery of key finders and other trackers in AirGuard (single-choice)
- AirGuard did not find any
- AirGuard found less than expected
- AirGuard found as many as expected
- AirGuard found more than expected
- AirGuard found much more than expected

(6) Which behaviour of AirGuard would you prefer? An alert is a notification sent by AirGuard that informs you that a potential tracking device has followed you. (single-choice)
- Sending more alerts even though some might be false alarms
- Sending less alerts even though it might take longer or some alerts might be missed
- Sending no alerts and as a user I can check manually in the app if I'm being tracked
- Allow me as a user to configure how fast & accurate alerts should be

(7) Did you receive a notification from AirGuard for a tracker / key finder that has been used to stalk you? (single-choice)
The next question is only show to respondents that answered "yes" in this question.
- Yes
- No

(8) Where was the tracking device located?
- Backpack or Purse
- Clothing
- Bike
- Car
- Other (open-ended answer)

(9) Did you experience incorrect/false notifications from AirGuard and when did they occur? In this case the Bluetooth Tracker close to you was not used to actually track your location.
- Never
- When many people have been around (concert, exhibition, etc.) When my phone was in flight mode
- When I deactivated GPS / location services
- When I was somewhere with a bad GPS signal (inside, underground) When I was commuting in public transport (Train, Airplane, etc.)

(10) Do many incorrect notifications make you feel unsafe or anxious? Please explain your experience with incorrect notifications below. Like all questions, this is an optional question.
This question was an open-ended answer.

(11) Do you think the current methods in AirGuard to find a tracker are helpful? The first screenshot shows the notification that you receive from AirGuard when it detects a potential tracker. The second one shows the screen that you get when you tap on the notification. It shows a map with locations at which the tracker has been seen. Also it offers buttons to interact with certain trackers. For AirTags you can start playing a sound on them to find them.
- Not helpful
- Hardly helpful
- Somewhat helpful
- Quite helpful
- Very helpful

(12) What are you missing in AirGuard?
This question was an open-ended answer.

A.3.5 Demographics.

(1) Please select your gender. (single-choice)
- Female
- Male
- Divers
- Other (open-ended answer)

(2) Please select the age group that matches your age. (single-choice)
- 16-19
- 20-25
- 26-35
- 36-45
- 46-55
- 56-65
- 66-75
- 75+

(3) Please select in which region you are located
- Northern Africa
- Sub-Sahara Africa

- North America
- Latin America and the Caribbean Central Asia
- Eastern Asia
- Northern Asia
- South-eastern Asia
- Southern Asia
- Western Asia
- Eastern Europe (including Northern Asia)
- Northern Europe
- Southern Europe Western Europe Oceania