ODYSEC

無聲的跟隨
藍牙追蹤器濫用

BLUETOOTH TRACKER ABUSE – DETECTION AND RESPONSE

無聲的跟隨

藍牙追蹤器濫用的偵測與應對

Odysec 研究報告 WP-001 ｜ **版本** 1.0 ｜ **發布日** 2026-08-22 **研究線**：融合領域（Cyber × Physical） **DOI**：10.5281/zenodo.22065463

目錄

關於本報告的性質

本報告屬於**綜整與方法論研究**。所有技術描述均依據廠商公開文件、公開的標準草案與已發表的學術研究，本團隊未於本版本中宣稱任何自有實測數據。凡涉及具體行為（例如警示觸發的時間長短）之處，均已標明其會隨作業系統版本與地區設定而變動，讀者應以自身裝置的當下行為為準。

第 8 章載明本團隊規劃中的對照實驗設計。實測結果將以 v2.0 發布。

摘要

低價藍牙追蹤器原本是為了尋找遺失物品而設計，但它們的三項特性——單價低廉、電池以年為單位、依附全球群眾外包網路而無須自備連線——使其同時成為理想的跟蹤工具。使用者不需要任何技術知識，只需要一次實體接觸的機會。

本報告的三個主要發現：

1. **保護機制的設計前提是「被追蹤者持有智慧型手機且藍牙開啟」：**不符合此前提的人——長者、兒童、使用功能型手機者、習慣關閉藍牙者——目前實質上不受任何自動保護。這不是實作缺陷，而是機制的結構性邊界。
2. **跨生態偵測仍是最大缺口：**各廠商的警示以自家網路為主，跨平台標準雖已推進，但涵蓋範圍取決於各家的實作進度；而加害者只要選擇被害者手機生態以外的裝置，就能顯著延後被發現的時間。
3. **技術偵測與法律救濟之間存在斷裂：**多數技術指南止於「找到追蹤器」，但被害者真正的難題在其後：如何保全證據、何時該優先確保人身安全、以及該向誰求助。本報告第 6 章專門處理這一段。

行動建議：若您懷疑自身遭受追蹤，請先確認人身安全，再進行偵測；發現裝置後切勿立即丟棄或重置——該裝置即為唯一之證據。

1. 問題陳述

1.1 為什麼是現在

藍牙追蹤器在市場上已流通數年，技術本身並不新穎。真正改變風險樣貌的是**群眾外包定位網路的規模**：當某個生態系的裝置數量達到都市環境中隨處可見的密度，一枚沒有 GPS、沒有行動網路、成本極低的標籤，就能取得接近即時的位置回報能力。

這使得跟蹤的門檻從「需要技術能力與持續投入」降至「一次接觸機會加上數百元台幣」。

1.2 台灣的具體情境

《跟蹤騷擾防制法》於 2022 年施行，法律工具已經存在。但本團隊檢視公開資源後認為，**技術面的自助偵測指引在中文圈幾乎空白**。被害者面對的實務問題是：

- 我懷疑遭到追蹤，但應如何證明？
- 手機未出現任何警示，是否即代表安全？
- 我發現了可疑裝置，下一步應如何處理？

法律規定了什麼行為違法，卻沒有教人如何發現違法正在發生。這中間的落差，正是技術研究者可以補上的部分。

1.3 本報告要回答的問題

1. 追蹤是如何發生的（威脅模型與技術原理）
2. 如何自行偵測（分層方法論與各層的限制）
3. 發現裝置後之處置（證據保全、人身安全、法律途徑）

---

2. 威脅模型

2.1 攻擊者分型

類型	動機	特徵
親密關係加害者	控制、監視行蹤	**最大宗**：具備長期實體接觸機會，熟悉被害者作息與物品
分手／離婚糾紛當事人	蒐證、騷擾	接觸機會隨關係結束而減少，但仍可能存在（共同財產、子女交接）
商業或職場跟蹤	競爭情報、監控員工	接觸機會限於特定場域
竊盜前置勘查	掌握屋主作息	目標是物品而非人，追蹤器多置於車輛

