

COSCUP TAIWAN 2026

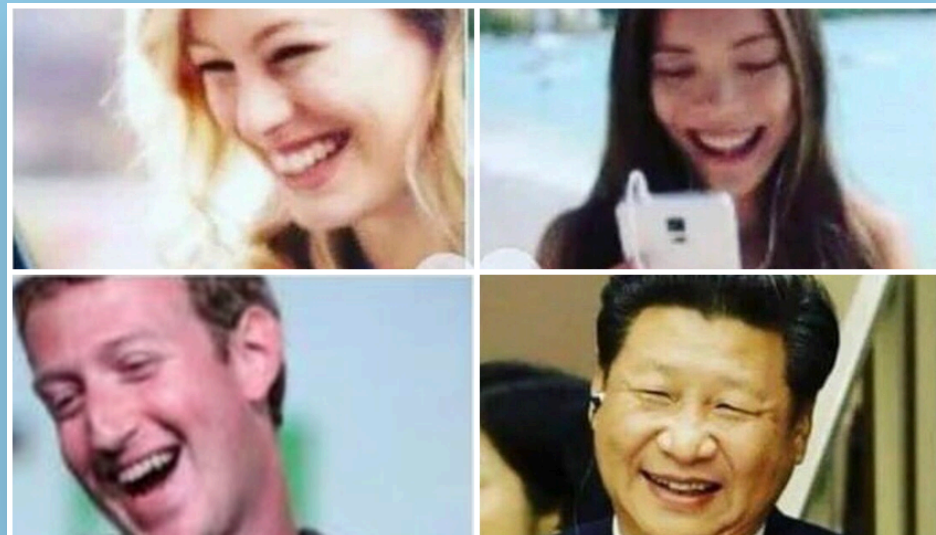
隱私指南 2026

從風險判斷，到更有隱私的數位生活

— matheme.Justyn

09.AUG.2026 | 臺科大 TR-510 @ 臺北

匿名網路社群議程軌 | COSCUP Taiwan 2026



你以為只是在使用服務；科技巨頭與政府也可能正在監視你。

今天用同一條主線，做四件事

01

第一章 | 先釐清你現在的生活情境

從正在做的事、接觸的資料與可能傷害，決定需要多強的保護。

02

第二章 | 讓日常工具更保護你

把風險轉成服務、裝置、帳號與部署選擇。

03

第三章 | 公開內容會出賣你

照片、影片與帳號，可能被拼回你的身分、地點與關係。

04

第四章 | 留下做得到的行動

保留參與與求助能力，完成一個 15 分鐘改善。



同一條主線 | 先釐清 → 再選型 → 再反查 → 最後行動

你平常是如何在網路上保護你的生活隱私的？

先憑直覺舉手，再掃碼看網站能看見什麼。

A | 我是 nobody，不需要

B | 我開無痕模式

C | 我用 VPN

D | 我用兩支手機



掃碼查看
手打備援網址
[coscup-privacy-form-demo
.matheme-justyn.workers.dev](https://coscup-privacy-form-demo.matheme-justyn.workers.dev)

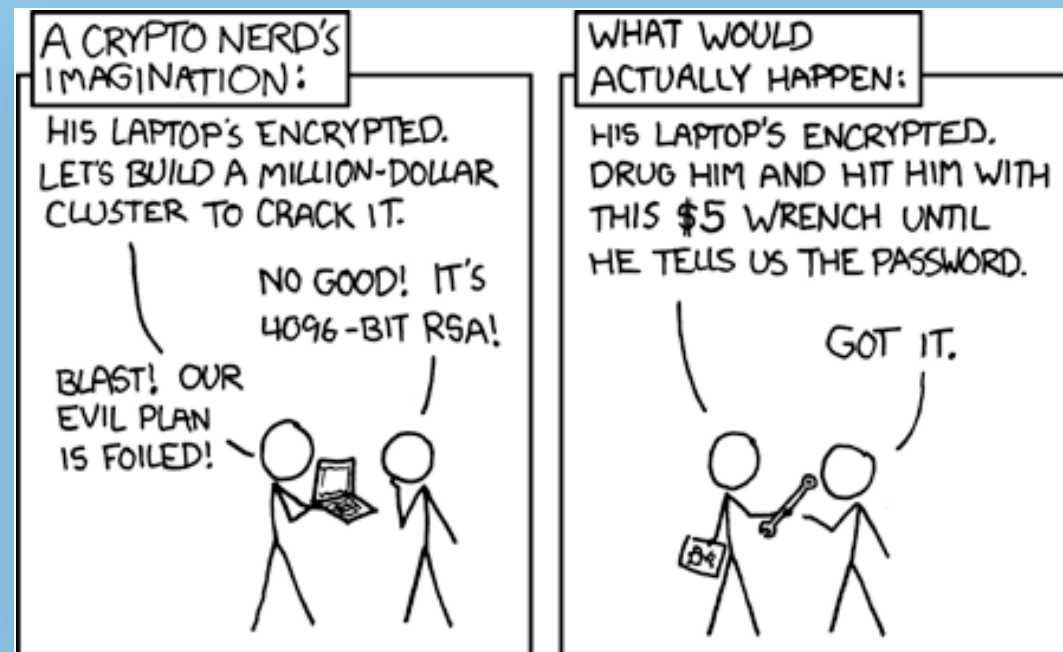


只回顯、不建立問卷資料庫。第 0／1 級不用登入；第 2 級 Google 登入完全自願。網站不要求相機、麥克風或定位權限。

01

第一章 | 先釐清你現在的生活情境

先看你正在做什麼、想保護誰；再看資料、行動者與傷害，決定做得到的控制。



加密很強，不代表對手會照你預想的方式出招。

旅遊不會抹掉職務、關係與價值



新聞圖卡，非案發照片；圖卡中的單週 10 人失聯與法官案是不同群組。

個案 | 2026年4月，一名法官赴中國旅遊
3名公安進入下榻旅館；案件於7月9日報導
2024至2026年6月，共30人通報遭留置或盤查
其中14人是公務員

美國 | 機密資訊會依洩漏後果分成三個等級
部分涉密人員即使私人出國，也要事前申報

臺灣 | 一般民眾赴中港澳，沒有普遍適用的事前申報
特定公務或涉密人員赴中，可能要先取得許可
政府人員赴港澳，也要在出發前通報

高風險者 | 這裡指數位安全風險，不是職業標籤
NCSC：記者、倡議者等因工作接觸敏感資訊
NGO工作者若符合相同條件，也可能屬高風險者
Freedom House：2025年共126起跨國鎮壓
其中49起拘留、48起非法遣返

出發前
先安裝並實測兩條通訊路徑。
能連線 ≠ 當地允許或不會要求交付。
換 SIM ≠ 換 IMEI；帳號與裝置也要分艙。

圖片 文獻 Pulse HK News. (2026, July 9). 赴中國風險再響警號：一周內10台灣人前往中國後失聯 [Instagram post]. Instagram. <https://www.instagram.com/p/DakborziPZa/>

陳國維. (2026, July 9). 陸委會警示：本週10名國人赴陸失聯、法官旅遊遭盤問. 中央廣播電臺. <https://www.rti.org.tw/news?uid=3&pid=219422>
法務部. (n.d.). 臺灣地區與大陸地區人民關係條例§9. 全國法規資料庫. Retrieved August 4, 2026, from <https://law.moj.gov.tw/.../Q0010001&Ino=9>
National Cyber Security Centre. (2023, December 7). Guidance for high-risk individuals on protecting your accounts and devices. <https://www.ncsc.gov.uk/.../guidance-for-high-risk-individuals>

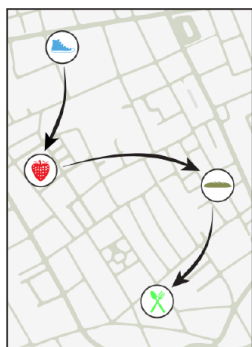
National Archives and Records Administration. (2009, December 29). The President Executive Order 13526. <https://www.archives.gov/isoo/policy-documents/cnsi-ee.html>
法務部. (n.d.). 國家機密保護法. 全國法規資料庫. Retrieved August 4, 2026, from <https://law.moj.gov.tw/.../I0060003>
Gorokhovskaia, Y., & Vaughan, G. (2026, April 16). Collaboration and resistance: Tracking transnational repression in 2025. Freedom House. <https://freedomhouse.org/.../tracking-transnational-repression-2025>

Defense Counterintelligence and Security Agency. (n.d.). SEAD 3 unofficial foreign travel reporting. <https://www.dcsa.mil/.../SEAD-3-Unofficial-Foreign-Travel-Reporting/>
大陸委員會. (2025, September 11). 行政院核定修正「行政院及所屬機關（構）人員赴香港或澳門注意事項」. https://www.mac.gov.tw/News_Content.aspx?...1BEFE3EF152C5479
anoni.net. (2026). 出差與研討會的數位準備. anoni.net

