THE INFORMANT IN YOUR POCKET

STALKERWARE – DETECTION AND RESPONSE

The Informant in Your Pocket

Detecting and Responding to Stalkerware

Odysec Research Report WP-002 | **Version** 1.0 | **Published** 2026-08-23 **Research line**: Convergence (Cyber × Physical)

> 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 platform vendors' public documentation, material published by the Coalition Against Stalkerware and similar organisations, and published academic research; this version claims no original test data of our own. Wherever concrete behaviour is involved (such as what triggers a particular protection), we note that it varies with operating-system version and regional settings — readers should treat their own device's current behaviour as the reference.

This report is a companion to WP-001 *Silent Companions*: that report dealt with physical trackers placed on objects, this one deals with surveillance living inside the phone itself — and what the latter can reach goes far beyond location. Chapter 8 sets out the controlled experiments we are planning. Measured results will be published as v2.0.

Executive summary

Stalkerware refers to software or services that, without the knowing consent of the device's holder, continuously report their location, messages, calls and other private information. Compared with a Bluetooth tracker, its reach is far greater: a tracker knows where you are, stalkerware also knows what you said and to whom.

Three principal findings:

1. **The most common route may require installing nothing at all**: with the password to a cloud account, an abuser can follow location, photos and messages through backup, sync and find-my-device services. This kind of account-level surveillance leaves nothing on the device for a scan to find — **a negative scan result does not mean you are not being watched**.
2. **Anti-malware thinking cannot catch permission abuse**: mainstream platform protections are built to block malicious software, yet much of the surveillance in stalking cases is achieved by turning legitimate, store-listed parental-monitoring, anti-theft or built-in sharing features against their subject. The software itself is lawful; the problem lies in the coercive context of its installation and authorisation — something a scanning engine cannot judge in principle.
3. **The act of checking is itself risky**: this is fundamentally unlike the tracker case. If the phone is already monitored, **every check, search and request for help you perform on it may be visible to the other person**. Our methodology therefore begins with Principle 0 — move to a clean device — rather than telling you to start scanning the phone in your hand.

Recommended action: if you suspect your phone is monitored, do not search for help or contact a supporter on that phone; use someone else's device or a public one. Having found monitoring software, do not delete it immediately — preserve evidence first, and assess whether removal would alert the abuser and escalate the danger.

1. Problem statement

1.1 Why now

The gap analysis in WP-001 noted that if tracker detection comes back negative while the victim's movements and private information continue to be known, the investigation should extend to stalkerware on the phone and to account-level surveillance. This report is that promised follow-up.

Stalkerware is not new, but two shifts have changed the shape of the risk:

- **The smartphone has become a complete mirror of a person's life**: location, conversations, photos, calendar, health data and finances all converge on one device. Control the phone and you control a panoramic view of someone's life.
- **The cost of entry has fallen to consumer level**: whether it is a subscription monitoring service or a platform's built-in sharing and supervision features, the interfaces are designed for ordinary people with no technical background.

1.2 The situation in Taiwan

Taiwan's Stalking and Harassment Prevention Act covers, among other conduct, using electronic communications to follow a person's whereabouts and activities; the Offences Against Computer Security and the Offences Against Privacy chapters of the Criminal Code address unauthorised intrusion into another's computer equipment and unauthorised recording of another's non-public activities. The legal tools exist, but the same gap identified in WP-001 reappears: **there is no complete self-help detection and response guide in Chinese**. The practical questions victims face are:

- The other person always knows where I have been and who I have spoken to, yet I can find nothing wrong. Where do I start?
- I installed anti-virus software and the scan found nothing. Does that mean I am safe?
- I found monitoring software. Is deleting it enough?

