ODYSEC

SILENT COMPANIONS
BLUETOOTH TRACKER ABUSE

DETECTION AND RESPONSE – ODYSEC WP-001

Silent Companions

Detecting and Responding to Bluetooth Tracker Abuse

Odysec Research Report WP-001 | **Version** 1.0 | **Published** 2026-08-22 **Research line**: Convergence (Cyber × Physical) **DOI**: 10.5281/zenodo.22065463

> This is a translation of the Chinese original, which is authoritative.

Table of Contents

Nature of this report

This is a **synthesis and methodology study**. All technical descriptions are based on vendors' public documentation, public standard drafts, and published academic research; this version claims no original test data of our own. Wherever concrete behaviour is involved (such as how long an alert takes to trigger), we note that it varies with operating-system version and regional settings — readers should treat their own device's current behaviour as the reference.

Chapter 8 sets out the controlled experiments we are planning. Measured results will be published as v2.0.

Executive summary

Low-cost Bluetooth trackers were designed to find lost belongings, but three of their properties — negligible price, battery life measured in years, and a global crowd-sourced network that removes any need for their own connectivity — also make them ideal stalking tools. No technical knowledge is required; a single moment of physical access is enough.

Three principal findings:

1. **The protection mechanisms assume the tracked person carries a smartphone with Bluetooth enabled:** People outside that assumption — the elderly, children, feature-phone users, people who habitually keep Bluetooth off — currently receive effectively no automatic protection. This is not an implementation bug; it is a structural boundary of the mechanism.
2. **Cross-ecosystem detection remains the largest gap:** Each vendor's alerts centre on its own network. A cross-platform standard is advancing, but coverage depends on each vendor's implementation progress — and an abuser can significantly delay discovery simply by choosing a tracker from outside the victim's phone ecosystem.
3. **There is a rupture between technical detection and legal remedy:** Most technical guides stop at "finding the tracker". The victim's real difficulties begin afterwards: preserving evidence, judging when personal safety outranks evidence, and knowing whom to turn to. Chapter 6 addresses exactly this stretch.

Key recommendation: if you suspect you are being tracked, secure your personal safety first, then detect; once you find a device, do not discard or reset it — it is the only evidence.

1. Problem statement

1.1 Why now

Bluetooth trackers have been on the market for years; the technology itself is not new. What changed the risk landscape is **the scale of crowd-sourced location networks**: once an ecosystem's devices reach urban ubiquity, a tag with no GPS, no cellular modem, and near-zero cost acquires close-to-real-time reporting capability.

This lowers the barrier to stalking from "technical skill plus sustained effort" to "one moment of access plus a trivial sum of money".

1.2 The Taiwanese context

Taiwan's Stalking and Harassment Prevention Act took effect in 2022; the legal tools exist. Our review of public resources, however, found that **technical self-detection guidance is nearly absent in the Chinese-speaking world**. The practical questions victims face are:

- I suspect I am being tracked — how do I prove it?
- My phone shows no alert — does that mean I am safe?
- I have found a suspicious device — what should I do next?

The law defines what conduct is illegal, but teaches no one how to discover that it is happening. That gap is precisely what technical researchers can fill.

1.3 Questions this report answers

1. How tracking happens (threat model and technical principles)
2. How to detect it yourself (a layered methodology and each layer's limits)
3. What to do after discovery (evidence preservation, personal safety, legal routes)

2. Threat model

2.1 Attacker types

Type	Motive	Characteristics
Intimate-partner abuser	Control, monitoring movements	**The majority:** Long-term physical access; knows the victim's routines and belongings
Separation/divorce party	Evidence-gathering, harassment	Access declines as the relationship ends but may persist (shared property, child handovers)
Commercial or workplace stalking	Competitive intelligence, employee monitoring	Access limited to specific venues
Pre-burglary reconnaissance	Learning occupants' routines	Targets property rather than a person; trackers usually placed on vehicles

This report focuses on the first type, which combines **the greatest access** with **the gravest physical consequences**.