少量日常足跡，比直覺更容易指向同一個人

4 個時間 + 商店 → **90%** 軌跡唯一化

2015 研究 | 110 萬人、3 個月信用卡資料；這是特定資料集的結果。



shop	user_id	time	price	price_bin
	7abc1a23	09/23	\$97.30	\$49 – \$146
	7abc1a23	09/23	\$15.13	\$5 – \$16
	3092fc10	09/23	\$43.78	\$16 – \$49
	7abc1a23	09/23	\$4.33	\$2 – \$5
	4c7af72a	09/23	\$12.29	\$5 – \$16
	89c0829c	09/24	\$3.66	\$2 – \$5
	7abc1a23	09/24	\$35.81	\$16 – \$49

唯一化不等於已知姓名；但只要外部線索對上，其餘交易就可能一起被接回。

2019 犯案 | 2026 最高法院判決

沒有姓名，也能從「誰當時在場」反向找人

維吉尼亞州持槍搶案一度無嫌疑人線索。令狀要求查詢案發地 150 公尺內、前後各 30 分鐘出現的裝置。

19 個匿名



9 個軌跡



3 個具名



Chatrie

經後續偵查，Chatrie 保留上訴權後認罪：判監 141 個月、出獄後監督 3 年。

2026-06-29 | 最高法院以 6-3 認定此次位置資料取得構成 `search`，發回審查是否合理；未宣告所有 geofence warrant 一律無效。

數位足跡的可識別度比直覺高；App / SaaS 日常服務資料生態系，正在替平台累積可被數位巨頭、資料商與國家級行為者利用的識別索引。

資料被串聯並拿來行動，監視才變成傷害



對手不一定先入侵；也可能取得或購買位置、通聯、付款與社群資料。

匿名服務不只保護內容；還要問資料能否被接回真人，並被拿來採取行動。

看得到 | RFC 6973

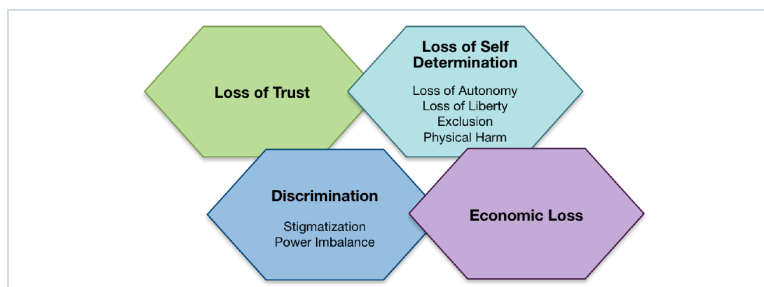
平台、端點、制度與市場
可見內容、識別子與詮釋
資料。

接得回 | LINDDUN

→ 偵測存在、串聯帳號、識
別真人並推論關係。

動得了 | 能力／權力

→ 限制、盤問、跟蹤、差別
待遇，或傷害第三人。



NIST 圖不是流程圖：它分類資料處理可能造成的四類個人問題。

失去信任

失去自主／自由

歧視／權力不平衡

經濟損失

切斷鏈的三個目標 | 資料用法可預期、個人可管理、非必要時活動可解離。

匿名服務要防整條識別鏈，不只加密內容；傷害也可能沿關係圖擴散到家人、消息來源與組織。

風險不是身分標籤：情境會改變處理強度



同一個人的手機，既是生活工具，也可能連到消息來源與敏感工作。

Alice | 虛構綜合人物

平常：聊天、地圖、搭車、行動支付與社群。

工作：人權與新聞採訪；接觸個案、消息來源、未刊稿與跨境合作。

她多數時候仍是普通使用者；只有敏感工作連到第三人，或出現具體威脅、扣押與迫切出境時，眼前情境才升高。		
四列是 Alice 的不同情境，不是四種人。		
本簡報自訂四級：可忽視／低／中／高；不是國際組織的官方分級。		
可忽視	日常生活 聊天、地圖、搭車與支付	帳號、更新與裝置鎖定基線
低	公開曝光 真名報導、活動與社群	公私分開；清查住址與位置
中	敏感工作 來源、未刊稿、人權個案	分艙、按需知悉、演練與支援
高	事件狀態 威脅、扣押、迫切出境	先保人；找法律與數位安全支援

中／高再跑 OPSEC：關鍵資訊與可觀察徵候 → 威脅 → 弱點 → 風險 → 對策

近兩年，隱私指南更重視情境與對抗



anoni.net | 臺灣語境

用威脅模型分流日常、敏感與跨境工作；補多重身分、AI 與緊急求助。



Privacy Guides | 產品與部署

從工具清單擴到情境、政策、資料邊界、自架責任與退出能力。



PSE | 新技術與攻防

以開源研究檢查私密身分、通訊、證明與 AI 時代的新攻擊面。



攻擊方法變快，指引也必須同步更新。

三個社群是輸入，不是答案；本簡報再用「任務 → 可見資料 → 串聯 → 傷害 → 控制」做臺灣情境裁決。

02

第二章 | 讓日常工具更保護你

帶著第一章的情境與傷害選服務，再補底座、部署與遷移；最後帶走情境速查。

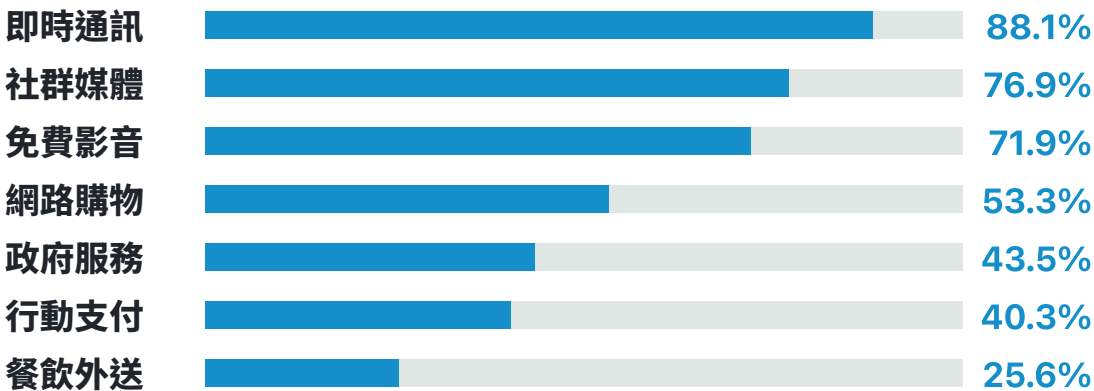


每天用的 App，不只提供功能，也決定資料往哪裡流。

先定義好服務，再比較常用產品

TWNIC 發布、典通執行電訪

2025-07-28 至 09-01 | 最近三個月使用服務



TWNIC 七類是調查入口；本章整成九個選型頁，並非一一對應。

通訊

即時通訊：誰能解密？
Email：哪些服務商能讀信？

社交與內容

社群：觸及、功能與可串聯資料
影音：觀看如何接回長期身分

交易與實名

叫車／外送／購物：後台累積多少生活規律
政府／支付：一次任務交出多少資料

工作

文件：誰握解密金鑰
個人 AI：能讀哪些私人來源

瀏覽與搜尋

同一供應商能否跨站接回你

服務使用率，不是手機安裝率；題目與樣本框不同，只看量級。

本章只停一次、20 秒：你是否因功能、同伴或成本選了別的 App？

好的通訊軟體，應預設只讓對話參與者解密

Q: So how do you encrypt data?

We support two layers of secure encryption. **Server-client encryption** is used in Cloud Chats (private and group chats), Secret Chats use an additional layer of **client-client encryption**. All data, regardless of type, is encrypted in the same way — be it text, media or files.