本報告主要針對第一類，因為它同時具備**最高的接觸機會**與**最嚴重的人身後果**。

2.2 能力假設

這是本威脅模型最需要強調的一點：**攻擊者的技術能力假設為零**。

不需要撰寫程式、不需要越獄或改機、不需要理解藍牙協定。攻擊者只需要：

- 一次將裝置放入對方物品或車輛的機會；
- 自己名下的一支手機與帳號。

正因為門檻如此之低，這類威脅的普遍程度遠高於需要技術能力的攻擊手法。防禦思考不能假設對手技術高明——恰恰相反，要假設對手完全不懂技術，卻擁有充足的實體接觸機會。

2.3 被害者處境

- **不知情期間長**：在收到警示或主動察覺之前，追蹤可能已持續數週。
- **知識不對稱**：加害者知道自己放了什麼、放在哪裡；被害者連該找什麼都不清楚。
- **求助管道斷裂**：報案時，警方需要具體事證；但取得事證需要技術知識；而提供技術協助的管道與保護服務體系之間缺乏銜接。
- **裝置本身可能已被控制**：在親密關係情境中，被害者的手機、雲端帳號、車輛也可能同時處於加害者的掌握之下。偵測方案若假設「手機是安全的」，在最需要它的情境下可能不成立。

---

3. 技術背景：群眾外包定位網路如何運作

3.1 基本流程

追蹤器本身**不知道自己在哪裡**。它沒有 GPS，也沒有行動網路。它做的事情只有一件：持續以低功耗藍牙廣播一段識別訊號。

定位發生在別人的裝置上：

1. 追蹤器廣播識別訊號；
2. 任何一支經過的、屬於同一生態系的手機接收到訊號；
3. 該手機用自己的 GPS 判斷「我在這裡，而我聽到了這個識別訊號」；
4. 這筆資訊經加密後上傳至廠商伺服器；
5. 追蹤器的擁有者查詢時，取得解密後的位置。

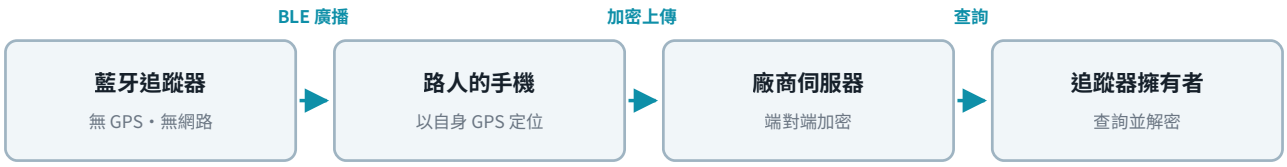

圖 1：群眾外包定位網路的運作流程

這個設計的巧妙之處在於，**代為回報的路人手機無從得知自己回報了什麼**，位置資訊以端對端加密方式僅有擁有者能解讀。對一般使用者的隱私而言，這是良好的設計。

3.2 輪替識別碼的雙面性

為避免追蹤器本身變成長期可追蹤的固定標記，各生態系的裝置會**定期輪替其廣播的識別碼**。

這項設計保護了一般使用者：路人無法透過持續觀察某個固定識別碼來記錄您的行蹤。

但對**被追蹤者**而言，同一項設計造成了困難：

- 您無法單純靠「這個識別碼一直跟著我」來判定，因為識別碼會變；

- 通用型藍牙掃描工具看到的是一串不斷變動的匿名裝置，難以與環境中大量的其他藍牙裝置區分；
- 有效的偵測必須理解各生態系的輪替規則，這正是官方偵測功能相較於通用工具的優勢所在。

這是一個經典的隱私設計權衡：保護多數人不被追蹤的機制，讓少數正在被追蹤的人更難自救。理解這一點，才能理解為何自助偵測不能只靠通用掃描 App。

3.3 三大生態系

生態系	網路來源	偵測支援的基本樣貌
Apple Find My	iPhone／iPad 等 Apple 裝置	iOS 內建意外追蹤警示；另提供 Android 端偵測 App
Samsung SmartThings Find	Galaxy 系列裝置	Samsung 生態內建偵測
Tile	Tile App 使用者	App 內提供主動掃描功能

