口袋裡的告密者
手機跟蹤軟體

STALKERWARE – DETECTION AND RESPONSE

口袋裡的告密者

手機跟蹤軟體（Stalkerware）的偵測與應對

Odysec 研究報告 WP-002 ｜ **版本** 1.0 ｜ **發布日** 2026-08-23 **研究線**：融合領域（Cyber × Physical） **授權**：
CC BY 4.0 — 可自由散布與改作，惟須註明出處。

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平台廠商公開文件、反跟蹤軟體聯盟（Coalition Against Stalkerware）等組織的公開資料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（例如某項系統防護的觸發條件）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。

本報告為 WP-001《無聲的跟隨》之姊妹篇：前者處理放置於物品上的實體追蹤器，本篇處理寄生於手機本身的監控——後者能取得的資訊遠不止位置。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

跟蹤軟體（stalkerware）泛指在未經裝置持有者知情同意之下，持續回報其位置、訊息、通話與其他私密資訊的程式或服務。與藍牙追蹤器相比，它的侵害範圍大得多：追蹤器只知道您在哪裡，跟蹤軟體還知道您對誰說了什麼。

本報告的三個主要發現：

1. **最普遍的監控途徑可能根本不需要安裝任何程式：**只要取得雲端帳號的密碼，加害者即可透過備份、同步與定位服務持續掌握位置、照片與訊息。此類「帳號層監控」在裝置上不留下任何可掃描的痕跡——**手機掃描結果為陰性，不代表沒有被監控**。
2. **防毒思維抓不到授權濫用：**主流平台的防護以「阻擋惡意程式」為思路，但跟蹤情境中大量的監控是透過合法上架的親子監護、防盜或內建共享功能反向使用達成。程式本身「合法」，問題出在安裝與授權的脅迫脈絡——這是掃描引擎在原理上無從判斷的。
3. **偵測行為本身有風險：**與追蹤器情境根本不同——若手機已被監控，**您在這支手機上所做的任何查證、搜尋與求助，都可能被對方看見**。因此本報告的方法論從「第零原則：改用乾淨裝置」開始，而非直接教您在原機上掃描。

行動建議：若您懷疑手機遭到監控，請勿在該手機上搜尋求助資訊或聯繫協助者；請改用他人裝置或公用裝置。發現監控程式後切勿立即刪除——請先完成證據保全，並先評估移除是否會使加害者察覺而升高危險。

1. 問題陳述

1.1 為什麼是現在

WP-001 的缺口分析指出：若追蹤器偵測結果為陰性，但被害者的行蹤與私密資訊仍持續被掌握，調查範圍應擴及手機上的跟蹤軟體與帳號層監控。本篇即為該預告之專文。

跟蹤軟體並非新事物，但兩項變化使風險樣貌不同於以往：

- **智慧型手機已成為個人生活的完整鏡像**：位置、對話、照片、行事曆、健康資料、金融往來全數集中於一機。控制了手機，等於控制了對一個人生活的全景視野。
- **監控的取得門檻已降至消費級**：無論是訂閱制的商用監控服務，或平台內建的共享與監護功能，操作介面都是為毫無技術背景的一般人設計的。

1.2 台灣的具體情境

《跟蹤騷擾防制法》所規範的行為態樣包含以電子通訊方式掌握行蹤與活動；《刑法》妨害電腦使用罪章與妨害秘密罪章對無故入侵他人電腦設備、無故竊錄他人非公開活動亦有規範。法律工具存在，但與 WP-001 相同的落差再次出現：**中文圈缺乏一份完整的自助偵測與處置指引**。被害者面對的實務問題是：

- 對方總是知道我去過哪裡、和誰說過什麼，但我查不到任何異常，應如何著手？
- 我在手機上安裝了防毒軟體且掃描無異常，是否即代表安全？
- 我發現了監控程式，直接刪除是否即可？

1.3 本報告要回答的問題

1. 監控是如何發生的（威脅模型與三條技術途徑）
2. 如何自行偵測（分層方法論、各層的限制、以及為何不能在原機上進行）
3. 發現監控後之處置（證據保全、人身安全、法律途徑、重建乾淨環境）

