Smart Tags and Cyber Stalking: A Forensic Analysis of Bluetooth Tags and Anti-Stalking Countermeasures

Parashuram Vananjakar
Inspector of Police, Cybercrime Police Station, Kalaburagi District, Karnataka

Abstract*-- The convenience offered by Bluetooth trackers is undeniable; however, their potential for misuse has raised significant privacy concerns worldwide, including in India. While devices like Apple AirTags and Android Trackers continue to evolve, so too do the risks associated with their unauthorized use. Stalking, in particular, has emerged as a pressing issue, as the use of tracking devices to monitor individuals without their consent constitutes a criminal offense. Study indicate an increasing number of both women and men experiencing stalking incidents at some point in their lives, underscoring a broader societal challenge related to intrusive surveillance behaviors. Numerous incidents have been reported where individuals have discovered Bluetooth trackers unexpectedly placed on their vehicles, within personal belongings, or used in contexts that suggest harassment or unauthorized monitoring of movements. These cases highlight growing concerns that cyber stalking is on the rise in tandem with advances in tracking technology.

***Index Terms*—Air Tag, Android Tag, Stalking, NFC, Smartphone, Find My network, GPS trackers, Bluetooth Scanner. Cyber stalking**

I. INTRODUCTION

Bluetooth trackers such as Apple AirTags and Android Tags have gained immense popularity in recent years. These compact devices provide a convenient solution for locating everyday essentials like keys, wallets, luggage, and even pets. Their small size, extended battery life, and innovative use of crowdsourced location networks make them indispensable gadgets in our fast-paced lives. However, the very features that make Bluetooth trackers effective have also sparked widespread discussions and growing concerns in India regarding privacy and the potential for misuse. Imagine receiving an unsettling notification that reads, “AirTag Found Moving With You,” or discovering a small, unfamiliar device attached to your belongings such scenarios underscore the importance of awareness and preparedness. When a tool designed to help find lost items can be secretly used to track individuals without their consent, it raises serious ethical and security questions. This paper aims to explain how Bluetooth trackers function, analyze the privacy implications associated with their use, and outline practical steps that individuals can take to safeguard themselves against unauthorized tracking.

II. BACKGROUND AND KEY CONCEPTS

A. What is Cyber Stalking?

Cyber stalking is the use of the internet, electronic devices, or digital communication tools to intimidate, harass, or threaten someone. This form of harassment can involve actions such as sending unsolicited messages, breaching personal accounts, impersonating the victim, or constantly monitoring both online behavior and real-world movements through tracking technologies. The impacts of cyber stalking can be severe, often resulting in emotional distress, or physical danger, and it can also lead to real-world confrontations or violence.

B. What is an AirTag?

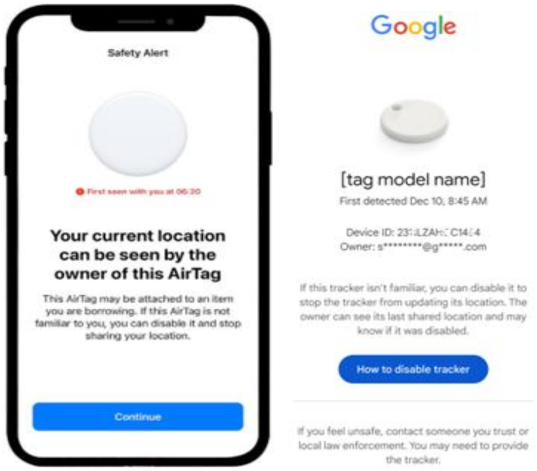
The AirTag is a compact, coin-sized tracker developed by Apple to assist users in easily finding lost or stolen belongings like keys, bags, wallets, and other valuables. Utilizing Apple’s expansive Find My network, the AirTag emits a secure Bluetooth signal that can be anonymously detected by nearby Apple devices. The devices transmit the AirTag's location to the owner via end-to-end encrypted communication, ensuring strong privacy and security. The AirTag offers a seamless, privacy-focused solution to track valuable items within the Apple ecosystem.