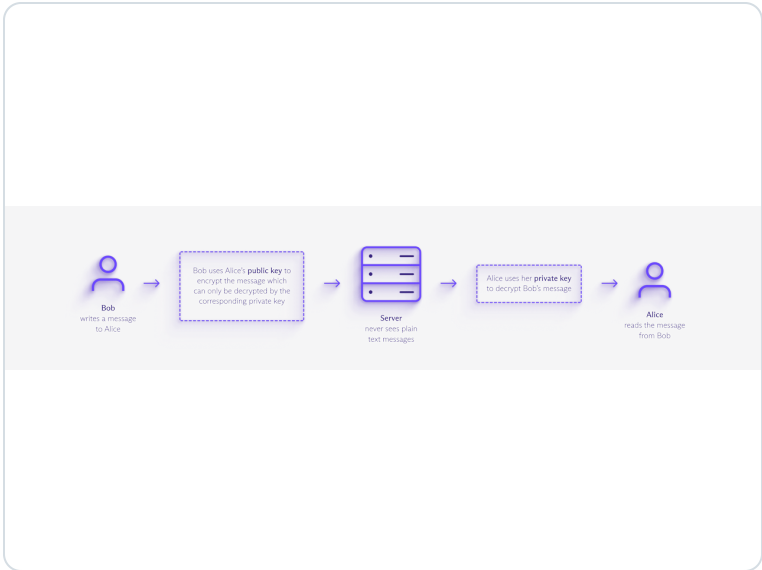
官方說明：一般 Cloud Chats 不是端對端加密；只有 1 對 1 Secret Chat 才是。

隱私主指標

完成對話時，參與者以外還有誰能解密？
再查備份、Bot、橋接與新裝置。

方案	優點／缺點	適用情境
★ 多數人起點 Signal	優點： 預設端對端加密。 缺點： 對方也要使用。	適用於： 敏感私訊與小群組。
組織／進階 Matrix／ Element	優點： 開放協定、可自架。 缺點： 復原與維運較難。	適用於： 有維運負責人的組織。
主流聯絡 LINE／ WhatsApp／ Messenger	優點： 聯絡人多。 缺點： 備份、Bot、客服可能擴大收件人。	適用於： 日常聯絡。
公開／低敏感 Telegram／ Slack／Discord ／WeChat	優點： 社群與協作功能成熟。 缺點： 一般文字非端對端加密；WeChat 另有內容監測與管轄風險。	適用於： 公告與低敏感協作。

Email 先問：服務商能不能讀信



Proton 彼此寄送可端對端加密；寄到外部信箱預設仍是 TLS，主旨也不加密。

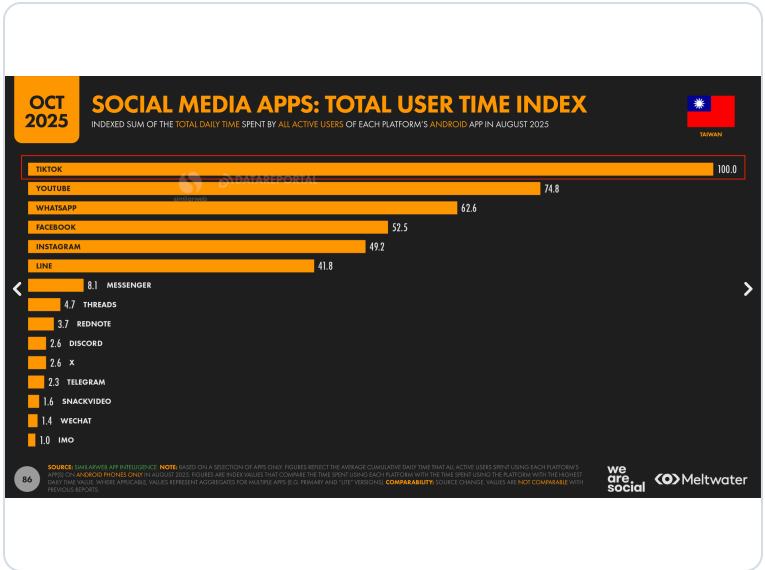
隱私主指標

寄收件人以外，哪些郵件服務商能取得明文？
跨服務、備份、搜尋與管理員分開查。

方案	優點／缺點	適用情境
★多數人起點 Proton Mail	優點：同服務預設端對端加密。 缺點：寄外部預設仍是 TLS。	適用於：願意讓敏感聯絡人也用 Proton。
主流相容 Gmail／Outlook	優點：互通與復原成熟。 缺點：服務商可讀一般信件。	適用於：低敏感、廣泛互通的一般信件。
敏感小圈 Tuta Mail	優點：同服務端對端加密。 缺點：跨服務要另交換密碼。	適用於：固定合作人與敏感往來。
開放進階 Thunderbird + OpenPGP	優點：私鑰可留本機。 缺點：雙方都要管金鑰。	適用於：已有 OpenPGP 流程的進階使用者。

只換 Email App，不會自動改變伺服器可見性。

社群平台：一起權衡觸及、功能與隱私



臺灣 Android 使用時間指數；不是月活躍人數或隱私分數。

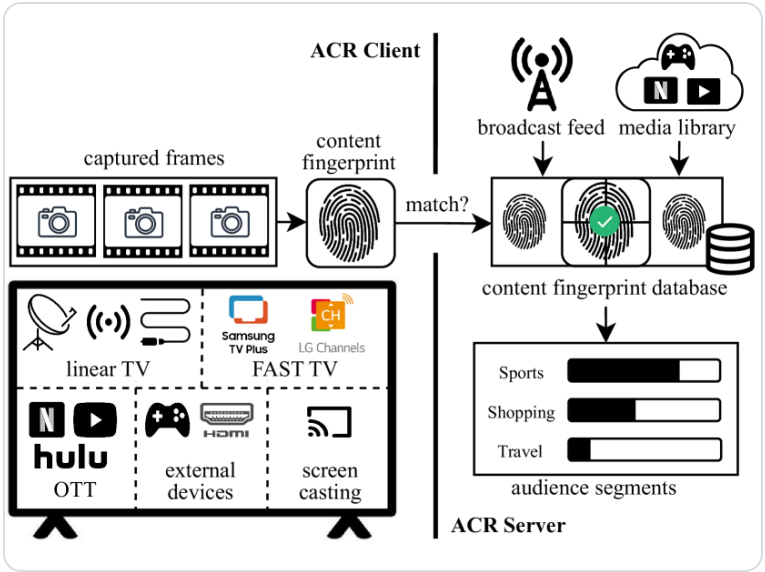
隱私主指標

平台能把幾類資料串回同一身分？
先比觸及與功能，再查輪廓、匯出與搬家。

方案	優點／缺點	適用情境
主流觸及 Facebook／Instagram／Threads	優點：臺灣觸及完整。 缺點：跨產品資料集中。	適用於：需要既有受眾。
高黏著影音社群 TikTok／X／Reddit	優點：話題與發現強。 缺點：行為輪廓密集。	適用於：願意接受平台輪廓換取觸及。
開放協定 Bluesky	優點：可攜身分與開放協定。 缺點：生態與治理仍在變動。	適用於：想降低單一平台鎖定。
社群自治 Mastodon	優點：可選社群規則與伺服器。 缺點：管理者仍可見部分資料。	適用於：小型社群與可承擔管理責任者。

沒有全能冠軍：先選受眾與功能，再用廣告偏好、資料匯出檢查平台已如何描述你。

影音服務先看：觀看紀錄會不會接回長期身分



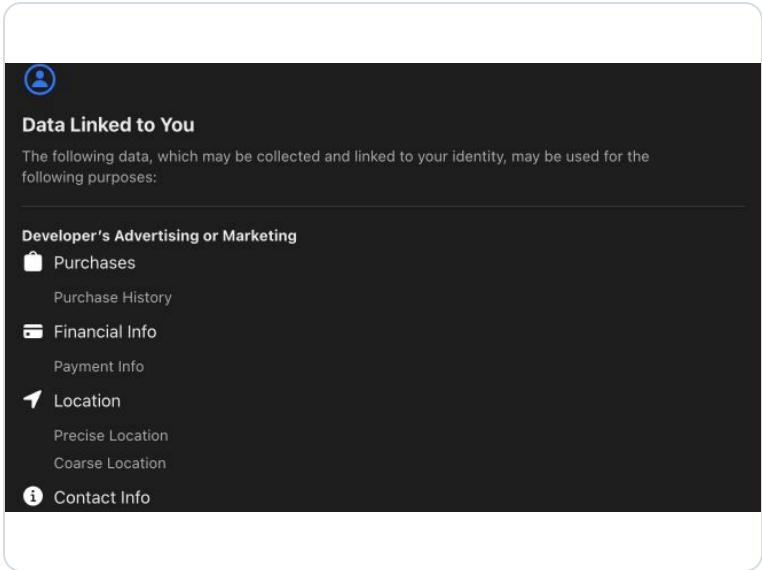
ACR 可比對畫面並形成觀看輪廓；特定實測不能外推所有裝置。

隱私主指標
一次觀看有幾層能接回長期身分或家庭？
逐層查帳號、平台與播放裝置。

方案	優點／缺點	適用情境
★多數人起點 YouTube 訪客／獨立設定檔	優點：內容完整。 缺點：登入會接回 Google 身分。	適用於：單支訪客；訂閱再分設定檔。
短影音 TikTok／Shorts／Reels	優點：發現內容快。 缺點：密集行為形成輪廓。	適用於：低敏感娛樂，不混用敏感搜尋。
地區內容庫 動畫瘋／Bilibili／愛奇藝／ABEMA／TVer	優點：特定地區內容。 缺點：政策與地區不同。	適用於：內容需求明確時逐服務查。
少留帳號 FreeTube／NewPipe／PeerTube	優點：可減少平台帳號連結。 缺點：功能與穩定性有折衷。	適用於：願意接受功能折衷者。