1.3 Questions this report answers

1. How the surveillance happens (threat model and three technical vectors)
2. How to detect it yourself (a layered methodology, the limits of each layer, and why it cannot be done on the phone in question)
3. What to do after finding it (evidence preservation, personal safety, legal routes, rebuilding a clean environment)

2. Threat model

2.1 Types of attacker

Type	Motive	Characteristics
Intimate-partner abuser	Control; monitoring movements and contacts	**The largest group**: sustained physical access, and often knows or can obtain the unlock code
Party to a separation or divorce	Gathering material; continued control	Account access established during the relationship often survives the separation
Surveillance within a family	Control in the name of care	Parental-monitoring tools used on adult or near-adult family members
Workplace overreach	Crossing the line in the name of management	Company devices or MDM privileges used for monitoring beyond work

This report addresses mainly the first two, because they combine **the greatest access** with **the most serious physical consequences**.

2.2 Capability assumptions

As in WP-001, **the attacker's technical ability is assumed to be zero**. The attacker need not write code or understand the operating system. All they need is **any one** of the following:

- one opportunity with the phone unlocked (or knowledge of the unlock code);
- the password to your cloud account (or the ability to pass its password-reset process);
- having once handled the device under the guise of "setting it up for you".

In an intimate relationship, all three are everyday occurrences. **Knowing a partner's unlock code is treated in most relationships as a sign of trust — the threat model has to acknowledge that social reality** rather than assume the code is secret.

2.3 The victim's position

- **Total loss of information**: unlike a tracker, which leaks only location, phone surveillance can reach message content, calls, photo libraries and browsing history.
- **The channel for checking is itself monitored**: the most natural reaction is to search for what to do on one's phone — and that phone is the monitored device.
- **Consent and coercion are indistinguishable**: in a controlling relationship, "voluntarily" handing over a password or "voluntarily" installing a location app may happen under pressure. The technical mechanism sees one lawful authorisation; it cannot see the coercion behind it.
- **Device and account may be lost together**: an abuser may hold the phone, the cloud account and the email account at once. Cleaning up any single point (changing one password, say) may be noticed and reversed from another.

3. Technical background: three vectors

Understanding this classification is the foundation of our methodology, because **the three vectors are detected in completely different places**: some require examining the device, some the account. Looking in the wrong place produces a false sense of safety.

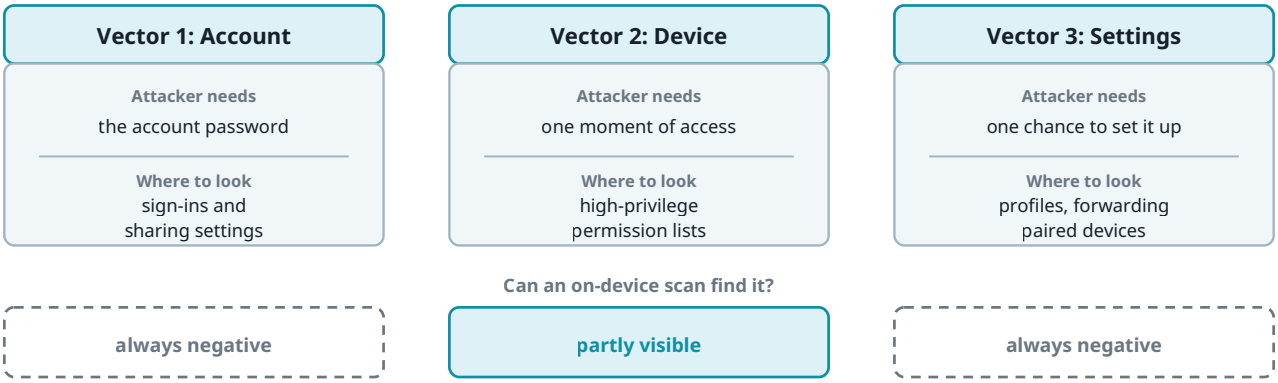

Figure 1: Three surveillance vectors and where each is detected

3.1 Vector one: account-level surveillance (nothing installed on the device)

With the cloud-account password, an abuser can sign in from their own device and obtain everything the account synchronises: location (find-my-device features), photos, backup contents, contacts, calendar, and depending on the platform possibly messages too.

Three properties make this vector extremely favourable to the abuser:

- **A device scan will always be negative**: there is nothing extra on the phone;
- **It persists**: as long as the password is unchanged and the session is not signed out, the access continues;
- **The source is hard to notice**: few people check the list of signed-in devices on their accounts.