C. What is an Android Tag?

Android Tags are Bluetooth-enabled tracking tags designed to help users locate lost items through Google’s Find My Device network. These small devices can be attached to a wide range of personal belongings from everyday essentials like keys, wallets, and backpacks to high-value items such as laptops and bicycles. When an item goes missing, users can trigger alerts and view its last known location on a digital map through a dedicated smartphone application. This technology represents a significant advancement in personal item security and management within the Android ecosystem.

D. Case study

Sample Case: A woman received repeated notifications on her iPhone stating, "AirTag Found Moving With You." One day, while traveling to her office in her car, she saw the same notification again. The following day, as she was driving, the alert reappeared. She then discovered that both her driver and daughter had received similar notifications. When her driver tapped on the alert, a message popped up saying, "Your current location can be seen by the owner of this AirTag." It was then that she realized someone was stalking her.



Safety Alert

First seen with you at 06:20

Your current location can be seen by the owner of this AirTag

This AirTag may be attached to an item you are borrowing. If this AirTag is not familiar to you, you can disable it and stop sharing your location.

Google

[tag model name]

First detected Dec 10, 8:45 AM

Device ID: 23::LZAH::C14::4
Owner: s********@g*****.com

If this tracker isn't familiar, you can disable it to stop the tracker from updating its location. The owner can see its last shared location and may know if it was disabled.

If you feel unsafe, contact someone you trust or local law enforcement. You may need to provide the tracker.

Figure 1: Safety alert displayed after clicking the notification.

She filed a complaint with the Cybercrime Police Station. The police registered a case for stalking and violation of privacy, stating that someone had hidden an AirTag a tracking device in her car to monitor her movements.

During an inspection at a car service center, a hidden AirTag was found secured with adhesive beneath the seat cover behind the driver's seat. Police later apprehended the accused, who was revealed to be the woman's ex-partner. He had reportedly been harassing her for several months and had hidden an AirTag, a tracking device, in her car to stalk and monitor her movements.

III. APPLICATIONS AND ABUSE OF TRACKING TECHNOLOGIES

1. Real-World Applications and Misuses of AirTags and Android Bluetooth Trackers

AirTags (Apple) and Android Tags, such as Samsung SmartTags, are small tracking devices designed to help users locate misplaced items. These Bluetooth-enabled trackers work with Smartphone apps to find everyday items like keys, wallets, and bags; track luggage during travel; locate parked vehicles; monitor valuable equipment; find pets when attached to collars; share item locations with family members; receive separation alerts when items are left behind; and create a digital record of frequently misplaced belongings.

- Stalking and Personal Surveillance

There has been a growing trend of Bluetooth trackers being utilized to monitor people without their knowledge or consent. Devices are often hidden in vehicles, bags, or personal belongings, enabling perpetrators to follow victims undetected. This type of digital monitoring presents serious threats to both personal safety and mental health.

- Corporate Espionage

In the competitive world of business, Bluetooth trackers have become tools for corporate espionage. Malicious actors can plant these devices to monitor the movement of executives, company vehicles, or sensitive equipment. Such surveillance can expose confidential business operations, strategic plans, or client interactions.

- Extortion and Blackmail

Bluetooth tracking technology is being exploited by criminals to gather sensitive information for extortion and blackmail. By mapping a target's daily routines or uncovering secretive behaviors, perpetrators can threaten to expose private details unless demands are met. Imagine receiving a message stating: “I know where you were last night. Pay me, or I’ll leak your location history.”

- Burglaries and Physical Crimes

Thieves use Bluetooth trackers to determine when individuals are away from their homes or vehicles. By analyzing patterns in a person's location data, they can identify the most opportune moments to commit burglaries or vehicle thefts.