智慧電視與串流盒要分別關閉 ACR；訪客瀏覽也不會抹掉裝置層。

叫車、外送、購物：便利也累積規律



App Store 標籤顯示 Uber 申報多類資料可連結身分；不是外洩證明。

隱私主指標

同一後台能串聯多少次路線、門牌、品項與付款？
先比保障，再看保存與刪除。

方案	優點／缺點	適用情境
叫車平台 Uber／LINE GO／55688	優點：媒合與客服完整。 缺點：累積精準移動規律。	適用於：需要即時媒合。
外送平台 Uber Eats／foodpanda	優點：店家與退款集中。 缺點：住址、餐點與作息合流。	適用於：需要規模與爭議處理。
大型購物平台 momo／PChome／蝦皮	優點：退貨與防詐成熟。 缺點：交易與收件關係集中。	適用於：高頻購物與需要保障者。
少集中路徑 商家官網／LINE 官方帳號／CoopCycle	優點：可少一層大型平台。 缺點：資安、退款與規模要逐店查。	適用於：可信商家／合作社。

平台不是原罪；先保留消費保障，再刪永久地址、卡片與不必要定位。

實名服務，也只交這次需要的資料



掃店家收款碼與出示自己的付款碼是兩條不同路徑；付款憑證若被截取，風險也不同。

隱私主指標

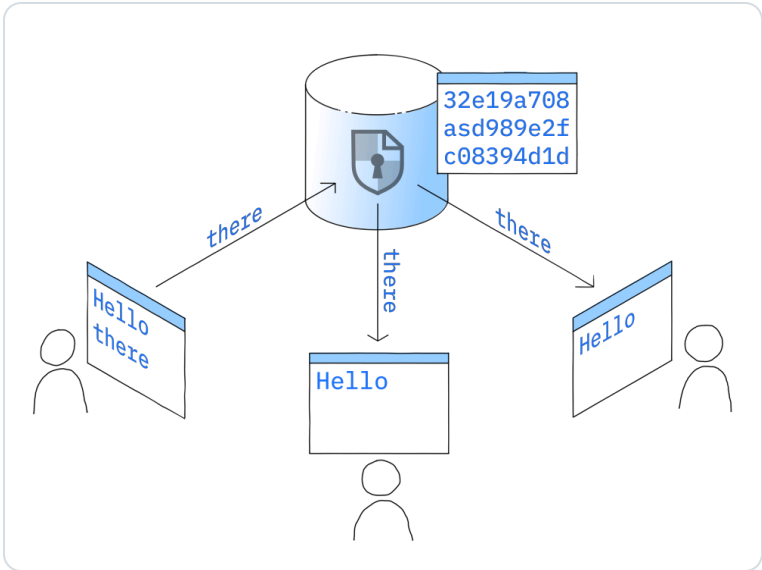
完成一次辦事或付款，要交出多少可重用資料？

分開看「證明身分」與「付款」；查最小揭露、驗證、爭議與撤銷。

方案	優點／缺點	適用情境
證明身分 數位憑證皮夾	優點： 可只出示特定屬性。 缺點： 支援場景仍在擴張。	適用於： 需要線上證明資格或身分。
通關必要服務 EZ WAY	優點： 進口實名委任集中。 缺點： 身分、物流與報關會合流。	適用於： 跨境網購；只給這次任務所需資料。
公共支付路徑 台灣 Pay	優點： 串接金融機構、通路廣。 缺點： 仍留下銀行與交易紀錄。	適用於： 想用銀行帳戶或金融卡付款者。
商業支付 LINE Pay／街口／全支付	優點： 通路、優惠與退款方便。 缺點： 帳號、裝置與消費輪廓集中。	適用於： 重視便利並會管理通知與限額者。

實名不等於整包交付：一次任務只交必要屬性，付款碼不要任人拍走。

文件協作先問：誰握有解密內容的金鑰？



端對端加密把內容金鑰留給參與者；分享連結與端點仍要管理。

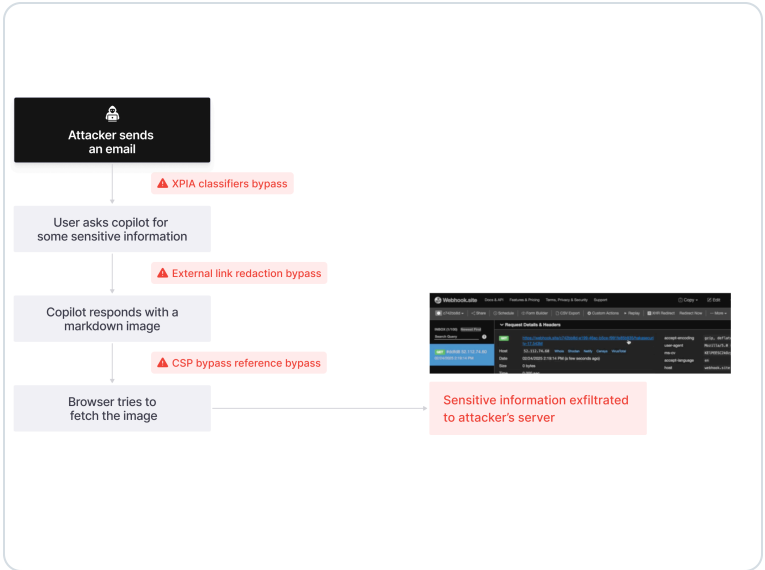
隱私主指標

協作參與者以外，多少角色能解密文件？
查服務商、管理員、外掛與備份。

方案	優點／缺點	適用情境
主流協作 Google Workspace ／Microsoft 365	優點： 同編與復原成熟。 缺點： 服務商與管理員可讀內容。	適用於： 一般團隊與低敏感文件。
★多數人起點 CryptPad	優點： 端對端加密協作。 缺點： 功能與相容性較少。	適用於： 敏感小組、可接受功能折衷。
組織控制 Nextcloud+ Collabora	優點： 可代管或自架。 缺點： 維運責任增加。	適用於： 有治理與資料落點需求的組織。
完全本機 LibreOffice + 加密交付	優點： 內容可不上協作雲。 缺點： 版本衝突與金鑰交換要自行處理。	適用於： 不需同編的敏感文件。

先決定誰能解密，再談即時同編、搜尋與便利。

個人 AI：先看它能讀什麼



已修補的 EchoLeak 顯示：外部內容可能經連接服務碰到私人資料；這不是所有 AI 常態。

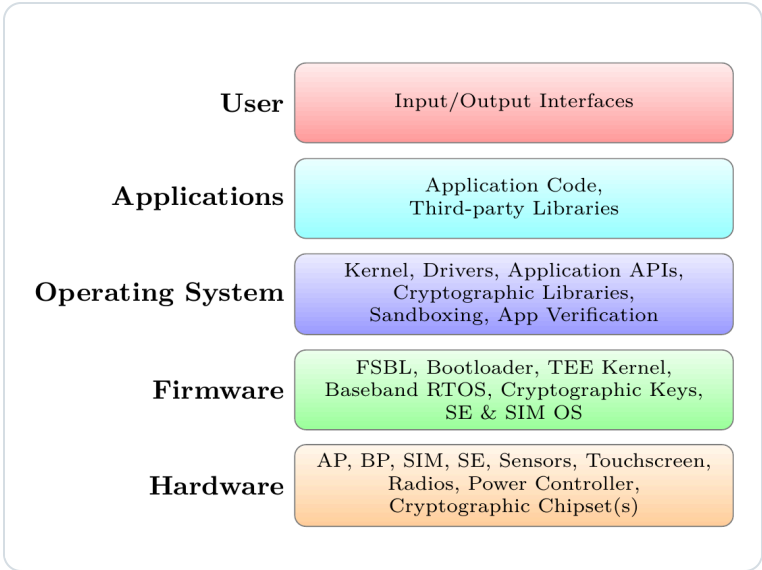
隱私主指標

AI 能讀到多少你沒主動貼上的私人來源？
查記憶、附件、檢索增強、連接服務與人工審閱。

方案	優點／缺點	適用情境
主流功能 ChatGPT Claude Gemini Copilot	優點：能力完整。 缺點：政策與連接範圍各異。	適用於：低敏感、可重建工作。
★多數人起點 Duck.ai	優點：降低帳號連結。 缺點：功能與模型選擇較少。	適用於：一般查詢不接主帳號。
隱私政策較強 Proton Lumo	優點：主打不以對話訓練。 缺點：能力與生態仍較小。	適用於：重視供應商資料政策的日常使用。
完全本機 Ollama／LM Studio	優點：原始資料可留裝置。 缺點：硬體、模型與更新自己負責。	適用於：離線草稿／摘要。