In addition, a platform's built-in **location sharing** and **family sharing** features, switched on during the relationship and never switched off as it deteriorated, amount to a forgotten surveillance channel.

3.2 Vector two: device-level surveillance (requires one moment of physical access)

That is, installing monitoring software on the phone. The two platforms differ:

- **Android**: permits installation from outside the store. Once installed, monitoring software typically requests high privileges such as **accessibility services** and **device administrator** — mechanisms designed for assistive use and enterprise management, turned around to read screen contents, intercept notifications and prevent removal. After installation such software usually hides its icon or disguises itself as a system component.
- **iOS**: without jailbreaking it is difficult to sideload software that persists, so surveillance in the iOS case usually takes vector one (account) or vector three (settings) instead. A jailbroken device is as

exposed as Android, and the jailbreak itself usually leaves identifiable traces: an unofficial store interface appears, system updates keep failing, or the device behaves noticeably unlike others of the same model.

Device-level monitoring software falls into two classes whose legal and detection positions differ sharply:

Class	How it is obtained	Detection position
Dual-use applications	Lawfully listed in the official store as parental monitoring, anti-theft or employee management	**The mainstream case**: the software is lawful, and a scanning engine has no legitimate reason to flag it
Dedicated monitoring suites	Sideloaded, marketed explicitly or implicitly for watching a partner	More readily flagged by security products, but hides itself once installed

This report deliberately does not name any monitoring product, its source, or how it is installed. Such information helps abusers far more than victims: what a victim needs is how to find something wrong on their own device, not a catalogue of what is on the market. This choice follows the treatment of offensive detail set out in our Research Ethics Code.

3.3 Vector three: settings and peripherals (not software, so not treated as software)

The third vector is neither a leaked password nor installed software, but **the misuse of the device's own legitimate settings**. It is the easiest to overlook, because each setting on its own is a reasonable feature:

- **Configuration profiles and work profiles**: mechanisms designed for enterprise device management which, once installed, can reach traffic routing, application delivery and some usage records. Installing one under the guise of "getting your phone set up" is unremarkable within a relationship.
- **Message and call forwarding rules**: automatic forwarding in email, call diversion with the carrier, or syncing text messages to another device. Once established, such settings persist even if the phone is replaced.
- **Paired peripherals**: watches, in-car systems, headphones, tablets. Pairings often survive the deterioration of a relationship, and in-car systems deserve particular attention — they hold both location history and contacts.
- **Desktop and browser sync**: phone messages synced to a shared computer, or a browser account syncing bookmarks and passwords, can each form a bypass that never touches the phone.
- **Built-in sharing features**: location sharing, family groups, shared albums. These are designed on the assumption of continuing mutual consent, but **no mechanism prompts you to reconfirm when the relationship changes**.

3.4 Comparing the three vectors

The crucial difference is not technical sophistication but **where you should look**:

	Vector 1: account	Vector 2: device	Vector 3: settings
Physical access needed	No	Yes	Usually
Findable by a phone scan	**No**	Partly	**No**
Where it is detected	Sign-in records and sharing settings	The device's high-privilege lists	Device settings and external service rules
How it is removed	Revoke sessions and change credentials	Remove the software and revoke privileges	Review and delete settings one by one
Does replacing the phone help	**No** (it follows the account)	Yes	**No** (most rules live outside the device)

That last row is the most common misconception in practice: **buying a new phone does not end account-level or settings-level surveillance**. If only the device is replaced and the account is left untouched, the new device is exposed the moment it signs in.

---

4. Current protections and their gaps

4.1 The logic of current protections

Both major platforms have developed protection along three lines:

1. **Controlling software provenance**: store review, plus warnings and restrictions on installation from outside the store.
2. **Making permissions visible**: high-risk permissions require explicit authorisation, with indicators while sensitive sensors are in use, and in recent years an interface for reviewing permission history.
3. **Account activity notices**: notifications on sign-in from a new device, and a list of signed-in devices.