- Human Trafficking and Abduction

One of the most disturbing misuses of Bluetooth trackers is in human trafficking and abduction. Traffickers may use these devices to monitor the movements of victims, coordinate illegal transportation across regions, or prevent escape.

- Domestic Abuse and Coercive Control

Trackers are also being used in intimate partner violence, where abusers monitor victims in real-time to control or intimidate them. Even when physical abuse is absent, the constant knowledge of being watched can cause psychological trauma.

- The Top Tracking tags available in the market

Several companies offer tracking tags similar to Apple's AirTag and Android tags, providing a variety of options for both iOS and Android users in the current market. Popular tracking tags include Apple AirTag, Samsung Galaxy SmartTag2, Tile, Chipolo, Xiaomi Smart Tag, Boat Tag, JioTag, and Noise etc. These devices use Bluetooth technology and crowdsourced location networks to help users locate personal belongings efficiently.

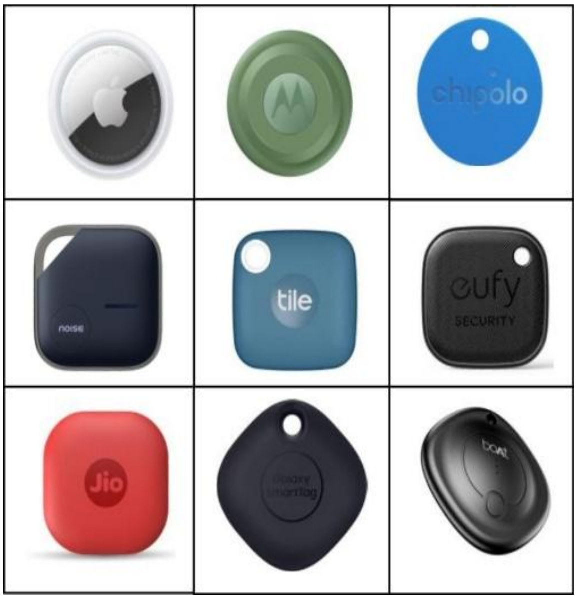


Figure 2: Available smart tags on the market

2. How do Bluetooth trackers differ from GPS trackers?

Bluetooth trackers, such as AirTags and many Android tags, use Bluetooth Low Energy (BLE) technology to connect to nearby smartphones. Their effective range is typically limited to about 100–300 feet (30–90 meters), and their accuracy depends on the proximity of a compatible device. Bluetooth trackers do not have built-in GPS; instead, they rely entirely on Apple's Find My network or Google's Find My Device network to determine their location. The more compatible devices nearby, the more effective and up-to-date the tracking becomes.

Bluetooth vs. GPS Trackers:

Feature	Bluetooth Trackers	GPS Trackers
Network Coverage	Millions of iPhone / Android phone users are part of the network	Works only within cell phone network coverage
Battery Life	Up to 1 year	Continuous power
Size	Compact & lightweight	Large & bulky
SIM & Data Plan	Not required	Required
Accuracy	Moderate	High precision
Real-time Tracking	Only last known location	Live tracking
Indoor Performance	Good	Poor
Best Uses	Keys, wallets, pets, bags	Vehicles, high-value assets,
Power Requirements	Replaceable or built-in battery	Rechargeable battery or hardwired
Connectivity	Bluetooth to smartphone	Cellular networks & GPS satellites

Table 1: Key differences between Bluetooth and GPS trackers.

3. How Apple AirTag Tracks Location?

The Apple AirTag uses both Bluetooth Low Energy (BLE) and Ultra Wideband (UWB) technologies, seamlessly integrated with Apple's broad Find My network to track location. When an AirTag is attached to an item, it emits a secure Bluetooth signal that can be detected by any nearby Apple device (iPhone, iPad, or Mac) participating in the Find My network. These devices anonymously transmit the AirTag's location, along with their own, to Apple's servers. The AirTag owner can then track the item's location on a map within the Find My app.