各生態系的網路密度差異極大，而**網路密度直接決定定位精度與更新頻率**。在 Apple 裝置密度高的都會區，追蹤的即時性遠高於裝置稀疏的區域。

---

4. 現行防護機制與其缺口

這是本報告的核心分析章節。結論先行：**現行機制對「典型情境下的典型使用者」有效，但跟蹤加害者往往不是典型情境**。

4.1 現行機制的基本邏輯

自動警示機制的判斷邏輯大致為：偵測到一個**不屬於您、且長時間與您同行**的追蹤器時發出通知。跨平台的偵測標準（DULT，Detecting Unwanted Location Trackers）由主要廠商共同推動，目標是讓不同生態系的裝置都能被偵測到。

此外，多數追蹤器在與擁有者分離一段時間後會**主動發出聲響**，這是獨立於手機的第二層提示。

> **版本差異提醒**：警示的觸發條件、延遲時間與涵蓋的裝置種類，會隨作業系統版本、地區與廠商政策而變動。本報告刻意不列出具體分鐘數——那類數字在發布後很快就會過時，而依賴過時數字做安全判斷比沒有數字更危險。

4.2 缺口分析

缺口一：機制的前提假設排除了部分人群

自動警示的成立需要三個前提同時滿足：被追蹤者**持有智慧型手機**、**藍牙開啟**、**系統版本支援該功能**。

不符合前提者實質上不受保護，包括：使用功能型手機的長者、未持有手機的兒童、基於省電或隱私習慣關閉藍牙者、以及使用舊版系統而未更新的人。

值得注意的是，**這幾個族群與跟蹤騷擾的高風險族群有相當程度的重疊**。

缺口二：跨生態偵測取決於各家實作進度

跨平台標準的存在不等於全面涵蓋。實際的偵測能力取決於各廠商在各自平台上的實作範圍與更新推送情形。

從攻擊者的角度，這意味著一個簡單的規避策略：**選擇被害者手機生態以外的追蹤器**。這不需要任何技術知識，只需要知道對方用什麼手機。

缺口三：非標準與經改裝的裝置

市面上存在移除或破壞發聲元件的改裝品，也存在不參與任何主流標準的自製或小廠裝置。前者使聲響提示失效，後者可能完全落在偵測機制的涵蓋範圍之外。

缺口四：同行判定的兩難

警示機制必須判斷「這個追蹤器是否與您長時間同行」。這個判斷天生存在兩難：

- 判定過於寬鬆 → 大量誤報（例如與家人同車、在公共運輸上與陌生人長時間同行），使用者很快學會忽略警示；
- 判定過於嚴格 → 漏報，尤其在**被害者與加害者共處同一空間**的情境下——而親密關係暴力恰恰經常是這種情境。

當加害者與被害者同住或共用車輛時，「異常同行」這個訊號本身就失去了鑑別力：這是機制的原理性限制，不是可以靠調參數解決的問題。

缺口五：非追蹤器類的替代手段

本報告聚焦於商用藍牙追蹤器，但需要指出：跟蹤行為也可能透過帳號共享的定位功能、車輛原廠的聯網服務、或安裝於手機的跟蹤軟體（stalkerware）進行。若追蹤器偵測結果為陰性但被害者的處境仍持續被掌握，應將調查範圍擴及這些管道。此議題將另行專文處理。

---

5. 自我偵測方法論

分為四層，由低成本、低風險者開始。**每一層皆有其無法偵測之範圍，因此陰性結果不等於安全**。

圖 2：四層自我偵測方法論

第一層：被動告警（設定，不需操作）

執行事項：確認手機的追蹤偵測功能處於可運作狀態。

- 開啟藍牙與定位權限（追蹤偵測需要兩者）；
- 保持作業系統為最新版本；
- 確認相關通知未被關閉或靜音；
- 若使用 Android 而周遭環境以 Apple 裝置為主，或反之，考慮另行安裝對應生態的官方偵測 App。

限制：只能偵測參與標準的裝置，且必然存在延遲。**收不到警示不代表沒有被追蹤。**

第二層：主動掃描（十分鐘，需操作手機）

執行事項：使用官方 App 的手動掃描功能，或以開源工具進行通用 BLE 掃描。

- 各生態系的官方 App 多提供「主動搜尋周邊未知追蹤器」的功能，這比等待被動警示更快；
- 學術界亦有開源的偵測工具（例如德國 TU Darmstadt 研究團隊發表的 AirGuard），其偵測邏輯公開可檢視；
- 掃描時**遠離自己的其他裝置**，並在移動中重複掃描——真正跟隨您的裝置會在不同地點重複出現。