---

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、監視行蹤與人際往來	**最大宗**：具備長期實體接觸機會，且經常知道或能取得解鎖密碼
分手／離婚糾紛當事人	蒐證、持續掌控	關係存續期間建立的帳號存取往往在分手後仍然有效
家庭內監控	以關心為名的控制	使用親子監護工具監控成年或近成年家庭成員
職場監控逾越	管理之名的越界	公司裝置或 MDM 權限被用於工作範圍外的監控

本報告主要針對第一類與第二類，因為它們同時具備**最高的存取機會**與**最嚴重的人身後果**。

2.2 能力假設

與 WP-001 相同，**攻擊者的技術能力假設為零**。攻擊者不需要撰寫程式，也不需要理解作業系統。他需要的只是下列**任一**項：

- 一次拿到解鎖狀態手機的機會（或知道解鎖密碼）；
- 知道您的雲端帳號密碼（或能通過其密碼重設流程）；
- 曾經以「幫您設定手機」之名義經手過裝置。

在親密關係中，這三項幾乎是日常。**知道伴侶的解鎖密碼在多數關係中被視為信任的表現——威脅模型必須承認這個社會現實**，而不是假設密碼保密。

2.3 被害者處境

- **資訊全面失守**：不同於追蹤器僅洩漏位置，手機監控可及於訊息內容、通話、相簿與瀏覽紀錄。
- **查證管道被監控**：被害者最自然的反應是「以手機搜尋因應方式」——而那支手機正是被監控的裝置。
- **無從區分同意與脅迫**：在控制型關係中，「自願」交出密碼、「自願」安裝定位 App 可能是在壓力下發生的。技術機制看到的是一次合法授權，看不到授權背後的脅迫。
- **裝置與帳號可能同時失守**：加害者可能同時掌握手機、雲端帳號與電子信箱。任何單點的清理（例如只改一組密碼）都可能立即被其他失守點察覺並復原。

---

3. 技術背景：監控的三條途徑

理解途徑分類是本報告方法論的基礎，因為**三條途徑的偵測位置完全不同**：有的要查裝置，有的要查帳號，查錯位置就會得到虛假的安全感。

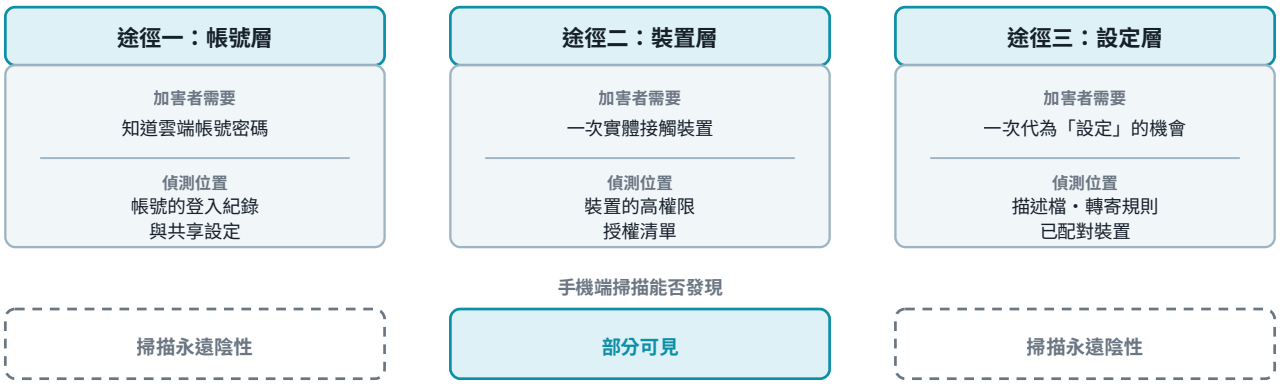

圖 1：監控的三條途徑與各自的偵測位置

3.1 途徑一：帳號層監控（無須在裝置上安裝任何東西）

只要知道雲端帳號的密碼，加害者即可從自己的裝置登入，取得該帳號同步的一切：定位（尋找裝置功能）、照片、備份內容、通訊錄、行事曆，視平台而定亦可能包含訊息。

這條途徑有三個對加害者極為有利的特性：

- **裝置掃描永遠陰性**：手機上沒有任何額外程式；
- **持續有效**：只要密碼不變、登入工作階段不被登出，存取就持續存在；
- **來源難以察覺**：多數人不會定期檢查帳號的登入裝置清單。