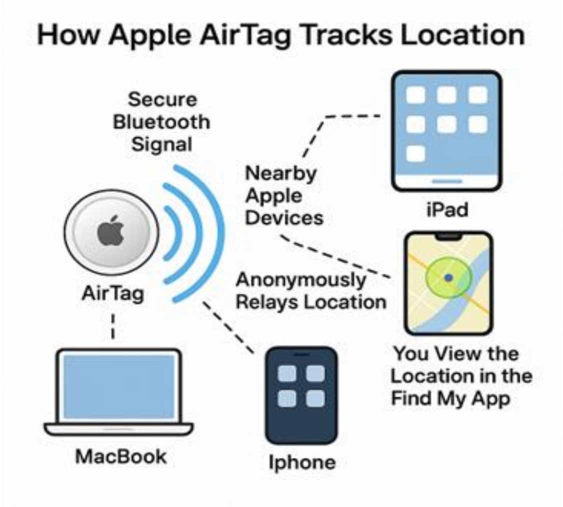

How Apple AirTag Tracks Location
Secure Bluetooth Signal
AirTag
Nearby Apple Devices
iPad
Anonymously Relays Location
You View the Location in the Find My App
MacBook
Iphone

Figure 3: Illustration of how AirTag track location.

4. How Android tag Tracks Location?

Android tags track location primarily using Bluetooth Low Energy (BLE) technology in combination with Google's Find My Device network. When an Android tag is attached to an item, it continuously emits a unique Bluetooth signal. Nearby Android smartphones that are part of the Find My Device network detect this signal and securely relay the tag's location to Google's servers. The owner can then view the last known location of the tag on a map within the Find My Device app. The effectiveness of location tracking depends on the number of Android devices in the vicinity-the more devices nearby, the more accurate and up-to-date the location information becomes.

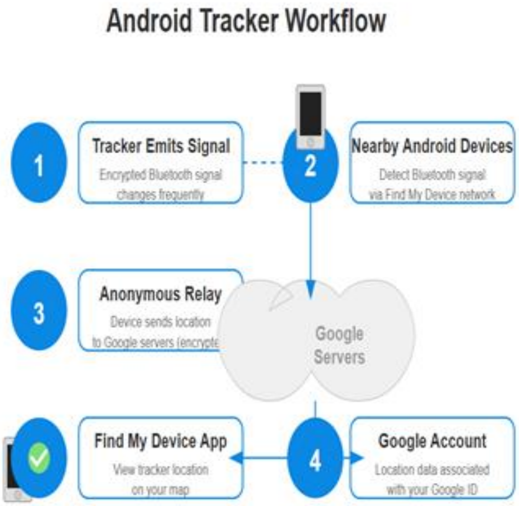
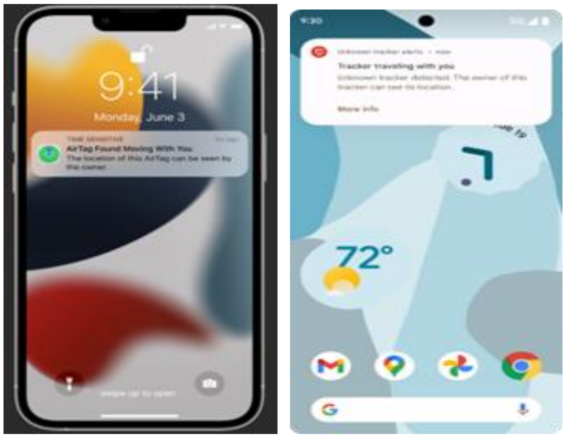

Android Tracker Workflow
1
Tracker Emits Signal
Encrypted Bluetooth signal changes frequently
2
Nearby Android Devices
Detect Bluetooth signal via Find My Device network
3
Anonymous Relay
Device sends location to Google servers (encrypte
Google Servers
Find My Device App
View tracker location on your map
4
Google Account
Location data associated with your Google ID

Figure 4: Illustration of how Android smart tags track location.

