# Detecting Unwanted Location Trackers

IETF 119
March 20, 2024

Presenter: Siddika Parlak Polatkan, Google

# Outline

- Overview of the current draft
- Deep dive into the key pieces
- Implementation support on Android and iOS

# Overview of the current internet draft

**May 2023**

Google & Apple jointly announce initiative to establish industry spec

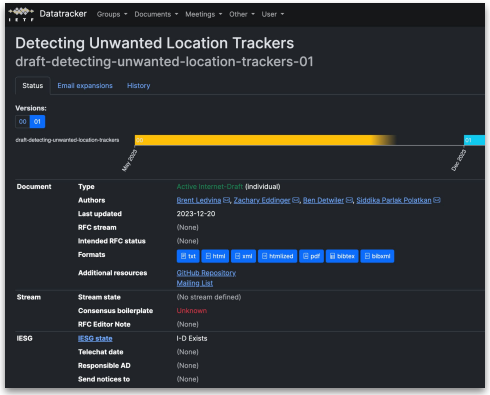
Google and Apple lead initiative for an industry specification to address unwanted tracking

May 2, 2023

***Companies welcome input from industry participants and advocacy groups on a draft specification to alert users in the event of suspected unwanted tracking***

**Dec 2023**

Internet draft integration version (v01) of spec published




**Mar 2024**

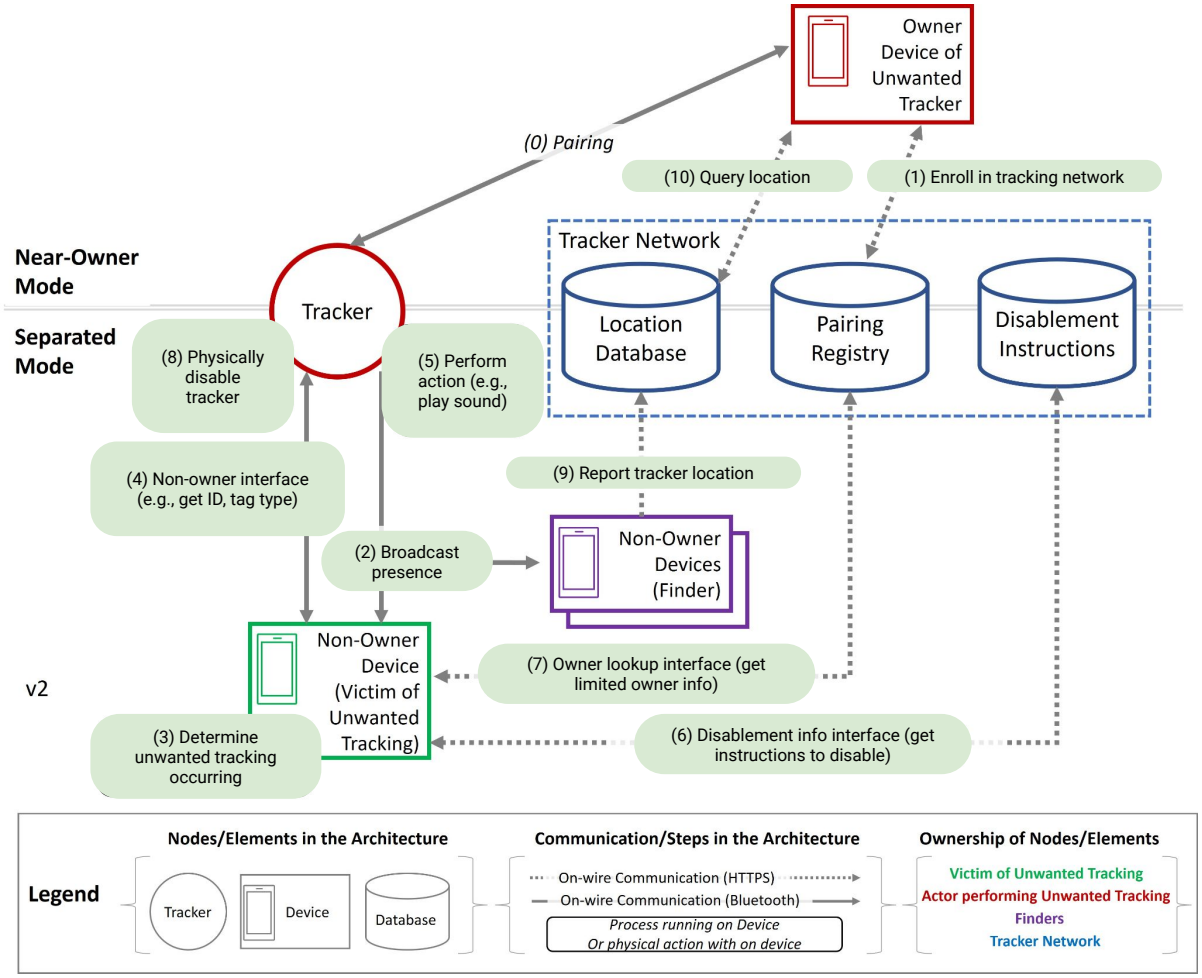
**DULT charter** and **working group** set up