All three are effective against the threat model of a stranger planting malware. The difficulty is that the threat model in this report is not a stranger.

4.2 Gap analysis

Gap one: account-level surveillance is outside the field of view of any scan

Security products scan files and software on the device. When the abuser signs in from their own device with the correct password, there is no suspicious object on the device at all. **This is not a**

deficiency in the scanning engine; it is looking in the wrong place. For a victim the consequence is the most dangerous kind: a negative scan report purchased at the price of a false conclusion about safety.

Gap two: the dual-use judgement problem

The feature list of a parental-monitoring application is almost identical to that of a monitoring application. The difference lies not in what the software does but in **whether the device's holder knows and consents** — a fact outside the code, which a scanning engine cannot determine in principle. A vendor that flags all of them harms legitimate use; a vendor that flags none of them admits the primary tool used in stalking cases.

Gap three: the coercive context of authorisation is technically invisible

The system sees a lawful authorisation: a prompt appeared, the user pressed accept. What the system cannot see is that another person was standing beside them at the time. **In a controlling relationship, "voluntary" is a concept the technical layer cannot verify.**

Gap four: the recipient of the alert may be the abuser

If the phone number, the bill or the family group is controlled by the abuser, then security notices, sign-in alerts and subscription statements arrive in their hands. More fundamentally, the device itself may have been bought and set up by the abuser. **At that point every protection premised on "notify the user" has its protected party inverted.**

Gap five: protections assume that discovery should be followed by removal

Current safety prompts almost invariably advise removing suspicious software at once. Under a stranger threat model that is correct; in intimate-partner abuse, a sudden halt in reporting announces to the abuser that they have been detected, and may trigger retaliation directly. **Between detection and removal there needs to be an intermediate step that current mechanisms do not provide at all: safety assessment and evidence preservation.**

Gap six: the chain of trust for devices within a relationship

A device bought, configured or "sorted out" by the other person has an incomplete chain of trust from the outset. No mechanism today lets a user establish after the fact what was done to a phone before it reached their hands. Second-hand devices and gifted devices are, in this sense, the same problem.

---

5. Self-detection methodology

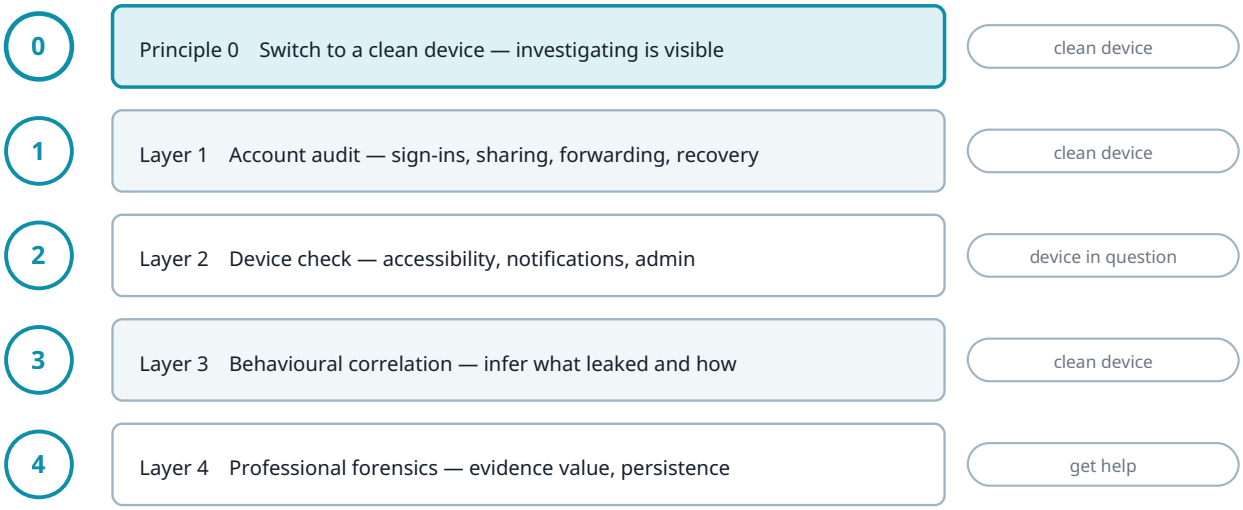

Figure 2: The methodology — Principle 0 and four layers of checks

Principle 0: obtain a clean device first

This is the greatest difference from WP-001, and the one step that cannot be skipped.