5. How to Detect Hidden AirTags and Android Tags in bag or vehicle?

If you think someone is using AirTag or another Tracking Tags to track your location, you can try to identify, locate, and remove any tracking devices that may have been placed near you or in your belongings without your knowledge or consent, using unknown tracker alerts. For example, if an AirTag that is not registered to your Apple ID is detected traveling with you for an extended period, your iPhone will automatically notify you as "**AirTag Found Moving With You**". This alert system ensures that you are promptly informed if someone attempts to use an AirTag to track you without your consent, enabling you to take swift action.

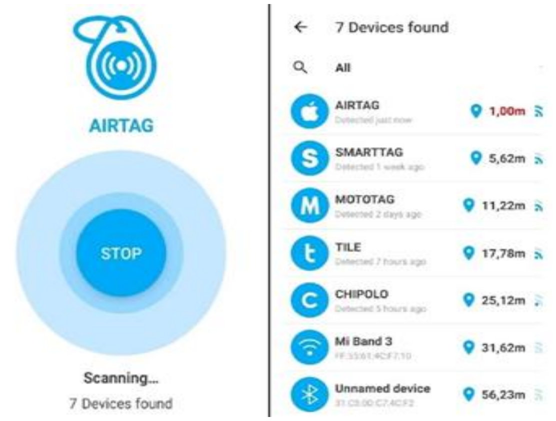

9:41
Monday, June 3

TIME SENSITIVE
AirTag Found Moving With You
The location of this AirTag can be seen by the owner.

Unknown tracker alerts • now
Tracker traveling with you
Unknown tracker detected. The owner of this tracker can see its location.
More info

Figure 5: Alert displayed when unknown trackers are detected.

Android users can detect if tracking tags such as Android Tracker have been placed in their bag or vehicle by downloading apps like 'Tracker Detect,' 'BLE Scanner,' or 'AirTag Scanner' from the Google Play Store. These apps scan for nearby AirTags or other compatible Bluetooth trackers that may be traveling with you without your knowledge.



Scanning...
7 Devices found

7 Devices found
All

AIRTAG Detected just now	1,00m
SMARTTAG Detected 1 week ago	5,62m
MOTOTAG Detected 2 days ago	11,22m
TILE Detected 7 hours ago	17,78m
CHIPOLO Detected 5 hours ago	25,12m
Mi Band 3 FF:35:61:4C:F7:10	31,62m
Unnamed device 31:C3:00:C7:4C:F2	56,23m

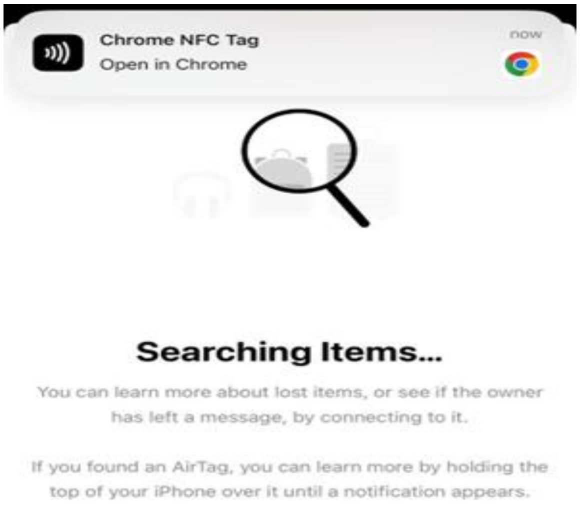
Figure 6: Image showing the AirTag app scanner detecting smart tags.

In addition to scanning, thoroughly inspect your bag and vehicle, including hidden compartments, under seats, inside glove boxes, trunks, wheel wells, Bumpers (front and rear), Battery terminals, between and under seats, Exhaust pipe area and other less obvious areas. Look for small, coin-sized devices that may be tracking tags.