判讀要點：單次掃描看到大量未知藍牙裝置是正常的（耳機、手環、車機、鄰居的裝置）。有意義的訊號是**同一裝置在多個不同地點重複出現**。

限制：已停止廣播或非標準之裝置無法被掃描發現；通用掃描工具因識別碼輪替而難以追蹤同一裝置。

第三層：實體搜查（一至數小時，不需任何工具）

當前兩層無所獲但懷疑仍然存在，實體搜查往往是最有效的方式。**應按固定順序進行，勿憑直覺隨意翻找。**

車輛（追蹤器最常見的放置處）： - 車外：前後保險桿內側、輪拱、車底樑架、牌照框後方、拖車勾附近； - 車內：座椅下方與椅縫、備胎槽、後車廂側邊置物槽、雜物箱深處、車頂內襯邊緣； - 檢查所有磁吸可附著的金屬平面——磁吸盒是常見的搭配配件。

隨身物品： - 背包與提包的夾層、底部襯墊下方； - 外套內襯、口袋縫線異常處； - 皮夾夾層、行李箱襯裡與輪座； - 常帶的物品中重量或厚度異常者。

住家與贈禮：- 對方贈送的物品——玩偶、擺飾、電子配件；- 兒童的書包與玩具（在監護權爭議情境中應特別檢查）；- 需注意此處也可能涉及錄音錄影裝置，處理方式不同，建議轉由專業協助。

搜查時的安全提醒：若加害者可能觀察到您正在搜查（例如同住），搜查行為本身可能升高風險。此情況下應先與專業協助者討論時機。

第四層：專業鑑識（何時應停止自行處理）

出現下列情形，建議停止自行處理並尋求專業協助：

- 找到裝置，但無法判斷其種類或是否具備錄音錄影能力；
- 懷疑手機本身已被安裝跟蹤軟體；
- 案件可能進入司法程序，需要具備證據能力的鑑識報告；
- 人身安全存在立即風險。