In the tracker case the victim's phone is usually a trustworthy tool; in the stalkerware case that phone is the subject of the investigation. If surveillance is present, then every search, every message asking for help and every call you make on that device may appear before the abuser in real time — **including the fact that you are reading this report**.

Therefore:

- Use another person's device, a public computer, or a device with no connection to any of your existing accounts;
- On that clean device, **do not sign in** to any of your existing accounts (signing in may itself trigger a sign-in notice and expose you);
- If you must keep using the original phone normally to avoid arousing suspicion, keep its pattern of use consistent with the past.

Of the four layers below, layers one and three should be carried out on the clean device; layer two must be performed on the phone in question and is the highest-risk layer.

Layer one: account audit (on the clean device; lowest risk)

The account layer is both the most common and the most frequently skipped. Review each of the following:

- **The list of signed-in devices**: is there a device or location you do not recognise? Watch for entries whose names look plausible but are not in fact yours.

- **Location sharing and family groups**: who can currently see your location? When was the sharing turned on?
- **Automatic forwarding and filter rules in email**: is there a forwarding rule you did not create? This is one of the most common and most persistent bypasses.
- **Account recovery options**: do the recovery email address and phone number still belong to the other person? **If recovery options are not cleaned up, a password change can be undone within minutes.**
- **Two-factor settings**: is the second factor bound to a device or number the other person can reach?
- **App-specific passwords and authorised third-party applications**: is there anything you do not remember authorising?
- **Backup settings**: does the backup destination account genuinely belong to you?

Layer two: device check (on the phone in question; highest risk)

Read section 6.1 before carrying out this layer. Everything you do in this layer may be recorded by the monitoring software.

To keep running, device-level surveillance must hold a small number of high privileges. The point of the check is therefore not to spot a suspicious icon but to **go through these lists one by one and confirm that you recognise every entry**:

- **The accessibility services list**: this is the key privilege for reading screen contents and simulating input, and very few legitimate applications need it.
- **The notification access list**: this privilege allows reading every application's notifications, message previews included.
- **Device administrator or device owner privileges**: software holding this cannot be removed in the ordinary way.
- **Configuration profiles and work profiles**: a company you never worked for, or an organisation name you do not recognise, is an anomaly.
- **Permission to install from unofficial sources**: which applications are allowed to install other applications?
- **Battery and mobile-data usage rankings**: software continuously reporting in the background leaves traces in these two lists even when its icon is hidden.
- **Paired Bluetooth devices and known wireless networks**: is there anything that is not yours?

If you find an entry you do not recognise in any of these lists, **record its full name and stop**, then go to chapter 6.

Layer three: behavioural correlation (on the clean device; the most underrated)

When the technical checks come back negative, this layer is often the only way forward. List, one by one, the things the other person knows, and work backwards to **the possible source of each item**:

- Do they know your **location**, or the **content of conversations**? The former may come from vector one or from a tracker; the latter points to the device layer or notification access.
- Do they know about **messages you sent**, or **drafts you never sent**? The range of possible sources for the latter is very narrow.
- Is what they know **immediate**, or **delayed by some hours**? The latter fits periodic sync or backup.
- Do they know something that appeared on **only one particular device**? That narrows the scope to that device directly.

In practice this list can often narrow the investigation to a single vector without any tools at all. Record in writing the date of each incident, exactly what the other person knew, and where you were at the time — this record is also the evidentiary basis for section 6.2.

Layer four: professional forensics (when to stop doing this yourself)

Stop checking on your own and seek professional help if any of the following applies:

- you have found unidentified software with high privileges on the device, and the situation involves immediate risk to your safety;
- the surveillance appears to come from a technically capable abuser, or involves a work device and enterprise management privileges;
- what you need is **evidence usable in legal proceedings**, not merely the removal of the surveillance;
- you have cleaned up repeatedly but the surveillance keeps returning — this usually means a persistence channel remains undiscovered.