此外，平台內建的**位置共享**與**家人共享**功能，若在關係存續期間開啟而在關係惡化後未關閉，效果等同於一條被遺忘的監控通道。

3.2 途徑二：裝置層監控（需要一次實體接觸）

即在手機上安裝監控程式。兩大平台的樣貌不同：

- **Android**：允許自商店以外來源安裝應用程式。監控程式安裝後，典型作法是請求**無障礙服務**（accessibility service）與**裝置管理員**等高權限——這些機制原為輔助功能與企業管理設計，被反向用於讀取畫面內容、攔截通知與防止移除。安裝後程式多會隱藏圖示或偽裝為系統元件。
- **iOS**：未經越獄的裝置難以側載具持續性的監控程式，因此 iOS 情境的監控多改走途徑一（帳號層）或途徑三（設定層）。經越獄的裝置則與 Android 的暴露程度相當，而越獄本身通常會留下可供辨識的痕跡：出現非官方商店的安裝介面、系統更新持續失敗、或裝置行為與同型號他機明顯不同。

裝置層監控的程式又可分為兩類，其法律與偵測處境截然不同：

類別	取得方式	偵測處境
雙用途程式	官方商店合法上架，名義為親子監護、裝置防盜、員工管理	**主流**：程式本身合法，掃描引擎無正當理由標記
專用監控套件	側載安裝，明示或暗示用於監看伴侶	較易被安全產品標記，但安裝後會主動隱藏

本報告刻意不列出任何監控產品的名稱、來源與安裝方式。該類資訊對加害者的助益遠大於對被害者：被害者需要的是「如何在自己的裝置上發現異常」，而非「市面上有哪些產品」。此一取捨依循本團隊《研究倫理準則》中關於攻擊性細節的處理原則。

3.3 途徑三：設定層與周邊裝置（不是程式，因此不會被當成程式看待）

第三條途徑既不是帳號密碼外洩，也不是安裝程式，而是**利用裝置本身的正當設定機制**。它最容易被忽略，因為每一項設定單獨看都是合理功能：

- **管理描述檔與工作設定檔**：原為企業管理裝置而設計的機制，一旦被安裝，可及於流量導向、應用程式派送與部分使用紀錄。以「幫您把手機設定好」為名義完成安裝，在關係中並不突兀。
- **訊息與通話的轉發規則**：於電子郵件設定自動轉寄、於電信服務設定通話轉接、或將簡訊同步至另一部裝置。此類設定一旦建立，即使更換手機也持續有效。
- **已配對的周邊裝置**：手錶、車載系統、耳機、平板。配對關係常在關係惡化後仍然存在，而車載系統尤其值得注意——它同時掌握位置歷程與通訊錄。
- **桌面端與瀏覽器的同步**：手機訊息同步至共用電腦、瀏覽器帳號同步書籤與密碼，皆可能形成一條不經過手機的旁路。

- **平台內建的共享功能**：位置共享、家人群組、相簿共享。這些功能設計時的假設是雙方持續同意，但**沒有任何機制會在關係改變時提醒您重新確認**。

3.4 三條途徑的比較

三者的關鍵差異不在技術複雜度，而在**應該去哪裡查**：

	途徑一：帳號層	途徑二：裝置層	途徑三：設定層
是否需要實體接觸	否	是	多數需要
手機掃描能否發現	**否**	部分可	**否**
偵測位置	帳號的登入與共享設定	裝置的權限與程式清單	裝置設定與外部服務規則
移除方式	撤銷工作階段並更換憑證	移除程式並撤銷高權限	逐項檢視並刪除設定
更換手機是否有效	**否**（帳號未處理則跟著移轉）	是	**否**（多數規則在裝置之外）