IV. IDENTIFICATION AND NEUTRALIZATION TECHNIQUES

A. Methods for Tracing the Owner of an AirTag or Android Tracker

To check the owner information of an AirTag or a compatible Android tracker, use any NFC-enabled smartphone (iPhone or Android) by holding the top of your iPhone over it until a notification appears, leading you to a webpage that displays details such as the serial number and, if the owner has marked the device as lost, a message with their contact information or the last four digits of their phone number or email address. On iPhones, you can also open the Find My app, tap the "Items" tab, and select "Identify Found Item" to scan the tracker and view similar details.



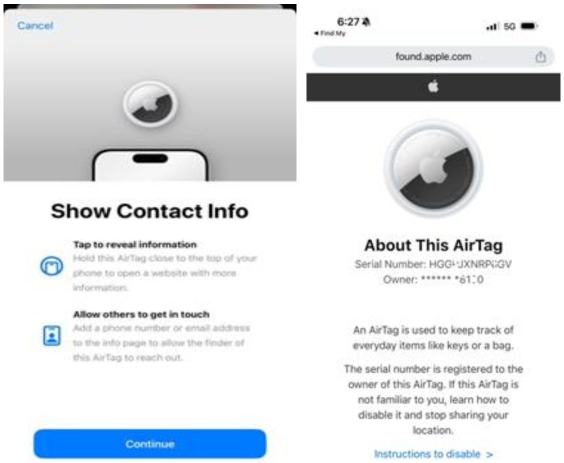
Searching Items...

You can learn more about lost items, or see if the owner has left a message, by connecting to it.

If you found an AirTag, you can learn more by holding the top of your iPhone over it until a notification appears.

Figure 7: Example of checking device details using NFC.

The AirTag is designed to be detected by victims and to enable Law Enforcement to request indentifying information about the owner. If the owner has not provided contact information, only the serial number may be visible, and for privacy reasons, Apple does not display full personal details; if needed, law enforcement can request owner information from Apple using the serial number



Show Contact Info

Tap to reveal information
Hold this AirTag close to the top of your phone to open a website with more information.

Allow others to get in touch
Add a phone number or email address to the info page to allow the finder of this AirTag to reach out.

About This AirTag
Serial Number: HGGJJXNRPGGV
Owner: ****** *61[illegible]0

An AirTag is used to keep track of everyday items like keys or a bag.

The serial number is registered to the owner of this AirTag. If this AirTag is not familiar to you, learn how to disable it and stop sharing your location.

Instructions to disable >

Figure 8: Screenshot showing the AirTag owner information.

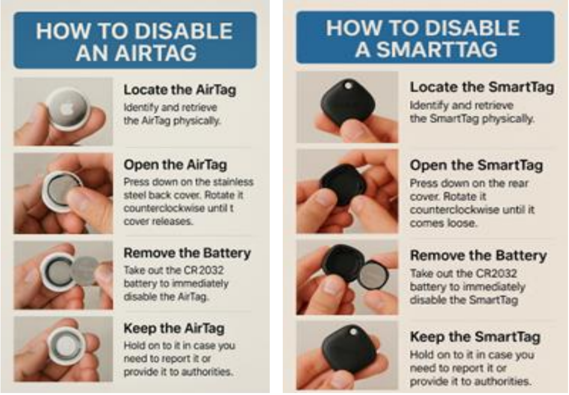
B. How to Disable AirTag and Android Bluetooth Trackers

C. Disabling an AirTag:

To stop the AirTag from tracking you, press down and twist the back of the AirTag counterclockwise to open it. Remove the cover and take out the battery. Once the battery is removed, the AirTag is immediately disabled from reporting your location.

D. Disabling an Android Tag:

Android users who receive an alert about an unknown Bluetooth tracker can use the 'Find Nearby' feature to help locate it. Once the tracker is found, it can be disabled by removing its battery or safely disposing of the device.



HOW TO DISABLE AN AIRTAG

Locate the AirTag
Identify and retrieve the AirTag physically.