Acting yourself and preserving forensic evidence are difficult to reconcile: any clean-up destroys the scene. If the legal route matters to you, **preservation takes priority over removal**.

---

6. What to do after finding surveillance

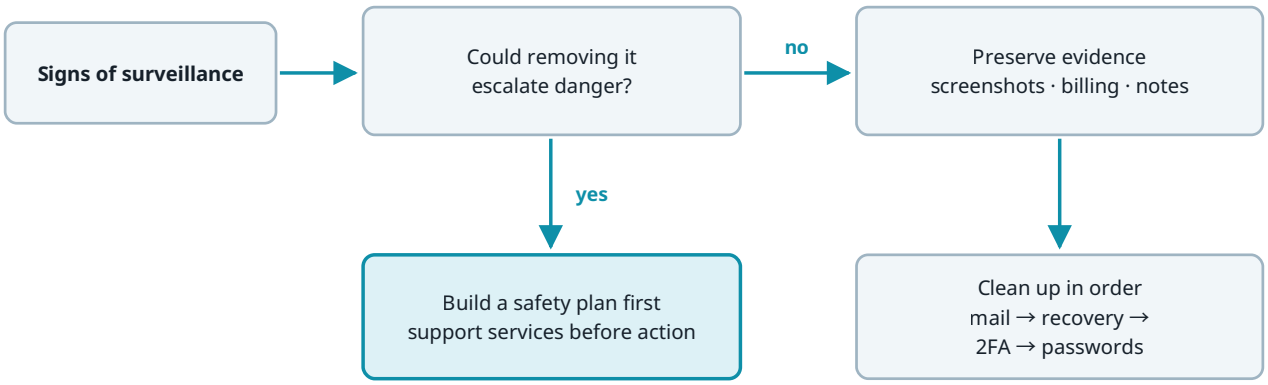

Figure 3: What to do after finding surveillance

6.1 First priority: personal safety

Here the stalkerware case differs most sharply from the tracker case: **removal is an act the other person will notice immediately.**

Reporting stops, the software disappears, accounts are signed out — to an abuser these are unambiguous signals that the victim has become aware and has begun to act. In research on intimate-partner abuse, the stage at which a victim resists or prepares to leave is the stage of greatest danger.

So, before removing anything, establish:

- do you have a workable safety plan (somewhere safe to go, someone to contact, the documents and money you would need)?
- if the other person arrives or makes contact immediately after removal, how will you respond?
- has a professional social worker or the police already become involved?

If the answer is no, the reasonable choice is to leave things as they are for now, build support first, and deal with the technical layer afterwards. Surveillance is hard to endure, but a technical clean-up cannot protect your safety; the order cannot be reversed.

If you are in immediate danger, call 110 (in Taiwan); for protective services and counselling, call 113.

6.2 Evidence preservation

Complete the following record before removing anything. Store all of it **somewhere other than the device in question**:

- screenshots of the suspicious software or settings, with full names and authorisation status;
- screenshots of account sign-in records, with device names, times and locations;
- subscription and billing records — commercial monitoring services must be paid for, and the money trail is among the strongest evidence available;

- the behavioural correlation record built in layer three (dates, what the other person knew, where you actually were);
- if possible, have someone **film you operating the device** with a second device, to corroborate that the screenshots were not fabricated afterwards.

Do not delete the suspicious software, do not reset the device, and do not replace the phone until evidence preservation is complete. A reset is the most thorough removal, and the most thorough destruction of evidence.