舉手 20 秒 你是否因功能、同伴或成本，選了不是隱私最強的 App？

選裝置是在選生態系，不是在比誰最新



裝置風險跨越 App、OS、韌體與硬體，也連到帳號、雲端與備份。

隱私主指標

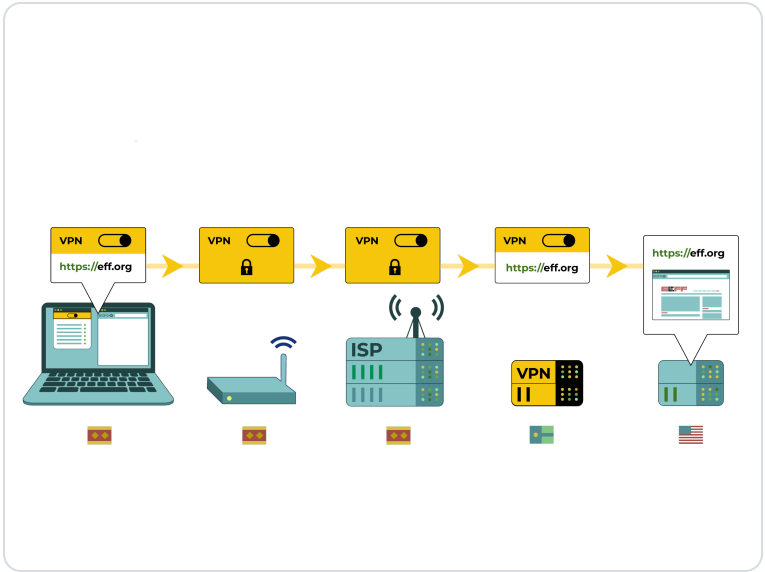
遺失、帳號接管或 App 越權時，能否止血並復原？

安全支援只回答還會不會修；它是門檻，不是總分。

方案	優點／缺點	適用情境
★ 多數人起點 仍受支援的 iPhone/iPad	優點：鎖定與復原整合。 缺點：帳號與 iCloud 集中。	適用於：重視事故後復原者。
Android 起點 仍受支援的 Pixel	優點：更新政策清楚。 缺點：Google 帳號集中。	適用於：偏好 Android 且要長期支援。
高風險技術選項 GrapheneOS+ Pixel	優點：隔離與權限較強。 缺點：相容與復原成本高。	適用於：能自行維護的高風險使用者。
筆電生態系 macOS/ Windows 11/ Ubuntu LTS	優點：依軟體需求選。 缺點：加密、備份、更新分別驗收。	適用於：工作軟體優先者。

最新不等於安全；先看能不能鎖、撤、復原與退出。

無痕、VPN、Tor：比較的是信任交給誰



VPN 把本地網路的可見性轉移給業者；不會自動匿名。

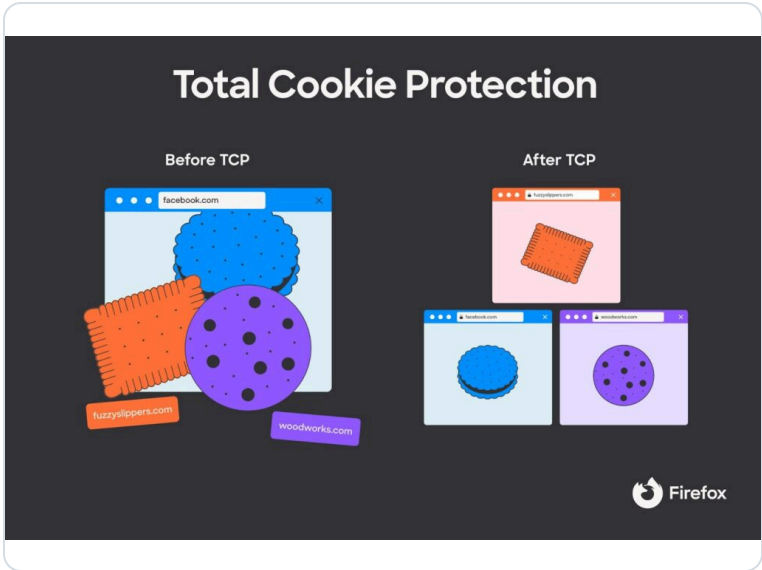
隱私主指標

哪一方能同時知道來源身分與目的地？
先分清只少留本機紀錄、防本地觀察、需要匿名，或組織內網存取。

方案	優點／缺點	適用情境
一般上網 一般連線＋ 私密瀏覽	優點：不用多交一個 VPN 業者。 缺點：網站、電信與帳號仍看得到。	適用於：一般上網與少留本機紀錄。
防本地網路 觀察 Mullvad／ Proton VPN	優點：隧道遮住本地 Wi-Fi 的目的地。 缺點：信任轉移到 VPN 業者。	適用於：不可信網路或想隱藏 IP。
匿名任務 Tor Browser	優點：分散來源與目的地觀察。 缺點：較慢，登入真名仍會接回。	適用於：需要降低可連結性的匿名瀏覽。
組織內網 公司／自架 VPN	優點：可控內網入口與稽核。 缺點：組織管理者就是觀察者。	適用於：存取內部系統，不當匿名工具。

不要先問哪家 VPN；先問你要防哪個觀察者。

瀏覽與搜尋，先看能否跨站接回你



Firefox 分隔各網站的第三方 Cookie；登入帳號與裝置訊號仍要另處理。

隱私主指標

同一供應商能否串起網站、搜尋與帳號活動？查跨站追蹤、同步、搜尋與登入。

方案	優點／缺點	適用情境
主流便利 Chrome+ Google	優點：相容與同步完整。 缺點：網站、搜尋、帳號合流。	適用於：便利優先者。
★多數人起點 Firefox+ DuckDuckGo	優點：隔離 Cookie；搜尋免登入。 缺點：仍有指紋與網站登入。	適用於：想減少跨站串聯者。
整合阻擋 Brave+ Brave Search	優點：預設阻擋追蹤。 缺點：部分網站需調整。	適用於：願意接受較積極阻擋者。
匿名任務 Tor Browser + DuckDuckGo	優點：降低 IP／指紋連結。 缺點：較慢；登入真名會破功。	適用於：確有匿名需求的特定任務。

密碼管理先避免重複使用，再守住復原路徑



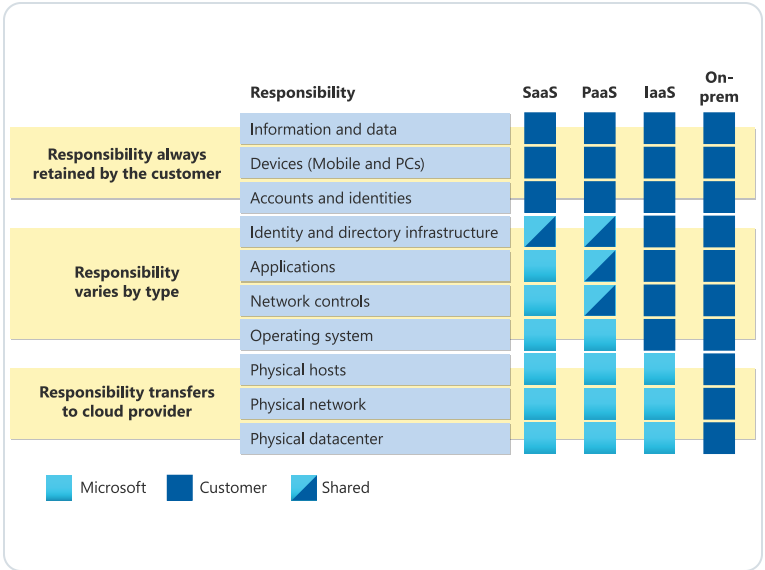
每個帳號要用不同鑰匙，但不必全靠人腦保管。

隱私主指標
外洩一站，還能登入幾個其他帳號？
目標是 0；先處理 Email、密碼庫與金融帳號。

方案	優點／缺點	適用情境
★ 多數人起點 通行密鑰／FIDO2 安全金鑰	優點： 抗網路釣魚。 缺點： 受服務支援與復原設計限制。	適用於： 已支援通行密鑰的重要帳號。
通行密鑰未支援 1Password／Bitwarden	優點： 每站自動產生唯一密碼。 缺點： 主密碼與復原成為集中責任。	適用於： 多數仍使用密碼的網站與 App。
本機控制 KeePassXC	優點： 密碼庫留在本機。 缺點： 同步與備份自己負責。	適用於： 重視本地控制且能自行管理備份。
沒有管理器 長密語＋安全紙本	優點： 不依賴特定 App。 缺點： 只適合少量帳號。	適用於： 緊急備援；不要再用同一密碼走天下。