2.2 Capability assumptions

The single most important point of this threat model: **the attacker's technical skill is assumed to be zero.**

No code, no jailbreaking, no understanding of Bluetooth protocols. The attacker needs only:

- one opportunity to slip a device into the victim's belongings or vehicle;
- a phone and account of their own.

Precisely because the bar is that low, this class of threat is far more prevalent than attacks requiring skill. Defensive thinking must not assume a sophisticated adversary — the correct assumption is an adversary who understands nothing technical and has abundant physical access.

2.3 The victim's position

- **Long unaware period**: tracking may have run for weeks before an alert or a suspicion.
- **Knowledge asymmetry**: the abuser knows what was planted and where; the victim does not even know what to look for.
- **Broken help channels**: police need concrete evidence; obtaining it needs technical knowledge; and the channels that provide technical help are poorly connected to protective services.
- **The victim's own devices may already be compromised**: in intimate-partner situations the victim's phone, cloud accounts, and car may also be under the abuser's control. A detection method that assumes "the phone is trustworthy" can fail exactly when it is needed most.

3. Technical background: how crowd-sourced location networks work

3.1 The basic flow

A tracker **does not know where it is**. It has no GPS and no cellular connection. It does exactly one thing: continuously broadcast an identifier over Bluetooth Low Energy.

Locating happens on other people's devices:

1. the tracker broadcasts its identifier;
2. any passing phone belonging to the same ecosystem hears it;
3. that phone uses its own GPS to determine "I am here, and I heard this identifier";
4. the pairing is encrypted and uploaded to the vendor's servers;
5. the tracker's owner queries and obtains the decrypted location.

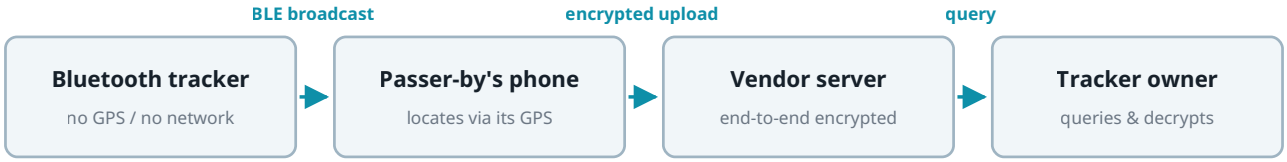

Figure 1: How a crowd-sourced location network works

The elegance of the design is that **the relaying phone cannot know what it relayed** — location reports are end-to-end encrypted and only the owner can read them. For ordinary users' privacy, this is good design.

3.2 The double edge of rotating identifiers

To prevent a tracker itself becoming a long-lived trackable beacon, devices in each ecosystem **rotate their broadcast identifiers periodically**.

This protects ordinary users: a bystander cannot log your movements by following one fixed identifier.

For a **person being tracked**, however, the same design creates difficulty:

- you cannot simply conclude "this identifier keeps following me", because the identifier changes;
- a generic BLE scanner sees a stream of ever-changing anonymous devices, hard to distinguish from the sea of other Bluetooth gear around you;
- effective detection requires understanding each ecosystem's rotation rules — which is exactly the advantage official detection features hold over generic tools.

This is a classic privacy trade-off: a mechanism that protects the many from being tracked makes self-rescue harder for the few who are. Understanding it explains why self-detection cannot rely on generic scanning apps alone.

3.3 The three major ecosystems

Ecosystem	Network source	Detection support in outline
Apple Find My	iPhones, iPads, and other Apple devices	Unwanted-tracking alerts built into iOS; a detection app offered for Android
Samsung SmartThings Find	Galaxy devices	Detection built into the Samsung ecosystem
Tile	Tile app users	In-app manual scan feature

Network density differs enormously between ecosystems, and **density directly determines precision and update frequency**. In an Apple-dense city, tracking is far closer to real time than in sparsely covered areas.

---

4. Current protections and their gaps

This is the report's core analysis. The conclusion first: **current mechanisms work for typical users in typical situations — but stalking is rarely a typical situation.**

4.1 The basic logic of current mechanisms

Automatic alerts follow roughly this logic: notify when a tracker that **does not belong to you has been travelling with you for an extended period**. A cross-platform detection standard (DULT — Detecting Unwanted Location Trackers) is being advanced jointly by the major vendors so that devices of any ecosystem can be detected.