6.3 Legal routes in Taiwan

- **Stalking and Harassment Prevention Act**: the conduct it covers includes persistent monitoring, following or ascertaining the whereabouts of a specific person by electronic communications, the internet or other equipment. A victim may report to the police; following investigation a written warning may be issued to the perpetrator, and a further offence within two years of that warning may support an application for a protection order.
- **Criminal Code, offences against computer security**: unauthorised intrusion into another's computer or related equipment, unauthorised acquisition or alteration of another's electromagnetic records, and producing programs specifically for committing these offences, all carry penalties.
- **Criminal Code, offences against privacy**: unauthorised recording — by audio, photography, video or electromagnetic record — of another's non-public activities, conversations, speech or intimate body parts carries penalties.
- **Personal Data Protection Act**: unlawful collection, processing or use of personal data causing harm to others carries corresponding liability.
- **Domestic Violence Prevention Act**: where the parties are family members or intimate partners, a protection order may be sought, which may include prohibiting harassment and stalking of the victim.

When reporting, we suggest going to a Women and Children Protection Unit, or stating clearly that the case involves stalking and domestic violence, so that it is handled by officers familiar with such cases. Bring the evidence preserved under section 6.2, and keep the original device.

6.4 The order for rebuilding a clean environment

Getting the order wrong is the most common reason a clean-up fails. **If you change a password while the account's recovery options are still controlled by the other person, the new password may be reset within minutes.** We suggest the following order:

1. **On the clean device, deal with the email account first**: it is the recovery exit for every other account and must be recovered first.
2. **Clean up recovery options**: remove any recovery email address or phone number that is not yours.
3. **Reset two-factor authentication**: bind it to a device only you hold, and regenerate the backup codes.

4. **Change passwords and revoke all sessions**: revoking sessions is the critical step — with a password change alone, existing sign-ins may remain valid on some services.
5. **Work through the other accounts**: cloud, social, financial, carrier.
6. **Clean up the settings layer**: forwarding rules, call diversion, location sharing, family groups, paired devices, configuration profiles.
7. **Only then deal with the device itself**: after evidence preservation is complete, restore it to factory settings — and **do not restore from an old backup**, which may carry the surveillance settings with it. Set it up again by hand.
8. **Review every other device**: tablets, computers, in-car systems, smart-home devices.

Afterwards, repeat the layer-one account audit within a few weeks. **A return of the surveillance usually means one channel on the list was never found.**

---

7. Recommendations for vendors and policymakers

1. **Bring the account layer into a single safety-check entry point**: a complete audit currently requires crossing several settings screens. One entry point should cover signed-in devices, location sharing, forwarding rules, recovery options and third-party authorisations, with one-tap revocation.
2. **Sharing relationships should expire and require periodic reconfirmation**: location sharing and family groups should not remain valid indefinitely with no review prompt. Periodic reconfirmation would let forgotten sharing lapse naturally.
3. **Persistent disclosure for dual-use software**: software capable of continuously reporting location or content should, whatever its store category, maintain a persistent indicator on the monitored device that cannot be switched off. Legitimate supervision is not harmed by the supervised party knowing.
4. **Redesign the "what happens after discovery" flow**: safety prompts should not uniformly advise immediate removal. There should be a branch for "this may be intimate-partner surveillance" leading to evidence preservation and support resources, rather than straight to a remove button.
5. **The recipient of notices should be independently configurable**: security notices should not go only to the bill payer or the family-group organiser.
6. **Verifiable device handover state**: users should have a way to establish which configuration profiles and high-privilege applications have been installed on a device since it left the factory or was last reset.
7. **Policy**: front-line staff receiving stalking and domestic-violence cases need basic literacy in digital surveillance, and the channels that help victims gather evidence should extend to digital evidence.

---

8. Limitations and further work

8.1 Limitations of this version

- This version is a synthesis and methodology study and **contains no original test data of our own**.
- Platform behaviour varies with operating-system version and regional settings; this report deliberately avoids recording specific figures and version numbers that would quickly become outdated.
- This report does not name specific vendor products, nor record how monitoring software is obtained or installed; this is a deliberate choice (see section 3.2).
- The legal discussion covers current Taiwanese law and does not constitute legal advice.