---

6. 發現裝置後之處置

多數技術指南止於第 5 章。但對被害者而言，**找到裝置的那一刻才是真正的難題開始**。

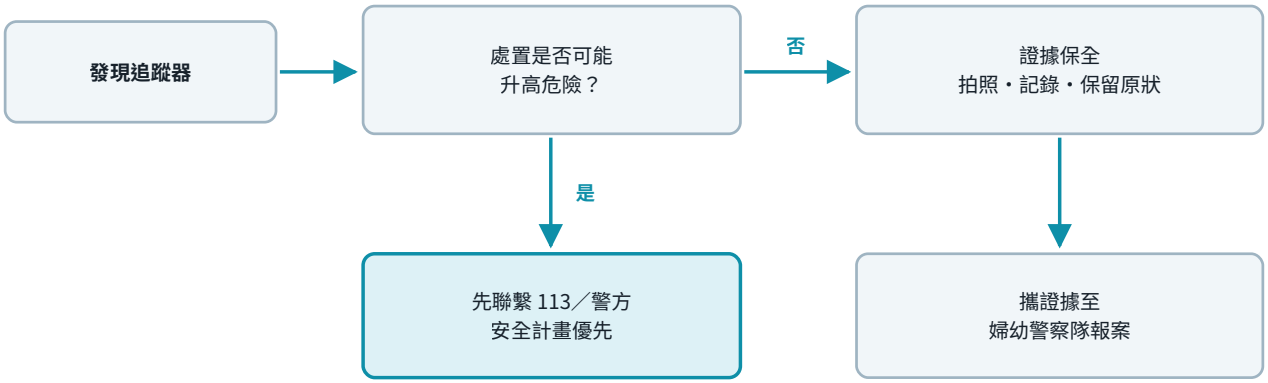

圖 3：發現裝置後的處置流程

6.1 第一優先：人身安全

在處理裝置之前，先做一個判斷：**加害者是否會因為裝置失效而察覺您已發現，並因此升高危險行為？**

追蹤器一旦被移除、遮蔽或關閉，位置回報就會停止或凍結在原地。對加害者而言，這是一個明確的訊號。

若您評估對方可能因此採取進一步的危害行為：

- **請勿立即處置裝置**；
- 先聯繫 113 保護專線或警方討論安全計畫；
- 在安全安排就緒後，再依專業建議處理。

證據重要，但人身安全優先於證據。

6.2 證據保全

若已確認處置裝置不會立即升高風險，依下列順序處理：

1. **拍照存證**：先在**原始位置**拍攝，含環境全景與特寫，讓照片能顯示裝置藏放的位置關係；
2. **記錄時間與地點**：發現的日期時間、確切位置（車輛哪個部位、包包哪一夾層）；
3. **記錄裝置資訊**：外觀、序號、可見的識別碼；若手機能讀取到裝置資訊，一併截圖；
4. **保留原狀**：**請勿重置裝置、請勿拆解、請勿取出電池**——重置會清除與擁有者帳號的關聯，那正是指向加害者的關鍵連結；
5. **裝入不透光的容器或包裝**（若需暫時中斷其功能而不破壞裝置）；
6. **記錄您自己的行蹤時間軸**：對照裝置可能記錄的期間，有助於說明侵害的範圍與持續時間。

> **最常見的錯誤**：發現後因驚嚇或憤怒而立刻丟棄或砸毀裝置。這使得唯一能將行為連結到特定人的物證消失，後續舉證會變得極為困難。

6.3 台灣的法律途徑

報案：向警察機關報案，可洽詢各地**婦幼警察隊**（處理跟蹤騷擾與家庭暴力案件的專責單位）。攜帶第 6.2 節所保全的證據。

《跟蹤騷擾防制法》：該法將反覆或持續的跟蹤騷擾行為納入規範，被害者得請求警察機關調查，並得向法院聲請**保護令**。以追蹤器掌握行蹤，屬於該法所欲規範的行為態樣。

其他可能涉及的規定：依具體情節，可能涉及《刑法》妨害秘密罪章（第 315-1 條就無故以工具或設備窺視、竊聽、竊錄他人非公開活動有所規範）、《個人資料保護法》，以及若裝置置於車輛或住宅內可能涉及的其他規定。**個案的法律評價應由律師判斷**，本報告不構成法律意見。

求助管道：

情境	管道
人身安全立即危險	110
家庭暴力、性侵害、兒少保護	113 保護專線
跟蹤騷擾案件報案	各地警察局婦幼警察隊
法律諮詢	各地律師公會、法律扶助基金會

6.4 後續的數位清理

找到實體追蹤器不代表結束。若加害者曾有實體接觸機會，建議一併檢視：

- 手機與電腦是否有非本人安裝的應用程式或設定檔；
- 雲端帳號的裝置清單、位置共享設定、家庭共享成員；
- 車輛原廠聯網服務的帳號綁定；
- 密碼與二階段驗證的重設（在確認裝置本身乾淨之後才有意義）。

順序很重要：若手機本身已被控制，在該手機上更改密碼等於把新密碼直接交給對方。清理應從確認一台乾淨的裝置開始。

---

7. 給廠商與政策制定者的建議

對廠商：

1. **偵測能力不應以生態系為界**：跨平台偵測的涵蓋範圍應盡快趨於完整，因為加害者選擇裝置時完全不受生態系限制。
2. **正視「共處空間」的漏報情境**：現行以「異常同行」為核心的判定邏輯，在親密關係暴力這個最主要的濫用情境中鑑別力最低。此處需要的可能不是更靈敏的參數，而是不同的判定思路。
3. **為不持有智慧型手機者提供路徑**：例如低成本的獨立偵測裝置，或可由第三方（社工、警察單位）代為執行的檢測工具。
4. **警示訊息應包含後續步驟**：目前的警示多半止於「偵測到未知追蹤器」，若能一併提示「請勿重置、如何保全證據、可聯繫之求助管道」，將顯著改善被害者的處境。

對政策制定者與實務單位：

1. **技術偵測能力應納入保護服務體系**：目前被害者需要自行跨越技術門檻，建議在婦幼警察隊與家暴防治中心層級建立基本的檢測能力與轉介機制。
2. **證據保全指引應公開且易取得**：本報告第 6.2 節的內容應該是每一位受理員警都能當場告知被害者的標準說明。

---

8. 研究限制與後續工作

8.1 本版本的限制

- 本報告為**綜整與方法論研究**，不含自有實測數據；
- 各廠商機制的具體行為（觸發條件、延遲）會隨版本變動，本報告刻意以原理層次描述而不列出具體數值；
- 未涵蓋跟蹤軟體（stalkerware）與車輛原廠聯網服務的濫用，此二者將另行處理。