Additionally, most trackers **emit a sound** after prolonged separation from their owner — a second layer of warning independent of any phone.

> **Version caveat**: trigger conditions, delays, and covered device types change with OS version, region, and vendor policy. This report deliberately quotes no specific minute counts — such numbers become outdated soon after publication, and a stale number used for a safety decision is worse than none.

4.2 Gap analysis

Gap 1: the mechanism's premises exclude part of the population

Automatic alerts require three premises at once: the tracked person **carries a smartphone**, **Bluetooth is on**, and **the OS version supports the feature**.

Those outside the premises receive effectively no protection: elderly feature-phone users, children without phones, people who disable Bluetooth to save power or by privacy habit, and users on old OS versions.

It is worth stating plainly: **these groups overlap substantially with the groups at highest risk of stalking.**

Gap 2: cross-ecosystem detection depends on implementation progress

A standard's existence does not equal full coverage. Actual detection capability depends on what each vendor has implemented and shipped on each platform.

From the attacker's perspective this implies a trivially simple evasion: **choose a tracker from outside the victim's phone ecosystem.** It requires no technical knowledge — only knowing what phone the victim uses.

Gap 3: non-standard and modified devices

Devices with speakers removed or disabled circulate in the market, as do small-brand or self-built tags that participate in no mainstream standard. The former defeat the acoustic warning; the latter may fall entirely outside detection coverage.

Gap 4: the co-travel dilemma

Alerting requires judging whether a tracker has been "travelling with you abnormally". That judgment faces an inherent dilemma:

- too loose → floods of false positives (family in the same car, strangers on long public-transport rides), teaching users to ignore alerts;
- too strict → missed detections, above all where **victim and abuser share the same space** — which is exactly the usual shape of intimate-partner abuse.

When abuser and victim live together or share a car, "abnormal co-travel" loses its discriminating power entirely: This is a limitation of principle, not something a parameter tweak can fix.

Gap 5: alternatives beyond trackers

This report focuses on commercial Bluetooth trackers, but stalking can also proceed through shared-account location features, a car's factory telematics, or stalkerware installed on the phone. If tracker detection is negative yet the victim's situation clearly remains known to the abuser, the investigation should widen to those channels. We will address them in a separate report.

---

5. A self-detection methodology

Four layers, starting with the lowest cost and risk. **Every layer has things it cannot detect; a negative result is not proof of safety.**

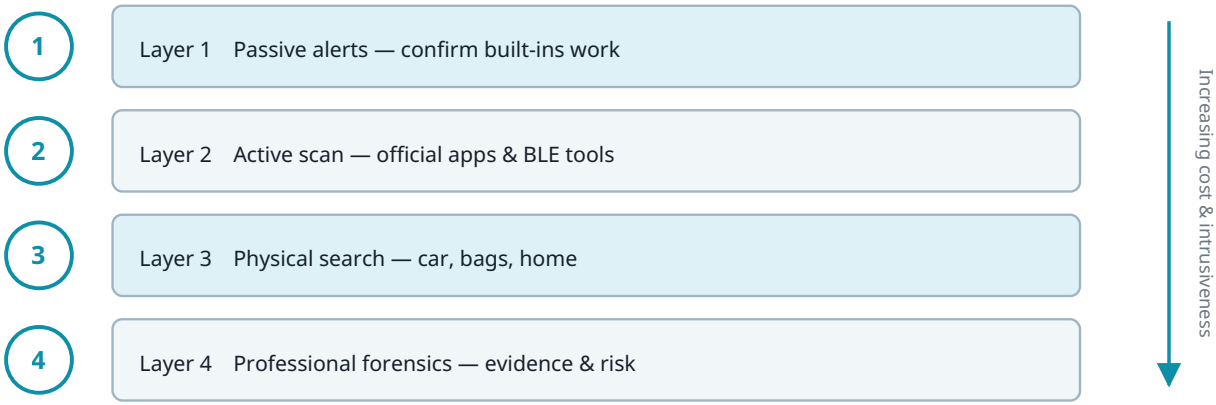

Figure 2: The four-layer self-detection methodology

Layer 1: passive alerts (settings; no action needed)

Actions: confirm your phone's tracking-detection features can actually operate.