8.2 Planned measurement (v2.0)

We plan to measure how effective each layer of detection actually is, by controlled experiment:

- **Test devices**: our own test devices, covering several versions of both major platforms.
- **Control design**: surveillance established separately by vectors one, two and three, against an unmonitored device as control.
- **Measurements**: the detection rate and false-negative rate of each layer, whether platform security notices actually fire, and verification that the clean-up procedure is complete (does the surveillance in fact stop afterwards).
- **Ethical limits**: **participants are limited to members of our own team, or participants who have given written consent.** No non-consenting third party is involved, and no real victim's device or data is used. The monitoring samples used in the experiment will not be distributed.

This design follows our Research Ethics Code and is published before the experiments begin, so that it can be scrutinised.

8.3 Feedback we would welcome

- Is this methodology workable in practice? In particular, is Principle 0 too demanding for a victim with no access to a second device?
- What corrections would front-line social workers, police and legal practitioners make to the order of steps in chapter 6?
- Are there persistence channels the layered checks do not cover?
- Is the wording of the translations appropriate to local practice?

Please send feedback to security@odysec.org (PGP-encrypted for sensitive material).

Appendix A: Detection checklist

Principle 0 - ☐ A clean device unconnected to my accounts has been obtained - ☐ No existing account has been signed in on that clean device - ☐ No search for help has been made on the phone in question

Layer one: account audit - ☐ Signed-in device list reviewed entry by entry - ☐ Location sharing and family groups reviewed entry by entry - ☐ Email forwarding and filter rules reviewed entry by entry - ☐ Recovery email address and phone number confirmed as mine - ☐ Two-factor authentication bound to a device I hold - ☐ Third-party application authorisations reviewed entry by entry - ☐ Backup destination account confirmed as mine

Layer two: device check - ☐ Accessibility services list - ☐ Notification access list - ☐ Device administrator or device owner privileges - ☐ Configuration profiles and work profiles - ☐ Sources permitted to install other applications - ☐ Battery and mobile-data usage rankings - ☐ Paired Bluetooth devices and known wireless networks

Layer three: behavioural correlation - ☐ What the other person knows has been listed - ☐ Location-type and content-type information distinguished - ☐ Immediate versus delayed knowledge assessed - ☐ Dates, contents and my own movements recorded

If surveillance is found - ☐ **Do not delete it immediately; do not reset the device** - ☐ Whether removal would escalate danger has been assessed - ☐ Screenshots and account records preserved (stored off the device in question) - ☐ Subscription and billing records preserved - ☐ Evidence taken to a Women and Children Protection Unit - ☐ Clean-up follows the order: mail → recovery options → 2FA → passwords and sessions → other accounts → settings layer → device - ☐ Not restored from an old backup - ☐ Layer-one audit repeated a few weeks later

Appendix B: Terminology

中文	English	日本語
跟蹤軟體	stalkerware	ストーカーウェア
雙用途程式	dual-use application	デュアルユース•アプリ
帳號層監控	account-level surveillance	アカウント層の監視
無障礙服務	accessibility service	ユーザー補助サービス
通知存取	notification access	通知へのアクセス
裝置管理員	device administrator	デバイス管理者
管理描述檔	configuration profile	構成プロファイル
工作設定檔	work profile	仕事用プロファイル
工作階段	session	セッション
救援管道	account recovery options	アカウント回復手段
雙因素驗證	two-factor authentication	二要素認証
乾淨裝置	clean device	クリーンな端末
證據保全	evidence preservation	証拠保全
持久化	persistence	永続化

Appendix C: Sources

This report draws on the following kinds of public material: the official support documentation and privacy descriptions of both major mobile platform vendors; material and practical guidance published by the Coalition Against Stalkerware and its participating organisations; published academic research on intimate-partner surveillance and stalkerware; and the text of Taiwan's Stalking and Harassment Prevention Act, Criminal Code, Personal Data Protection Act and Domestic Violence Prevention Act.

For the concrete behaviour of platform mechanisms, treat the current version of the vendor's own documentation as authoritative. This report and WP-001 *Silent Companions* are companion pieces sharing the same threat model and methodological structure.

Citation: Odysec (2026). *The Informant in Your Pocket: Detecting and Responding to Stalkerware.* Odysec Research Report WP-002, 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); for protective services and counselling, call 113.