最後一列是實務上最常見的誤解：**換一支新手機並不會解除帳號層與設定層的監控**。若僅更換裝置而未處理帳號，新裝置在登入的當下即再度暴露。

---

4. 現行防護機制與其缺口

4.1 現行機制的基本邏輯

兩大平台目前的防護，大致沿三條線發展：

1. **程式來源管制**：官方商店的上架審查，以及對非商店來源安裝的警告與限制。
2. **權限的可見化**：高風險權限改為明示授權，並在使用敏感感測器時提供指示。近年並增加了權限使用紀錄的回顧介面。
3. **帳號活動通知**：新裝置登入時寄送通知、提供已登入裝置的清單。

這三條線對「陌生人植入惡意程式」的威脅模型是有效的。問題在於，本報告的威脅模型並非陌生人。

4.2 缺口分析

缺口一：帳號層監控不在任何掃描的視野內

安全產品掃描的是裝置上的檔案與程式。當加害者是以正確的密碼、從自己的裝置登入時，裝置端不存在任何可疑物件。**這不是掃描引擎不夠好，而是查錯了位置。**對被害者而言，其後果是最危險的一種：一份陰性的掃描報告，換來一個錯誤的安全結論。

缺口二：雙用途程式的判定困境

一款監護程式的功能清單，與一款監控程式幾乎完全相同。差別不在程式做了什麼，而在**裝置持有者是否知情且自願**——這是程式碼之外的事實，掃描引擎在原理上無從判斷。廠商若一律標記，將誤傷正當使用；若一律不標記，則放行了跟蹤情境中的主力工具。

缺口三：授權的脅迫脈絡技術上不可見

系統看到的是一次合法的授權：畫面出現、使用者按下同意。系統看不到的是按下同意時，另一個人正站在旁邊。**在控制型關係中，「自願」是一個技術層無法驗證的概念。**

缺口四：告警的收件人可能是加害者

若手機的門號、帳單或家庭群組由加害者掌握，則安全通知、登入提醒與訂閱明細會送到加害者手上。更根本的情況是：裝置本身即為加害者所購買與設定。**此時所有以「通知使用者」為設計前提的防護，其保護對象都反轉了。**

缺口五：防護設計假設「發現即應移除」

現行的安全提示幾乎一律建議立即移除可疑程式。在陌生人威脅模型下這是正確的；在親密關係暴力情境下，突然中斷的資料回報等同於向加害者宣告「對方已經察覺」，可能直接觸發報復。**偵測與移除之間，需要一個現行機制完全沒有提供的中介步驟：安全評估與證據保全。**

缺口六：關係中的裝置信任鏈

由對方購買、設定或「幫忙處理過」的裝置，其信任鏈自始即不完整。目前沒有任何機制能讓使用者事後確認「這支手機在交到我手上之前被做過什麼」。二手裝置與贈與裝置在此一意義上是同一個問題。

---

5. 自我偵測方法論

圖 2：偵測方法論——第零原則與四層檢查

第零原則：先取得一部乾淨裝置

這是本報告與 WP-001 最大的差異，也是唯一不可跳過的步驟。

在追蹤器情境中，被害者的手機通常是可信的工具；在跟蹤軟體情境中，那支手機本身即為調查對象。若監控存在，則您在該裝置上的每一次搜尋、每一則求助訊息、每一通電話，都可能即時呈現在加害者面前——**包含您正在閱讀本報告這件事**。

因此：

- 使用他人的裝置、公用電腦，或一部與您所有既有帳號皆無關聯的裝置；
- 在該乾淨裝置上，**請勿登入**任何您原有的帳號（登入即可能觸發登入通知，反而暴露）；
- 若必須在原手機上維持日常行為以避免引起懷疑，請保持其使用樣態與過去一致。

