

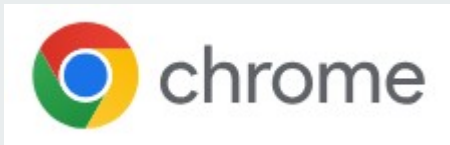


瀏覽器追蹤技術、反追蹤策略和 使用者自主

Pellaeon @ COSCUP 2026

Blog: <https://nylle.wordpress.com>

第三方 Cookie 跨站追蹤



唯一支援

1. 網站 A 塞一個 cookie 給瀏覽器，並通知廣告平台
2. A 跟瀏覽器說如果你造訪 B 網站的時候記得交這個 cookie 給 B
3. 瀏覽器造訪 B，B 把 cookie 資料傳遞給廣告平台
4. 廣告平台得知同一瀏覽器造訪了 A, B 網站（及時間）



不需第三方 cookie 的 追蹤：瀏覽器指紋

追蹤方法歸類

來自 [*A Survey of Browser Fingerprint Research and Application*](#)

推薦閱讀 Allen Chou 的 [*Web Tracking 筆記*](#)

1. JavaScript-based fingerprints
2. CSS-based fingerprints
3. Canvas-based fingerprint
4. Hardware-based fingerprints
5. Fingerprint based on Audio API
6. Plugin-based fingerprint
7. Other: performance, network delay, etc



現代網頁也包含很多你 極少用到的功能

1. WebUSB
2. WebBluetooth
3. WebVR
4. WebGL



大多數時候，
WebGL 的用途是辨
識使用者，而不是繪
製圖形

dl.acm.org

正在執行安全驗證

此網站使用安全服務抵禦惡意機器人。當網站驗證並確認您不是機器人時，便會顯示此頁面。



驗證您是人類





瀏覽器指紋追蹤的方法

1. 收集瀏覽器或使用者的特徵值 (features)
 - a. 上述的瀏覽器技術都可以收集資訊作為特徵
2. 綜合不同特徵，提高獨特性
 - a. 如：zh_TW 語系、字型 A, B, C、Windows 11、視窗 1920*1200、CPU 8 核心
3. 記錄
4. 收集每個使用者的特徵，在過往紀錄找最相似的
5. 成功關連

反追蹤：
操弄追蹤器讀取的特徵值

反追蹤策略：差異化 / 一致化 都有缺點



差異化：讓瀏覽器特徵對每一次瀏覽、每一個網站都看起來不一樣，**Brave** 採行這種策略，換句話說就是一個人每次看起來都像是不同人。

- 並不是每一個會被收集的資料項目都那麼容易差異化
- 有時多個來源可以得知同一項特徵，要確保不同來源取得的特徵一致
- 進階的追蹤器有可能可以透過多次收集數據獲得平均值拿來追蹤，因為取多次平均值可以抵消隨機演算的效果