復原也是第二登入入口：復原 Email、備援碼與舊裝置不要落在同一個失效點。

要不要自架？先算控制需求、責任與成本



從 SaaS 到地端，控制增加，修補、備份與事件責任也回到你。

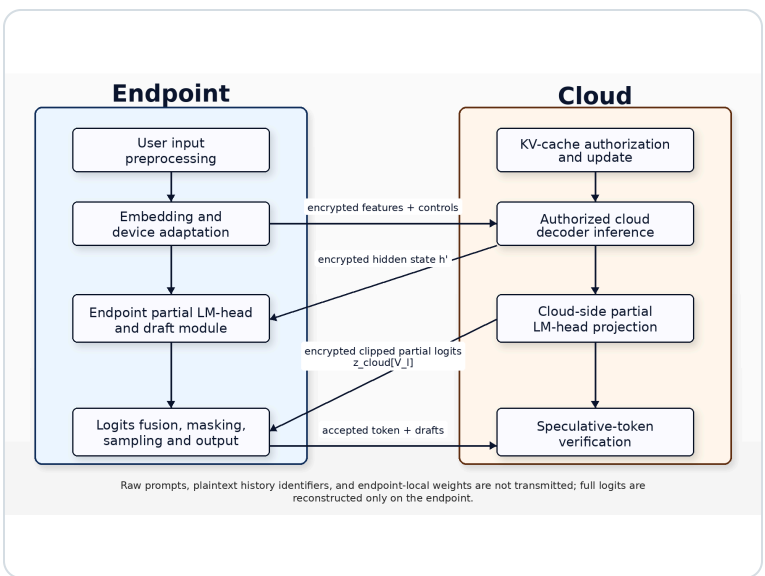
隱私主指標

需要控制什麼？誰能長期維運並完成還原？
比較資料邊界、固定維運、變動成本與事故尾端。

方案	優點／缺點	適用情境
★多數組織起點成熟 SaaS	優點：按人／用量付費，供應商維運。 缺點：受服務商政策限制。	適用於：沒有專職維運者。
受管代管受管 Nextcloud／單一租戶	優點：可選地區與較多控制。 缺點：契約與退出仍要治理。	適用於：要控落點但不想全自架。
IaaS 自架 Hetzner／AWS／GCP VPS	優點：系統路徑可自訂。 缺點：修補、憑證、備份、值班全接手。	適用於：有長期維運負責人與還原演練。
地端自架 Proxmox／自有主機	優點：可完全不上公有雲。 缺點：硬體、網路、電力與災難復原成本最高。	適用於：確實禁止上雲。

沒有長期維運負責人與還原演練，就不要自架；三年總成本要含人力、事故與退出。

AI 部署：資料邊界與維運一起算



端點保留提示詞，雲端只接手授權運算；不是通用保證。

隱私主指標

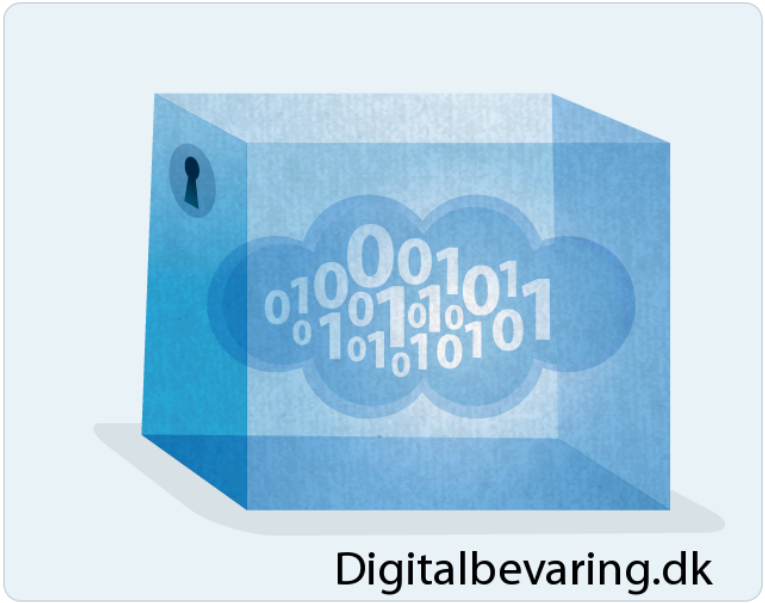
多少敏感資料離開信任邊界？

盤點提示詞、附件、檢索增強（RAG）、連接服務與備份。

方案	優點／缺點	適用情境
一般消費雲端 ChatGPT／Claude／Gemini／Copilot	優點： 能力完整。 缺點： 保存政策各異。	適用於： 低敏感、可重建工作。
★ 多數組織起點 Azure OpenAI／Vertex AI／Bedrock	優點： 契約與地區可治理。 缺點： 檢索資料仍要自己管。	適用於： 需法遵與雲端整合的組織。
完全本機 Ollama／LM Studio	優點： 原始資料可留裝置。 缺點： 硬體、模型與更新自己負責。	適用於： 敏感草稿／離線摘要。
自架／混合 vLLM／TGI+本地去識別	優點： 可自訂資料邊界。 缺點： 認證、GPU、值班全接手。	適用於： 能實測邊界的平台團隊。

本地不必然安全；高風險資料不要交給消費雲端 AI。

個人換一個任務，組織搬一條 workflows



先界定資料、帳號、權限與退路；不是整個數位生活一起搬。

遷移完成標準
新路能完成任務、能復原；舊路不再收到新資料。
朋友不換 App 也沒關係：先只搬一段敏感對話。

共用的是階段目的；個人與團隊不需要有相同步驟數。		
A 界定單位	個人 選一個可回復的低風險任務。	團隊 框出一條 workflows，列入、資料與失敗後果。
B 可回復試行	個人 備份、確認復原，再用低敏感資料完成一次。	團隊 指定負責人；演練加入、撤權、復原與匯出。
C 切換與退場	個人 停新資料，解除電話、信箱與復原綁定。	團隊 舊路唯讀；撤整合與離職帳號，再依義務刪除。
停損： 已發生接管、扣押、跟蹤或人身事件時，先找真人支援，不拿風險等級為「高」的事件試辦。		

第二章帶走：通用基線，再依條件升級

多數人通用基線

帳號

通行密鑰；否則每站唯一密碼。

通訊／Email

Signal；敏感信件進同一加密路徑。

瀏覽／裝置

Firefox＋DuckDuckGo；選可鎖定與復原的生態系。

生活平台

分開帳號個人檔案、最小權限、少存地址與卡片。

匿名／雲端

匿名用 Tor；雲端只放低敏感、可重建資料。

四個條件才升級		
團隊治理	起點 Matrix、Workspace／M365、受管 AI。	責任 撤權、復原與事件演練。
服務商不可解密	起點 CryptPad／Proton／Tuta。	責任 端點、分享、金鑰與備份。
指定地區／不上雲	起點 先代管；真不上雲才用本機。	責任 負責人、還原、事件、三年總成本。
匿名／高風險	起點 Tor＋Signal；按任務分開身分。	責任 先找真人支援。

回收互動

剛才那一次選擇沒有標準答案；今天先搬一個任務。

03

第三章：公開內容會出賣你

俗稱「人肉」：照片、影片、帳號與日常行為，會怎麼被拼成地點、身分與關係。

WHAT THE NUMBER OF DIGITS IN YOUR COORDINATES MEANS	
LAT/LON PRECISION	MEANING
28°N, 80°W	YOU'RE PROBABLY DOING SOMETHING SPACE-RELATED
28.5°N, 80.6°W	YOU'RE POINTING OUT A SPECIFIC CITY
28.52°N, 80.68°W	YOU'RE POINTING OUT A NEIGHBORHOOD
28.523°N, 80.683°W	YOU'RE POINTING OUT A SPECIFIC SUBURBAN CUL-DE-SAC
28.5234°N, 80.6830°W	YOU'RE POINTING TO A PARTICULAR CORNER OF A HOUSE
28.52345°N, 80.68309°W	YOU'RE POINTING TO A SPECIFIC PERSON IN A ROOM, BUT SINCE YOU DIDN'T INCLUDE DATUM INFORMATION, WE CAN'T TELL WHO
28.5234571°N, 80.6830941°W	YOU'RE POINTING TO WALDO ON A PAGE
28.523457182°N, 80.683094159°W	"HEY, CHECK OUT THIS SPECIFIC SAND GRAIN!"
28.523457182818284°N, 80.683094159265358°W	EITHER YOU'RE HANDING OUT RAW FLOATING POINT VARIABLES, OR YOU'VE BUILT A DATABASE TO TRACK INDIVIDUAL ATOMS. IN EITHER CASE, PLEASE STOP.