Open the AirTag
Press down on the stainless steel back cover. Rotate it counterclockwise until t cover releases.

Remove the Battery
Take out the CR2032 battery to immediately disable the AirTag.

Keep the AirTag
Hold on to it in case you need to report it or provide it to authorities.

HOW TO DISABLE A SMARTTAG

Locate the SmartTag
Identify and retrieve the SmartTag physically.

Open the SmartTag
Press down on the rear cover. Rotate it counterclockwise until it comes loose.

Remove the Battery
Take out the CR2032 battery to immediately disable the SmartTag

Keep the SmartTag
Hold on to it in case you need to report it or provide it to authorities.

Figure 9: Example of the steps to disable an AirTag/Android Tag.

V. REPORTING AND LEGAL ACTION

A. How to Report to Law Enforcement if You Find an AirTag or Android Tag

If you discover an unknown AirTag or Android Bluetooth tracker and suspect it may be used for unauthorized tracking or malicious purposes, and if you feel your safety is at risk, you should report it to your local law enforcement authorities. Make sure to note the serial number and any owner information displayed when you scan the tag with your phone. Provide this information, along with details about where and how you found the tracker, to the police. Law enforcement can contact Apple, Google, or the relevant manufacturer with the serial number to request additional information about the device's registered owner as part of their investigation.

B. How Police Track Down Stalkers Using AirTags and Bluetooth Devices

When law enforcement investigates the misuse of AirTags or Android Bluetooth trackers, they can request specific information from manufacturers through a subpoena or valid legal process. For Apple AirTags, each device is linked to a unique serial number and is associated with an Apple ID. Upon a lawful request, Apple can provide details such as the owner's Apple ID, full name, email addresses, phone numbers, account activation dates, and the activation date for the "Find My" feature on the AirTag. Additionally, Apple may supply logs of account activity, stored electronic communications, and other data that can help attribute the device to a specific user or reveal patterns of use relevant to an investigation.

For Android trackers, Google can provide specific data in response to a subpoena, notice, court order or valid legal process. This may include the Google account associated with the tracker device, the full name of the account holder, email addresses linked to the account, phone numbers registered to the account, account creation and activation dates, device registration information and timestamps, location history data (if enabled by the user), IP addresses used to access the tracking service, login and logout activity logs, communication logs related to the tracker service, Find My Device activity history, device identifiers such as MAC addresses and serial numbers, and any stored electronic communications related to the device or its use.

VI. CONCLUSION

Cyber stalking is a serious issue that can cause emotional harm and invade victims' privacy through harassment, threats, and surveillance. The rise of Bluetooth tracking devices like Apple AirTags and Android Tags has added a new layer of risk, as these tools can be misused for stalking. While they offer convenience for locating items, they also pose significant privacy and safety concerns. Case studies show how easily these devices can be exploited, often without the victim's immediate knowledge.

Combating cyber stalking requires public awareness, vigilance, and legal action when necessary. Education and promoting safe digital habits are essential for prevention and creating a more secure digital environment for everyone.

REFERENCE

[1] Matthew Twells (2023) Network Basics for Hackers

[2] Dr. Ananth Prabhu G (2023) Cyber Safe Girl 6.1

[3] https://www.indiatoday.in/technology/news/story/ex-partner-uses-apple-airtag-to-stalk-ahmedabad-woman-device-found-hidden-under-drivers-seat-2430063-2023-09-02

[4] https://www.apple.com/in/airtag/

[5] https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf

[6] https://www.android.com/intl/en_uk/articles/airtag-alternatives-android/

[7] https://support.google.com/android/

[8] https://www.hackers-arise.com/blog/categories/bluetooth-hacking

[9] https://www.apple.com/in/newsroom/2022/02/an-update-on-airtag-and-unwanted-tracking/

[10] https://www.gonoise.com/products/noise-tag-1-smart-tracker

[11] https://www.jio.com/jiotag-go