- Keep Bluetooth and location permissions on (detection needs both);
- Keep the OS current;
- Confirm the relevant notifications are not disabled or muted;
- If you use Android in Apple-dense surroundings (or vice versa), consider installing the other ecosystem's official detection app.

Limits: only standard-participating devices are detectable, and delay is inherent. **No alert does not mean no tracker.**

Layer 2: active scanning (ten minutes; phone in hand)

Actions: use the manual-scan feature of official apps, or a generic BLE scanner.

- Most ecosystems' official apps can actively search for unknown trackers nearby — faster than waiting for a passive alert;
- Academia offers open-source detectors (for example AirGuard, published by the research group at TU Darmstadt) whose detection logic is publicly reviewable;
- Scan **away from your own devices**, and repeat while moving — a device genuinely following you reappears across locations.

Reading the results: seeing many unknown Bluetooth devices in one scan is normal (earbuds, wristbands, car units, neighbours). The meaningful signal is **the same device recurring across different places**.

Limits: devices that stop broadcasting, or non-standard ones, will not appear; generic scanners struggle to follow one device across identifier rotations.

Layer 3: physical search (one to several hours; no tools)

When the first two layers find nothing but suspicion remains, a physical search is often the most effective step. **Search in a fixed order, not by intuition.**

Vehicle (the most common placement): - Outside: inside bumpers front and rear, wheel arches, underbody rails, behind the licence-plate frame, near the tow hook; - Inside: under and between seats, spare-wheel well, boot side pockets, deep in the glovebox, roof-lining edges; - Check every magnetic-friendly metal surface — magnetic cases are a common accessory.

Carried items: - Bag compartments and under base padding; - Coat linings, seams that feel odd; - Wallet slots, suitcase linings and wheel housings; - Any regularly carried item with unusual weight or thickness.

Home and gifts: - Items given by the person concerned — plush toys, ornaments, electronic accessories; - Children's schoolbags and toys (especially amid custody disputes); - Note that this territory may also involve audio/video recording devices, which are handled differently — professional help is advisable.

Safety note while searching: if the abuser may observe you searching (e.g., cohabitation), the search itself can escalate risk. Discuss timing with professional support first.

Layer 4: professional forensics (when to stop handling it yourself)

Stop handling it yourself and seek professional help when:

- you have found a device but cannot determine its type or whether it records audio/video;
- you suspect the phone itself carries stalkerware;
- the case may enter legal proceedings and needs forensically sound reporting;
- there is immediate danger to personal safety.

---

6. What to do after discovery

Most technical guides end at chapter 5. For the victim, **the moment of discovery is when the real problem begins**.