8.2 規劃中的實測（v2.0）

本團隊規劃以下對照實驗，實測設計於此公開，以便同業檢視與複製：

實驗	目的
三大生態 × 兩種手機平台的偵測矩陣	量化跨生態偵測的實際落差
警示延遲測量	從裝置與擁有者分離到被害端收到警示的時間分布
共處空間情境	驗證「與加害者同住／共乘」情境下的漏報程度
藍牙關閉與省電模式情境	量化非典型使用習慣者的暴露程度
通用 BLE 掃描工具的實際判讀難度	評估非官方工具對一般使用者的可用性

倫理與法律前提：依本團隊《研究倫理準則》第 4.1 節，所有實驗的受測對象僅限研究人員本人，或經書面知情同意的自願者。不對任何未同意者進行測試。

8.3 我們希望收到的回饋

- 實務工作者（社工、員警、律師）對第 6 章流程可行性的意見；
- 對第 4 章缺口分析的補充或反證；
- 台灣本地的案例樣態（**請勿提供可識別當事人的資訊**）。

意見請寄 `contact@odysec.org`；涉及敏感內容請以 PGP 加密寄至 `security@odysec.org`。

附錄 A：偵測檢查表

> 可單獨列印使用。

開始之前 - ☐ 評估：處置裝置是否可能升高加害者的危險行為？若是，先聯繫 113 或警方

第一層：確認被動保護有效 - ☐ 藍牙已開啟 - ☐ 定位權限已授予 - ☐ 作業系統為最新版本 - ☐ 追蹤警示通知未被關閉 - ☐ 已安裝對應另一生態系的偵測 App

第二層：主動掃描 - ☐ 遠離自己的其他藍牙裝置 - ☐ 執行官方 App 的手動掃描 - ☐ 於**不同地點**重複掃描至少三次 - ☐ 記錄重複出現的未知裝置

第三層：實體搜查 - ☐ 車外：保險桿內側、輪拱、車底、牌照框後方 - ☐ 車內：座椅下方與椅縫、備胎槽、後車廂側槽、雜物箱、車頂內襯邊緣 - ☐ 背包提包：夾層、底部襯墊下方 - ☐ 衣物：外套內襯、縫線異常處 - ☐ 皮夾、行李箱襯裡與輪座 - ☐ 對方贈送的物品 - ☐ 兒童的書包與玩具

若找到裝置 - ☐ 先在原始位置拍照（全景＋特寫） - ☐ 記錄日期時間與確切位置 - ☐ 記錄外觀、序號、識別碼 - ☐ **請勿重置、請勿拆解、請勿取出電池** - ☐ 記錄自己的行蹤時間軸 - ☐ 攜帶證據至婦幼警察隊報案 - ☐ 檢視手機、雲端帳號、車輛聯網服務

附錄 B：名詞對照

中文	English	日本語
藍牙追蹤器	Bluetooth tracker	Bluetooth トラッカー
群眾外包定位網路	crowd-sourced location network	クラウドソース型位置ネットワーク
意外追蹤警示	unwanted tracking alert	不要な追跡の通知
輪替識別碼	rotating identifier	ローテーション識別子
跟蹤騷擾	stalking	ストーキング
跟蹤軟體	stalkerware	ストーカーウェア
證據保全	evidence preservation	証拠保全

附錄 C：資料來源

本報告依據下列類型的公開資料撰寫：各追蹤器廠商的官方支援文件與隱私說明、跨平台偵測標準（DULT）之公開草案、學術界關於藍牙追蹤器隱私與偵測的已發表研究（含德國 TU Darmstadt 研究團隊之相關成果與其開源工具 AirGuard）、以及台灣《跟蹤騷擾防制法》、《刑法》、《個人資料保護法》之條文。

各廠商機制的具體行為請以其官方文件之當下版本為準。

引用格式：Odysec（2026）。《無聲的跟隨：藍牙追蹤器濫用的偵測與應對》。Odysec 研究報告 WP-001，版本 1.0。

免責聲明：本報告為技術研究與教育用途，不構成法律意見。個案的法律評價請諮詢執業律師。若您正處於人身安全的立即危險，請撥打 110。