以下四層檢查，第一層與第三層應於乾淨裝置上進行，第二層必須在受檢手機上操作，屬於風險最高的一層。

第一層：帳號稽核（於乾淨裝置進行，風險最低）

帳號層是最普遍也最常被略過的一層。請逐項檢視：

- **已登入的裝置清單**：是否有您不認得的裝置或地點？請留意名稱貌似合理但實際上並非您所有的項目。
- **位置共享與家人群組**：目前有誰能看到您的位置？共享是何時開啟的？
- **郵件的自動轉寄與過濾規則**：是否存在您未曾建立的轉寄規則？此為最常見且最持久的旁路之一。
- **帳號的救援管道**：救援電子郵件與救援電話號碼是否仍為對方所有？**若救援管道未清理，更換密碼的效果可能在數分鐘內被撤銷。**
- **雙因素驗證的設定**：第二因素是否綁定在對方能取得的裝置或號碼上？
- **應用程式專用密碼與已授權的第三方應用**：是否存在您不記得授權過的項目？
- **備份設定**：備份的目的地帳號是否確實為您本人所有？

第二層：裝置檢查（於受檢手機操作，風險最高）

請先閱讀第 6.1 節再進行本層。本層的所有操作都可能被監控程式記錄。

裝置層監控為求持續運作，必須取得少數幾類高權限，因此檢查的重點不是「找出可疑的圖示」，而是**逐一檢視這幾份權限清單，確認每一個項目您都認得**：

- **無障礙服務的授權清單**：此為讀取畫面內容與模擬操作的關鍵權限，正當用途的程式數量極少。
- **通知存取的授權清單**：取得此權限即可讀取所有應用程式的通知內容，包含訊息預覽。
- **裝置管理員或裝置擁有者權限**：取得此權限的程式無法以一般方式移除。
- **管理描述檔與工作設定檔**：您未曾任職的公司或您不認得的組織名稱，皆屬異常。
- **非官方來源安裝的授權**：哪些應用程式被允許安裝其他應用程式？
- **電池與行動數據的用量排行**：持續於背景回傳資料的程式，會在這兩份清單上留下痕跡，即使其圖示已隱藏。
- **已配對的藍牙裝置與已知的無線網路**：是否有不屬於您的項目？

若您在上述任一清單中發現不認得的項目，請**記錄其完整名稱後停止操作**，直接進入第 6 章。

第三層：行為面交叉比對（於乾淨裝置進行，最容易被低估）

技術檢查為陰性時，本層往往是唯一能夠推進的方法。作法是把「對方知道的事」逐一列出，並回推**該項資訊的可能來源**：

- 對方知道的是**位置**，或是**對話內容**？前者可能來自途徑一或追蹤器，後者則指向裝置層或通知存取。
- 對方知道的是**已寄出的訊息**，或**尚未寄出的草稿**？後者的來源範圍極窄。
- 對方掌握的資訊是**即時**，或**延遲數小時**？後者較符合定期同步或備份的模式。
- 對方是否知道**只出現在特定一部裝置**上的事？此可直接縮小範圍至該裝置。

實務上，這份清單常能在無須任何工具的情況下，將調查範圍縮小到單一途徑。請以書面記錄每一次事件的日期、對方所知的具體內容，以及您當時所在之處——此份紀錄同時也是第 6.2 節的證據基礎。

第四層：專業鑑識（何時應停止自行處理）

出現下列任一情形時，請停止自行檢查並尋求專業協助：

- 您已在裝置上發現高權限的不明程式，且該情形涉及人身安全的立即風險；
- 監控疑似來自具技術能力的加害者，或涉及工作用裝置與企業管理權限；
- 您需要的是**可用於法律程序的證據**，而非僅止於解除監控；
- 您已多次清理但監控狀態反覆恢復——此通常代表尚有未被發現的持久化管道。