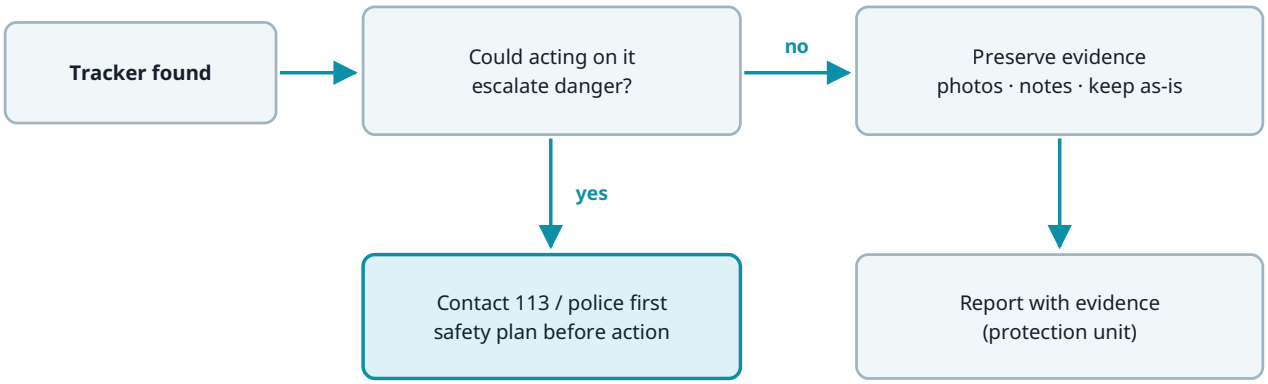

Figure 3: What to do after finding a device

6.1 First priority: personal safety

Before touching the device, make one judgment: **will the abuser notice the device has stopped reporting — and escalate?**

Once a tracker is removed, shielded, or disabled, its location reports stop or freeze in place. To the abuser, that is an unambiguous signal.

If you judge escalation possible:

- **do not act on the device yet**;
- contact the 113 protection hotline or the police first and discuss a safety plan;
- act on the device only after safety arrangements are in place, as advised.

Evidence matters; personal safety outranks evidence.

6.2 Evidence preservation

Once acting on the device will not create immediate risk, proceed in this order:

1. **Photograph in place**: wide shots and close-ups at the **original position**, showing where it was hidden;
2. **Record time and place**: date, time, and the exact location (which part of the car, which bag compartment);
3. **Record device details**: appearance, serial number, any visible identifiers; screenshot anything your phone can read from it;
4. **Preserve its state**: **do not reset, do not disassemble, do not remove the battery** — a reset severs the link to the owner's account, which is precisely the connection that points to the abuser;
5. **Place it in an opaque container** if its function must be interrupted without damaging it;
6. **Write down your own movement timeline** over the likely tracking period — it helps establish the scope and duration of the intrusion.

> **The most common mistake**: discarding or destroying the device in shock or anger. That destroys the only physical evidence linking the conduct to a specific person, and later proof becomes very difficult.

6.3 Legal routes in Taiwan

Reporting: file with the police; the **Women's and Children's Protection units** are the specialist divisions for stalking and domestic-violence cases. Bring the evidence preserved per 6.2.

The Stalking and Harassment Prevention Act covers repeated or sustained stalking conduct; victims may request police investigation and petition the court for a **protection order**. Monitoring someone's movements with a tracker is within the conduct the Act addresses.

Other potentially applicable provisions: depending on the facts, the Criminal Code's offences against privacy (art. 315-1 addresses surreptitious surveillance and recording of non-public activity with tools or equipment), the Personal Data Protection Act, and other provisions where a device was placed in a vehicle or residence. **Legal assessment of a specific case belongs to a lawyer**; this report is not legal advice.

Where to call:

Situation	Channel
Immediate danger	110
Domestic violence, sexual assault, child protection	113 protection hotline
Filing a stalking case	Local police Women's and Children's Protection units
Legal consultation	Local bar associations; the Legal Aid Foundation

6.4 Digital clean-up afterwards

Finding a physical tracker is not the end. If the abuser ever had physical access, also review:

- apps or configuration profiles on your phone and computer that you did not install;
- cloud accounts: device lists, location sharing, family-sharing members;
- the car vendor's connected-services account binding;
- password and two-factor resets — meaningful only after the device itself is confirmed clean.

Order matters: changing passwords on a compromised phone delivers the new passwords directly to the abuser. Clean-up starts from one known-clean device.

---

7. Recommendations for vendors and policymakers

For vendors:

1. **Detection should not stop at ecosystem borders:** Cross-platform coverage should be completed quickly, because abusers face no ecosystem constraint when choosing a device.
2. **Confront the shared-space miss:** Judgment logic centred on "abnormal co-travel" is least discriminating in intimate-partner abuse — the single largest abuse scenario. What is needed may not be sharper parameters but a different judgment approach.
3. **Provide a path for people without smartphones:** For example low-cost standalone detectors, or testing tools that third parties — social workers, police units — can operate on a victim's behalf.
4. **Alerts should include next steps:** Today's alerts mostly end at "unknown tracker detected". Adding "do not reset it, how to preserve evidence, whom to contact" would materially improve victims' outcomes.