多種線索接起來，可能一路逼近一個人。

先盤點一段影音會洩漏哪些隱私線索



背對鏡頭的路人，被接成姓名、職業、年收入與敏感描述。虛構介面，不是實測。

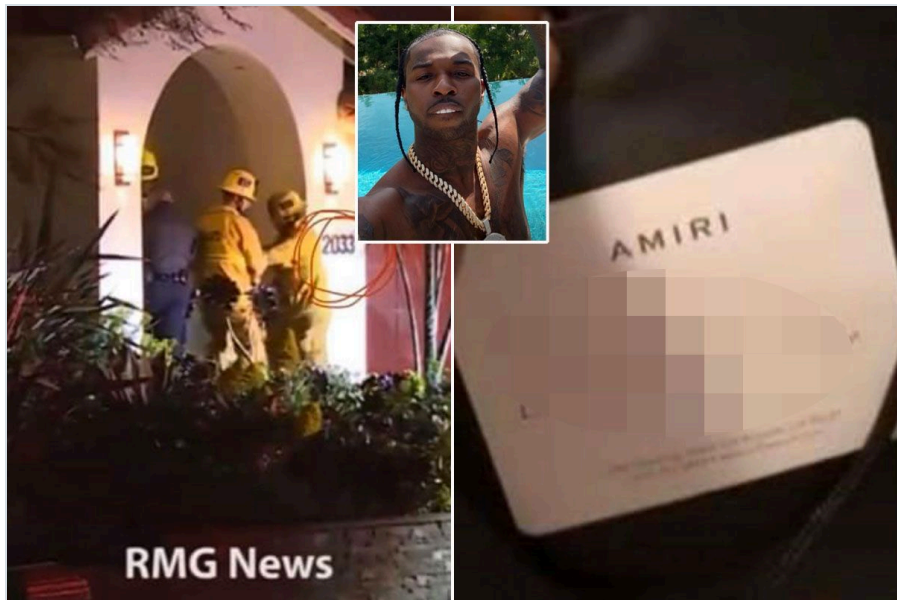
問題不是一張照片自帶全部欄位，而是不同服務與公開內容能否把欄位接起來。

五面不是新模型：它把第一章的可見資料／入口拆成可檢查項；調查最終公開副本＋服務。

A 檔案與平台副本	EXIF、縮圖、字幕、通知、下載檔 → AO
B 畫面與聲音	地址、反光、窗景、陰影、廣播、背景對話 → BA／BC
C 人、關係與帳號	衣物、刺青、假名、同框者、重複影像 → BD
D 地點、時間與規律	即時發布、路線、作息、固定背景、跨平台同步 → BA／BC／AQ
E 基礎設施與生命週期	定位、電信、支付、同步、備份、管理端、AI 連接服務 → AQ／AO

優先順序 | 直接可行動內容 → 跨篇串聯 → 系統副本／後台 → 最後才決定處置

人肉不是魔法：公開線索會把你找出來

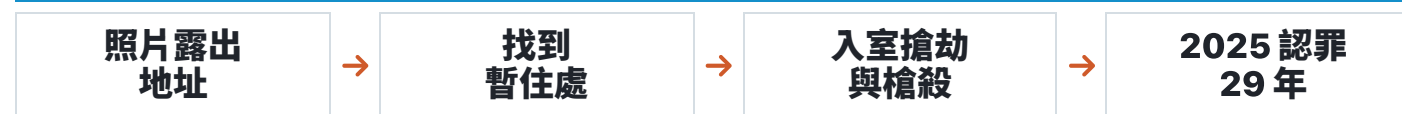


地址已由來源像素化；不顯示真實住址。2020 案件，2025 認罪。

一次地址可能已足夠；更多時候，是公開內容與規律長期累積。

多年公開內容 + 舊帳號 + 固定規律 + 社交關係 + 即時貼文 → 接近成本持續下降

2020-02-19 | 公開照片裡的地址，接成入室搶劫致死案



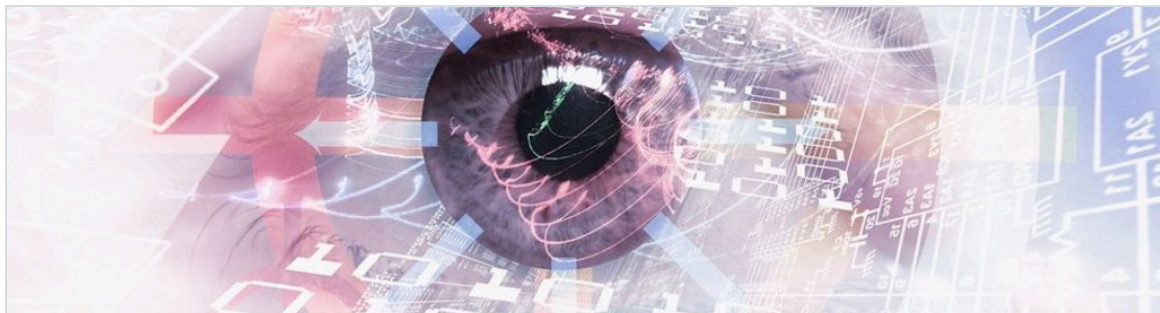
框架位置 | B 畫面／聲音 + D 地點／時間／規律

第一優先 | 先移除地址、證件與即時行程；不能安全重作就不發布。

國家／任務延伸 | 2026 Strava：跑步時間與路線 + 已知人員／任務，可升級成航艦近即時位置；報導未證明造成攻擊。

正確 App 能保護傳輸，不會替你遮掉主動貼出的地址、帳號、關係與下一步。

清掉 EXIF，畫面仍可能把人帶到門口



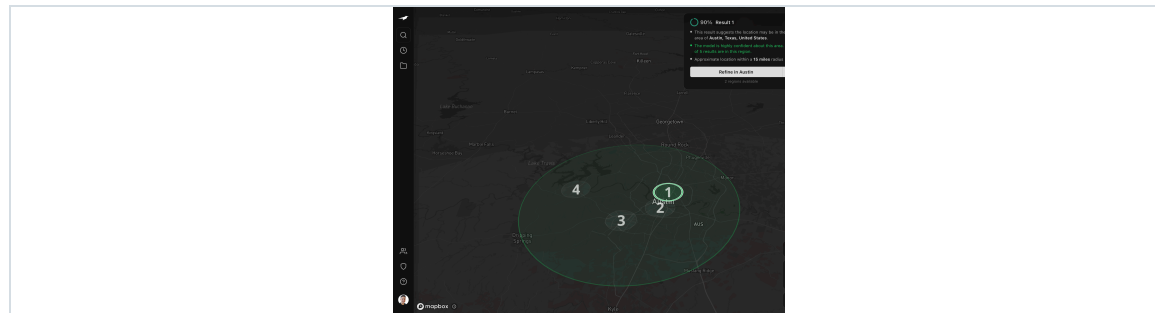
概念圖；不使用受害者照片、真實車站或住址。

2019 刑案 | 傷害已發生

自拍反光，被接到住處

眼中倒影 → 車站候選 → 街景比對 → 等候、尾隨；窗簾與自然光又形成樓層假說。

2020 年判刑 30 個月



官方產品介面截圖；已移除精準座標、地址與結果清單。

2026 Raven | 能力成本下降

單張影像，也能自動提出位置候選

官網宣稱秒級、街道／公尺級；這是廠商宣稱，不是獨立實測。

404 Media：公眾曾可使用；執法機關採購

1 | 觀察



2 | 假說



3 | 交叉驗證



4 | 結論邊界

框架位置 | B 畫面／聲音 + D 地點／時間／規律 **第一優先** | 逐格看最終公開副本，再單獨聽完整聲軌。工具降低提出候選的成本；不會取消誤判。

遮住臉不等於匿名：多張照片會露出互補特徵



起訴材料中的監視與比較影像；不是演算法辨識結果。

2025-02-09 / 03-30 兩起縱火案 | 04-14 聯邦起訴

遮臉
監視畫面



身形／衣物
白盒



白車／筆跡
跨場景物件



搜索扣得
相符物證

2025-08-07 報導：審判排定 2026-09-14；刑事起訴只是指控。官方並列照片不代表臉部辨識命中。

框架位置 | C 人／關係／帳號

第一優先 | 把多張照片、舊帳號、衣物、背景、物件與同框者當成一組檢查。

安全 demo | 只用講者自有／合成小帳號

Maigret

自有假名跨站檢查；同名命中只是候選。

TinEye

裁切、縮放、調色後的相同影像副本仍可能被找到。

DeepFace 本機

只在自有小圖庫比對；結果只是候選。

素人只用自有／合成；公眾人物只用公開來源，不主張知情同意，不碰住址、私人電話、家人、即時位置、金融、醫療。

沒有打卡，位置仍可能被記錄並接回真人



案件被告法院外照片；不使用被害人、車輛或追蹤器藏匿處影像。

2024-06-24 至 07-27 | AirTag 被暗藏在伴侶車輛內



- 留下位置 | 追蹤器、相簿、地圖、穿戴、車機與各種 App。
- 接回真人 | 電話／SIM、付款、交通、Email／單一登入 與主帳號。
- 框架位置 | D 地點／時間／規律＋E 基礎設施／生命週期
- 第一優先 | 一般盤點關閉非必要來源；疑似跟騷／家暴先安全計畫，不一定先關追蹤器。