自行操作與鑑識取證之間存在難以兼顧之處：任何清理動作都會破壞現場。若法律途徑對您而言重要，**保存優先於清除**。

6. 發現監控後之處置

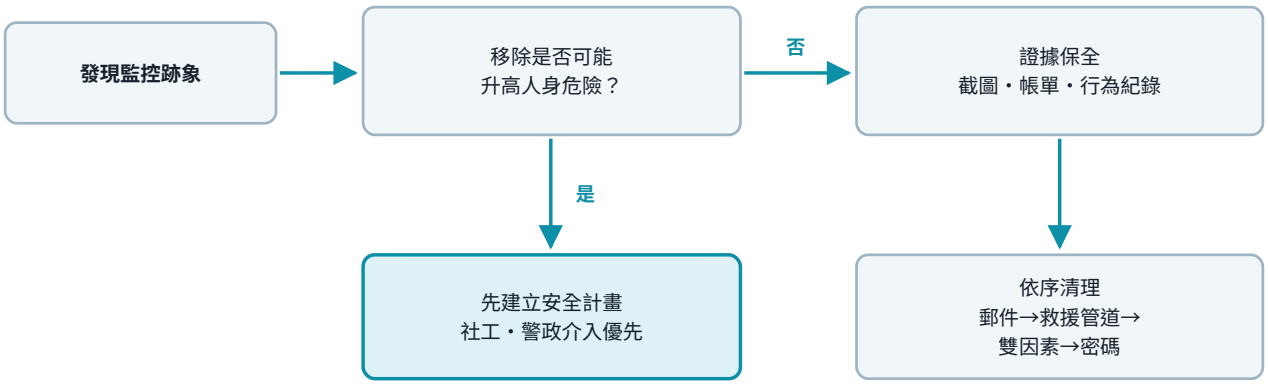

圖 3：發現監控後的處置流程

6.1 第一優先：人身安全

跟蹤軟體情境與追蹤器情境在此處的差異最為關鍵：**移除監控是一個會被對方立即察覺的動作。**

資料回報中斷、程式消失、帳號被登出——這些對加害者而言都是明確的信號，代表被害者已經察覺並開始行動。在親密關係暴力的研究中，被害者採取抵抗或準備離開的階段，正是危險程度最高的階段。

因此，在移除之前，請先確認：

- 您是否已有可執行的安全計畫（安全的去處、可聯繫的人、必要的證件與財物）？
- 移除之後，若對方立即到場或聯繫，您將如何應對？
- 是否有專業的社工或警政管道已經介入？

若答案為否，合理的選擇是暫時維持現狀，先建立支援，再處理技術層面。監控令人難以忍受，但技術上的清理無法保障人身安全，順序不可顛倒。

若您正處於立即危險，請撥打 110；若需要保護服務與諮詢，請撥打 113。

6.2 證據保全

在移除之前完成下列紀錄。所有紀錄請儲存於**受檢裝置之外**：

- 對可疑程式或設定的畫面截圖，含其完整名稱與授權狀態；
- 帳號登入紀錄的截圖，含裝置名稱、時間與地點；
- 訂閱與帳單紀錄——商用監控服務需要付費，金流是最有力的證據之一；
- 第三層所建立的行為對照紀錄（日期、對方所知內容、您的實際行蹤）；
- 若可能，請他人以另一部裝置**拍攝您操作受檢裝置的過程**，以佐證截圖並非事後製作。

請勿刪除可疑程式、請勿重置裝置、請勿更換手機，直到證據保全完成為止。重置是最徹底的清除，也是最徹底的證據銷毀。

6.3 台灣的法律途徑

- **《跟蹤騷擾防制法》**：其規範的行為態樣包含以電子通訊、網際網路或其他設備對特定人持續進行監視、追蹤或掌握行蹤。被害者得向警察機關報案，經調查後得對加害人核發書面告誡；書面告誡後二年內再犯者，得聲請保護令。
- **《刑法》妨害電腦使用罪章**：無故入侵他人電腦或其相關設備、無故取得或變更他人電磁紀錄，以及製作專供犯本章之罪的程式，均設有處罰規定。
- **《刑法》妨害秘密罪章**：無故以錄音、照相、錄影或電磁紀錄竊錄他人非公開之活動、言論、談話或身體隱私部位，設有處罰規定。
- **《個人資料保護法》**：非法蒐集、處理或利用個人資料並足生損害於他人者，設有相關責任。
- **《家庭暴力防治法》**：若雙方具有家庭成員或親密關係伴侶關係，得聲請保護令，其款項包含禁止對被害人為騷擾、跟蹤等行為。