For policymakers and practitioners:

1. **Bring technical detection into protective services:** Victims currently must overcome the technical barrier alone; basic detection capability and referral mechanisms should exist at the level of Women's and Children's Protection units and domestic-violence prevention centres.
2. **Publish accessible evidence-preservation guidance:** The content of section 6.2 should be a standard explanation every receiving officer can give on the spot.

8. Limitations and future work

8.1 Limitations of this version

- This is a **synthesis and methodology study** with no original test data;
- Concrete mechanism behaviour (trigger conditions, delays) varies by version; this report deliberately stays at the level of principle;
- Stalkerware and factory car-telematics abuse are out of scope and will be treated separately.

8.2 Planned experiments (v2.0)

We publish the experimental design here so that peers can review and replicate it:

Experiment	Purpose
Detection matrix: three ecosystems × two phone platforms	Quantify the real cross-ecosystem gap
Alert-latency measurement	Distribution of time from owner-separation to victim-side alert
Shared-space scenarios	Verify the miss rate when cohabiting or sharing a vehicle
Bluetooth-off and battery-saver scenarios	Quantify exposure of non-typical usage habits
Usability of generic BLE scanners	Assess how interpretable non-official tools are for ordinary users

Ethical and legal premise: per section 4.1 of our Research Ethics Code, all test subjects are the researchers themselves or volunteers with written informed consent. No one is tested without consent.

8.3 Feedback we hope to receive

- Practitioners' views (social workers, police officers, lawyers) on the feasibility of chapter 6;
- Additions or counter-evidence to the gap analysis in chapter 4;
- Local case patterns in Taiwan (**please do not include identifying information**).

Write to `contact@odysec.org`; PGP-encrypt sensitive material to `security@odysec.org`.

Appendix A: Detection checklist

> Printable as a standalone page.

Before you start - ☐ Judge: could acting on a device escalate the abuser's behaviour? If yes, contact 113 or the police first

Layer 1: confirm passive protection works - ☐ Bluetooth on - ☐ Location permission granted - ☐ OS up to date - ☐ Tracking alerts not disabled - ☐ The other ecosystem's detection app installed

Layer 2: active scan - ☐ Away from your own Bluetooth devices - ☐ Run the official app's manual scan - ☐ Repeat in at least three **different places** - ☐ Note unknown devices that recur

Layer 3: physical search - ☐ Car exterior: bumper interiors, wheel arches, underbody, behind plate frame - ☐ Car interior: under/between seats, spare-wheel well, boot side pockets, glovebox, roof lining - ☐ Bags: compartments, under base padding - ☐ Clothing: coat linings, odd seams - ☐ Wallet, suitcase lining and wheels - ☐ Gifts from the person concerned - ☐ Children's schoolbags and toys

If you find a device - ☐ Photograph in place first (wide + close) - ☐ Record date, time, exact position - ☐ Record appearance, serial, identifiers - ☐ **Do not reset, disassemble, or remove the battery** - ☐ Write down your movement timeline - ☐ Take the evidence to the Women's and Children's Protection unit - ☐ Review phone, cloud accounts, car telematics

---

Appendix B: Terminology

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

Appendix C: Sources

This report draws on the following classes of public material: tracker vendors' official support and privacy documentation; the public drafts of the cross-platform detection standard (DULT); published academic research on Bluetooth-tracker privacy and detection (including the TU Darmstadt group's work and its open-source tool AirGuard); and the texts of Taiwan's Stalking and Harassment Prevention Act, Criminal Code, and Personal Data Protection Act.

For the concrete behaviour of any vendor mechanism, consult the current version of that vendor's documentation.

Citation: Odysec (2026). *Silent Companions: Detecting and Responding to Bluetooth Tracker Abuse.* Odysec Research Report WP-001, version 1.0.

Disclaimer: This report serves technical research and education; it is not legal advice. Consult a practising lawyer for any specific case. If you are in immediate danger, call 110 (in Taiwan).