***Today***

IETF-119 WG meeting

**What does v01 version of the draft achieve?**

- Addresses some of the community feedback to v0 (more details can be found in the github repository).
- iOS and Android are referring to this version for implementing for initial support of cross-platform support.




| State | In scope? |
|---|---|
| (1) Enroll in Tracking Network | **Yes:** *Design mechanisms to ensure that devices that do not correctly implement or adhere to the DULT protocol can be detected and excluded...* |
| (2) Broadcast Presence | **Yes:** *Allow a tracking accessory to identify & advertise its presence....* |
| (3) Determine unwanted tracking occurred | **Yes:** *Reference algorithm in scope of charter...* |
| (4) Non-Owner Interface | **Yes:** *Allow a nearby device to trigger behavior...* |
| (5) Perform Action | |
| (6) Disablement Info Interface | **Yes:** *Allow nearby devices to fetch additional information about a tracker accessory...* |
| (7) Owner Lookup Interface | |
| (8) Disable Tracker | **Yes:** *Includes physical security considerations, such as user impact when device has been physically modified to diminish findability...* |
| (9) Report location | **Yes:** *Design mechanisms to ensure that devices that do not correctly implement or adhere to the DULT protocol can be detected and excluded...* |
| (10) Query location | |

# Broadcast Presence

*Advertisement Payload Format*

| Description | Bytes | Requirement |
|---|---|---|
| MAC Address | 0 - 5 | REQUIRED |
| Flags TLV *<br>*Length = 1 byte, type = 1 byte, value = 1 byte* | 6 - 8 | OPTIONAL |
| Service Data TLV<br>*Length = 1 byte, type = 0x16, value = 0xFCB2* | 9 -12 | REQUIRED |
| Network ID | 13 | REQUIRED |
| Near-owner bit **<br>*1 bit: least significant bit; 7 bits: reserved* | 14 | REQUIRED |
| Proprietary company payload data *** | 15 - 36 | OPTIONAL |

* When Flags TLV is omitted, MAC address type needs to be set to random
** Transitioning out of near-owner mode (and into separated mode), requires the accessory to be not detectable by the owner (either via physical separation or BT off) for more than 30 mins. Additional condition of a location reporting to the owner device is acceptable.
*** Company payload data can be variable in length

# MAC Address Format

- The Bluetooth LE advertisement payload SHALL contain an address in the 6-byte Bluetooth MAC address field which looks **random to all parties while being recognizable by the owner device**.

- The owner MUST be able to predict the MAC address or the payload advertised by the accessory at any given time **in order to suppress unwanted tracking alerts** caused by a device's owned accessory.

- **The address SHALL rotate periodically:** When in near-owner state, the accessory SHALL rotate its address every 15 minutes. When in a separated state, the accessory SHALL rotate its address every 24 hours. This duration allows a platform's unwanted tracking algorithms to detect that the same accessory is in proximity for some period of time, when the owner is not in physical proximity.

# Non-Owner Interface & Actions

*Capabilities Provided By Opcodes*

## Available via a GATT service and characteristic over LE (newly defined)

| Capability | Description |
|---|---|
| Read product data | A unique identifier for the particular finding network for the accessory make and model |
| Read manufacturer and model names | Company whose brand will appear on the accessory and model name |
| Read accessory capabilities | 4 bits indicating support for the following:<br>0: play sound 1: motion detector 2: identifier lookup via NFC 3: identifier lookup via BLE |
| Play sound | Start/stop: write to accessory; Command response/sound complete: indication from accessory |
| Read identifier | Applicable when the accessory supports identifier lookup via BLE only.<br><br>To enable this opcode, the accessory MUST be in the identifier read state. To enter the identifier read state, a user action on the accessory MUST be performed (for example, press and hold a button for 10 seconds) |
| Other capabilities | Read protocol implementation version, firmware version, network ID, battery type and level (optional) |

# Identification & Owner Lookup

The accessory MUST include a way to uniquely identify it - either via a serial number or other privacy-preserving solution.

Identifier retrieval can be available through NFC tap or Bluetooth LE.

- Accessories that support identifier retrieval over Bluetooth LE MUST have a physical mechanism, for example a button, to enable identifier retrieval.

Obfuscated owner information (that is associated with the identifier) should include at least one of the following:

- The last four digits of the owner's telephone number. e.g., (***) ***-5555
- An email address with the first letter of the username and entity visible, as well as the entire extension. E.g., b********@i*****.com

# What is NOT in this draft?

Work-in-progress

- Onboarding process

Out-of-scope for this draft

- Crowdsourcing network specifics
- Unwanted tracking detection algorithm and platform specifics
- Network-specific details specific to platforms
  - E.g., Disablement information interface

# What is being implemented on Platforms

Apple and Google teams are working on implementing the v01 version of the draft in their platforms.

When available, manufacturers would need to complete the onboarding process to make their accessories detectable by platforms.

- During onboarding, a product data registry will be created that includes information such as
  - Product data: an 8-byte string representing the unique identifier of a product
  - Disablement instructions: Information on how a user can disable the tracker
  - Identifier lookup method and instructions: A method to retrieve the obfuscated owner information and the identifier.

# Thank You