報案時建議前往**婦幼警察隊**或於報案時明確說明涉及跟蹤騷擾與家庭暴力，以便由熟悉此類案件的單位承辦。攜帶第 6.2 節所保全的證據，並保留原始裝置。

6.4 重建乾淨環境的順序

順序錯誤是清理失敗最常見的原因。**若在帳號救援管道仍為對方掌握的情況下更換密碼，新密碼可能於數分鐘內被重設。**建議依下列順序進行：

1. **於乾淨裝置上，先處理電子郵件帳號**：它是所有其他帳號的救援出口，必須最先奪回。
2. **清理救援管道**：移除不屬於您的救援電子郵件與電話號碼。
3. **重設雙因素驗證**：改綁至僅您本人持有的裝置，並重新產生備用碼。
4. **更換密碼並撤銷所有工作階段**：撤銷登入是關鍵動作——僅更換密碼，既有的登入狀態在部分服務上仍可能持續有效。
5. **依序處理其他帳號**：雲端、社群、金融、電信服務。
6. **清理設定層**：轉寄規則、通話轉接、位置共享、家人群組、已配對裝置、管理描述檔。
7. **最後才處理受檢裝置本身**：於證據保全完成後，將裝置回復為原廠設定，並且**切勿自舊備份還原**——舊備份可能含有監控設定。請以手動方式重新設定。
8. **檢視所有其他裝置**：平板、電腦、車載系統、智慧家庭裝置。

完成後，請於數週內重新執行第一層帳號稽核。**監控狀態的復發，通常代表清單上仍有一項未被發現的管道。**

---

7. 給廠商與政策制定者的建議

1. **將帳號層納入安全檢查的單一入口**：目前使用者必須橫跨多個設定畫面才能完成一次完整稽核。單一入口應涵蓋已登入裝置、位置共享、轉寄規則、救援管道與第三方授權，並可一鍵撤銷。
2. **共享關係應設有效期與定期再確認**：位置共享與家人群組不應永久有效而無任何回顧提示。定期的再確認能使「被遺忘的共享」自然失效。

3. **雙用途程式的常駐揭露**：具備持續回報位置或內容能力的程式，無論其上架分類為何，皆應在被監控裝置上維持不可關閉的常駐指示。監護的正當用途不因被監護者知情而受損。
4. **重新設計「發現後」的引導**：安全提示不應一律建議立即移除。應提供「這可能是親密關係監控」的分支，引導至證據保全與求助資源，而非直接提供移除按鈕。
5. **通知的收件人應可獨立設定**：安全通知不應僅送往帳單持有人或家庭群組管理者。
6. **裝置交付狀態的可驗證性**：應提供機制，使使用者能確認一部裝置自原廠或自上次重置以來，被安裝了哪些管理描述檔與高權限程式。
7. **政策面**：跟蹤騷擾與家庭暴力案件的第一線受理人員，需要具備數位監控的基本識讀能力；被害者取證的協助管道，亦應納入數位證據的處理。

---

8. 研究限制與後續工作

8.1 本版本的限制

- 本版本為綜整與方法論研究，**未包含本團隊之自有實測數據**。
- 平台的具體行為隨作業系統版本與地區設定而變動，本報告刻意避免記載會迅速過時的具體數值與版本編號。
- 本報告不點名特定廠商產品，亦不記載監控程式的取得與安裝方式，此為刻意的取捨（見第 3.2 節）。
- 本報告的法律敘述以台灣現行法規為範圍，且不構成法律意見。