沒有打卡仍可能留下位置；匿名位置紀錄也可能被識別鏈接回真人。

刪除 App，不等於所有副本都消失



404 Media 案件報導主圖；照片不是案發現場，也沒有顯示真實訊息。

2025-07-04
槍擊與破壞事件

2026-03-13
多項罪名成立

2026-04-22
Apple 修補漏洞

傳入 Signal
訊息



通知
預覽



iOS 留存
副本



刪 App 後
仍可鑑識

不是破解 Signal：解密後的通知副本，沒有跟著 App 與自動消失訊息一起刪除。

框架位置 | A 檔案／平台副本＋E 基礎設施／生命週期

第一優先 | 用自有測試資料逐層驗收通知、縮圖、同步、備份與管理端。

已確認 | iPhone 通知資料庫的傳入訊息。

同類檢查 | 縮圖、同步、備份、收件者與管理員匯出。

新增資料流 | AI：轉錄、瀏覽器／IDE、辦公助理、記憶與 連接服務。

刪除不是按鈕，而是跨層驗收工作。

先保人，再管理影音完整生命週期



迫切事件先找安全方向與真人支援，不要把一般設定清單機械套用。

Gate 0 | 跟騷、家暴、裝置可能受控：先用安全裝置建立可信通道與安全計畫。

1 拍攝前	決定能不能拍；寫清目的、受眾、不可拍人物／空間與可理解的同意。WITNESS
2 公開副本	另做最小副本；清 EXIF 仍不夠，還要處理地址、兒少、聲音、反光與時間／位置。CNIL／eSafety
3 對抗性複核	用 EA 五面地圖檢查最終成品；觀察、假說、交叉驗證與結論邊界分開。Berkeley Protocol
4 發布時	人已離場、任務結束、路線不可攔截、共同發布者完成複核。NCSC
5 發布後	監測標註、轉貼、縮圖、通知、備份、管理端與 AI 連接服務；準備撤下與事件升級。Holistic Security

從傷害反推暴露與控制 | 先保人 → 直接內容 → 跨篇身分／規律 → 系統副本 → 生命週期

04

第四章 | 留下做得到、撐得久的行動

隱私不是退出社會；是保留參與、求助與選擇的能力。



隱私生活不是一個人硬撐；和可信任的人一起練習、求助、調整。

網站看見的訊號，可能被接成傷害

剛才的網站沒有問卷：第 0 級回顯請求資料；第 1 級只在本機算特徵；第 2 級才自願登入；第 3 級只解釋更多授權。

A | nobody：無差別攻擊不必先認識你

B | 無痕：不會刪掉服務與城市後台

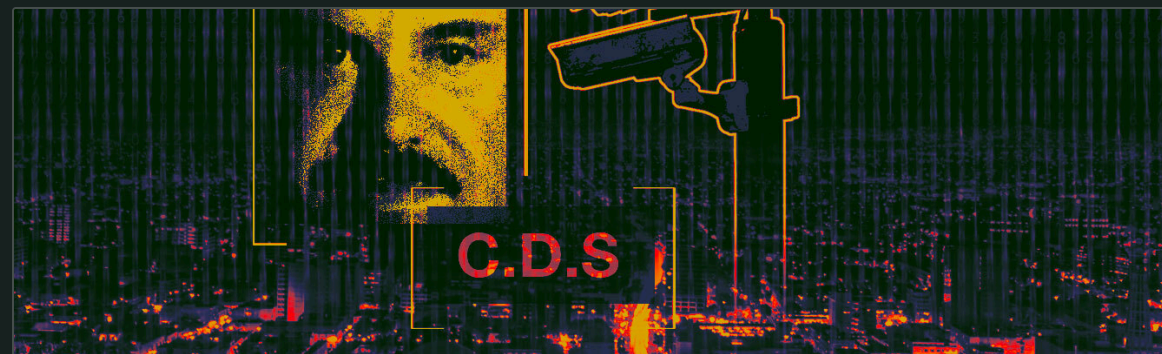
C | VPN：不遮電信位置、帳號與攝影機

D | 雙機：共同行動與復原路徑仍會合流

風險模型決定控制強度；數位足跡決定無差別、陌生或國家級能力對手找到你與關係人的成本。

DOJ OIG 稽核 | 2018 案件・2025 公開

手機資料＋城市攝影機，找到了會面者



通聯／位置 → 城市攝影機 → 會面者 → 威脅／殺害

稽核記載：錫納羅亞販毒集團僱用的駭客取得 FBI 駐墨官員通聯與位置資料，再以城市攝影機辨識會面者。公開報告未說明手機資料取得方法。

編輯合成圖，非案發截圖。

隱私要能參與、能求助、撐得久

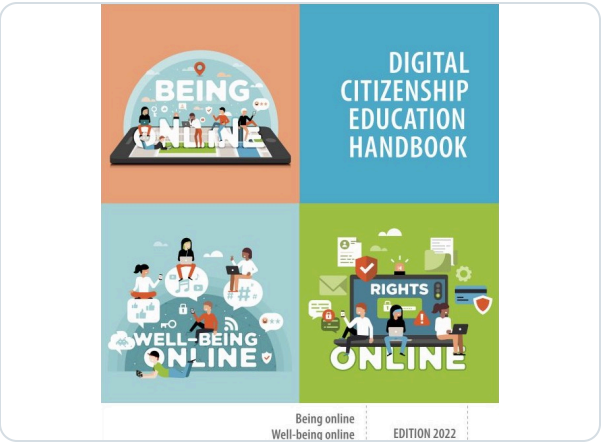


前三章已判斷風險、完成選型並反查；現在驗收：控制本身會不會造成新的傷害？

看得懂	我知道交出了什麼，也能拒絕或撤回嗎？	NIST PRAM+ 歐洲理事會
用得了	我還能工作、上學、使用公共服務嗎？	歐洲理事會：近用與參與
找得到人	可信任的家人、同伴與合作人還聯絡得到我嗎？	歐洲理事會+ Holistic Security
求得到助	出事時，有第二條安全通道和真人嗎？	NCSC+ Access Now
撐得下去	三個月後，我還做得到嗎？	歐洲理事會+ Holistic Security

這五問是本簡報綜合驗收，不是任何單一國際標準的原文。

有一問失敗 | 縮小工作流、更換或減少控制、補上真人支援；不要要求使用者更用力。



歐洲理事會把線上參與、福祉與權利放在同一套數位公民框架。

下一頁壓力測試 | 資料越少越好，為什麼還要讓裝置說得通？

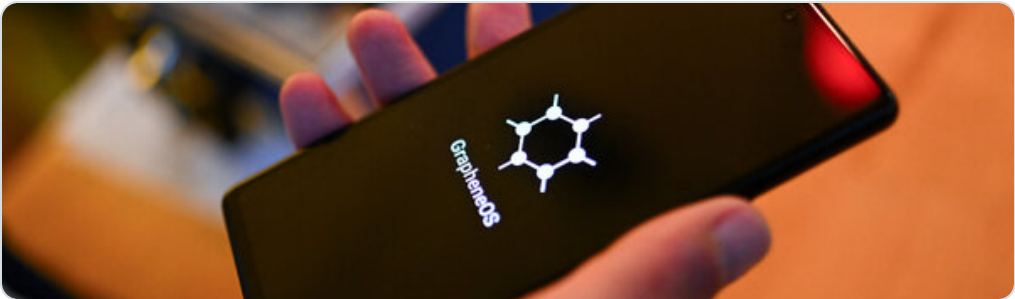
資料越少越穩；高風險盤查還要讓裝置說得通

僅適用確有盤查、扣押或人身脅迫的高風險情境。

最穩起點：真秘密根本不隨身；事前最小化優先於臨場清除。

- 1 不帶 只帶旅程需要的裝置、帳號與檔案。
- 2 合理脈絡 保留真實、無害、旅程必要資料；不要編身分或撒謊。
- 3 可否認 外層只開合理資料；系統紀錄、雲端與備份仍可能拆穿。

情報史只能類比：CIA 的 pocket litter 強調脈絡一致；一般旅客仍以 EFF「不要說謊、只帶必要資料」為界線。



技術示意照，非 Tunick 手機或盤查現場。

Tunick 案 | 檢方指控；被告不認罪



清除功能 ≠ 可否認性：盤查者看見了清除。

VeraCrypt 桌面；相對成熟	Arcanum Android；新、未獨立稽核	Shufflecake Linux；實驗	Flowvault Web／自架；新
----------------------	----------------------------	-------------------------	-----------------------

沒有成熟 SaaS 能完整保證高風險可否認性。

離場前，完成一個 15 分鐘行動

先做一件能驗收的改善；不要一次重做整個數位生活。

可忽視 | 顧帳號

開通行密鑰；否則用密碼管理器。

低 | 少一個入口

刪一個非必要權限或公開位置。

中 | 搬一個任務

朋友不換也沒關係；先搬敏感對話。

高 | 先找真人

停止自行清除；改用可信裝置求助。

依第一章架構找文章

情境與對手

文章 | 威脅模型；日常基線

串聯與識別

文章 | 多個網路身分

可見資料

文章 | 詮釋資料；平台蒐集

行動與傷害

文章 | 跨境；記者；緊急求救



掃描閱讀

個人隱私指引研究專題
本場不另提供簡報檔；
此碼只連文章目錄。

臺灣求助

詐騙／帳號冒用：165

犯罪、急迫危險、跟騷：110

保護案件：113 或就近警察機關

Q&A先做一個行動，再帶問題來。