8.2 規劃中的實測（v2.0）

本團隊規劃以對照實驗量測各層偵測方法的實際有效性，設計要點如下：

- **受測裝置**：本團隊自有之測試裝置，涵蓋兩大平台的多個版本。
- **對照組設計**：分別以途徑一、途徑二、途徑三建立監控狀態，並以未受監控之裝置為對照。
- **量測項目**：各層檢查的偵測率與偽陰性率、平台安全通知的實際觸發情形、以及清理程序的完整性驗證（清理後監控是否確實中斷）。
- **倫理限制**：**受測者僅限本團隊成員本人，或經書面同意之參與者**。不涉及任何未同意之第三人，不使用任何真實被害者的裝置或資料。實驗所使用的監控樣本不對外散布。

本設計依循本團隊《研究倫理準則》，於實驗開始前公開，以便外界檢驗。

8.3 我們希望收到的回饋

- 本報告的方法論在實務上是否可行？特別是第零原則對於缺乏第二部裝置的被害者是否過於嚴苛？
- 第一線的社工、警政與法律實務工作者，對第 6 章的處置順序有何修正意見？
- 各層檢查是否有本報告未涵蓋的持久化管道？
- 翻譯版本的用語是否符合當地實務？

回饋請寄至 security@odysec.org（敏感內容請以 PGP 加密）。

附錄 A：偵測檢查表

第零原則 - ☐ 已取得一部與自身帳號無關聯的乾淨裝置 - ☐ 未在該乾淨裝置上登入既有帳號 - ☐ 未於受檢手機上搜尋求助資訊

第一層：帳號稽核 - ☐ 已登入裝置清單逐項確認 - ☐ 位置共享與家人群組逐項確認 - ☐ 郵件自動轉寄與過濾規則逐項確認 - ☐ 救援電子郵件與救援電話號碼確認為本人所有 - ☐ 雙因素驗證綁定於本人持有之裝置 - ☐ 第三方應用程式授權逐項確認 - ☐ 備份目的地帳號確認為本人所有

第二層：裝置檢查 - ☐ 無障礙服務授權清單 - ☐ 通知存取授權清單 - ☐ 裝置管理員或裝置擁有者權限 - ☐ 管理描述檔與工作設定檔 - ☐ 允許安裝其他應用程式的來源清單 - ☐ 電池與行動數據用量排行 - ☐ 已配對藍牙裝置與已知無線網路

第三層：行為面交叉比對 - ☐ 已列出對方所知之具體事項 - ☐ 已區分位置類與內容類資訊 - ☐ 已判斷資訊為即時或延遲 - ☐ 已記錄日期、內容與自身行蹤

若發現監控 - ☐ **請勿立即刪除，請勿重置裝置** - ☐ 已評估移除是否會升高人身危險 - ☐ 已完成截圖與帳號紀錄之保全（存於受檢裝置之外） - ☐ 已保存訂閱與帳單紀錄 - ☐ 已攜帶證據至婦幼警察隊報案 - ☐ 清理依「郵件→救援管道→雙因素→密碼與工作階段→其他帳號→設定層→裝置」之順序進行 - ☐ 未自舊備份還原 - ☐ 已於數週後重新執行第一層稽核

附錄 B：名詞對照

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

附錄 C：資料來源

本報告依據下列類型的公開資料撰寫：兩大行動平台廠商的官方支援文件與隱私說明、反跟蹤軟體聯盟（Coalition Against Stalkerware）及其參與組織所公開的資料與實務指引、學術界關於親密關係監控與跟蹤軟體的已發表研究，以及台灣《跟蹤騷擾防制法》、《刑法》、《個人資料保護法》、《家庭暴力防治法》之條文。

平台機制的具體行為請以其官方文件之當下版本為準。本報告與 WP-001《無聲的跟隨》互為姊妹篇，兩者的威脅模型與方法論架構一致。

授權：本報告以創用 CC 姓名標示 4.0（CC BY 4.0）釋出，歡迎轉載與翻譯，請註明出處。

引用格式：Odysec（2026）。《口袋裡的告密者：手機跟蹤軟體的偵測與應對》。Odysec 研究報告 WP-002，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；保護服務與諮詢專線為 113。