一致化：讓用同一個瀏覽器的不同用戶看起來一模一樣，無法分辨，**Tor Browser** 採行這種策略，換句話說就是每個人看起來都像同一個人。

- 有些東西一致化之後會降級使用者體驗，比如說所有人都必須要使用 UTC+0 時區、固定的視窗大小
- 所屬的一致化群體必須要夠大才有意義

反追蹤一旦被追蹤器識破， 反而會成為一項強烈的有用特徵

但若高比例的人使用同一種反追蹤則此特徵不那麼有用
但使用反追蹤的人比例實際上不高

那難道我們要放棄反追蹤嗎？

或許我們還沒考慮過的：
建立多重身份
知情拒絕

—



多重身份

既然網頁追蹤的主要目的是廣告，廣告平台的目的是得知興趣
那不如我們依照興趣，自主將自己切割為多個分身？

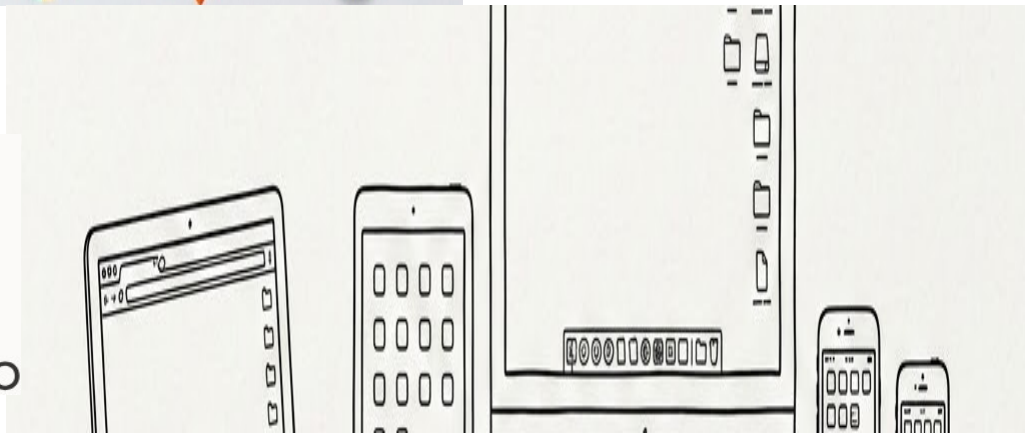
多個程式 / 平台
多個裝置
多個目的



kagi



DuckDuckGo



個人、興趣、社交
工作、金融、旅行
購物、影音
遊戲



跨裝置環境的追蹤仍可能關聯多個分身

- 線上帳戶登入
- 同 IP / 地理定位
- 超連結追蹤參數
- 硬體特徵
- 行為模式

看個人的威脅模型決定應對層級



其他想法、工具

- Firefox Container, uBlock origin
- 使用搜尋引擎及網頁瀏覽以外的來源替代網頁資訊
 - RSS, LLM 搜尋, Privacy redirect (e.g. Invidious)
 - 使用原生應用程式，有更多追蹤，但可以分散行為
- 設定檔 (profiles)



停下來想想，其實一切都是為了廣告

- 偶爾，我們有能力不選擇這個以廣告、營利為基礎的網際網路
- 選擇自架、非營利網站、自由開源方案，主動避開追蹤
- 現代提倡小農、環境友善的產品很多，那電腦產品可不可以也對網路環境友善？
- 如果考慮選擇權，那是否有可能在**得知**被追蹤之後拒絕造訪？



知情

- 跳出 CAPTCHA
- 插件偵測
 - Jshelter, [FP-Radar](#)
- 權限請求對話框
 - 但 WebGL 不需權限

拒絕

- 回上一頁
- 看有沒有其他來源
- 有時候不看其實沒差



知情了什麼

- Cloudflare CAPTCHA 有不同的控制層級，有些網站我過得去
- 航空公司網站會收集**超多**瀏覽器特徵：
 - 長榮超多追蹤 (Akamai)，幾乎每個操作都要一次 CAPTCHA
 - 華航次多，其他外國航空公司一般沒有這麼誇張難用
- 若使用 Firefox / 反追蹤，蝦皮會偷偷取消你的訂單

JShelter

Fingerprint detector report Blocks fingerprinting

*Still can't pass Cloudflare

Extension: (JShelter) - Fingerprint Detector Report — Mozilla Firefox

Fingerprint Detector Report ?

www.dcard.tw

FingerprintingActivity

Track calling scripts

Export full FPD Report as JSON

Show details

Definition of fingerprinting behavior by FPD module.

BrowserProperties

Fingerprinting methods based on simple information gathering by accessing certain APIs.

NavigatorBasic

Basic information about browser and system.

NavigatorHardware

Hardware information about device.

NavigatorMobile

Information about features supported by mobile devices.

ScreenInfo

Information about screen and its properties.

WindowInfo

Information about screen from root Window object.

StorageInfo

Availability of WebStorage technology.

NavigatorFlags

Binary browser settings.

TimeInfo



IP 位址追蹤

- 行動網路很多人共享同 IP (v4)
- 定期更換 IP
- VPN, split tunneling



反追蹤不是一切：反 feature creep

- Javascript , WebAssembly 本質上是一種遠端程式執行
- 有 sandbox ，但還可以存取這麼多硬體資源？！
- 開發者要存取硬體資源應該好好開發一個原生應用程式
- 這我的電腦，在上面跑什麼程式是我說了算
- 所以我決定停用 webassembly, WebGL
- 有些網站會壞掉，且會形成強烈的追蹤信號，與反追蹤的目的相反

The **inner-platform effect** is the tendency of software architects to create a system so customizable as to become a replica, and often a poor replica, of the software development platform they are using.



反追蹤不是一切：我也想表達立場

- 我通常想要表達自己是 Firefox / Linux 使用者
- 但這些其實是很強烈的特徵
- 如果每個 Linux 使用者為了反追蹤都要偽裝成 Windows 使用者，那廠商就更不會做 Linux 支援



我的環境區隔實作：多個 Firefox profile

Profile= 設定檔，類似於開另一個系統帳號來用 Firefox

1. 主要日常瀏覽：留下痕跡比較沒關係
2. 主要工作瀏覽
3. 允許 feature creep 瀏覽：Facebook messenger, WhatsApp, Google meet, cloudflare, 機票
4. 完全不想要留下紀錄：使用 Tor Browser

對於大部分人來說，單純區分私人及工作瀏覽器就已經建立有用的區隔



小結

- 要想清楚自己的威脅模型
- 不同的目標可能不相容
- 區分不同目標考量的使用情境
- 知情同意或拒絕
- 有時候無法拒絕，但不是所有狀況都無法拒絕，在能拒絕的時候拒絕很重要，而非一律同意



我為什麼要講這些

- 當然不是要求所有人都要做到像我一樣
- 大家都會在意自己生活的環境，
我的生活一部分在網路上，所以我在意網路環境
- 「你講的聽起來真麻煩」——那其實可以不用在意
- 但如果碰巧你也有點在意，本議程提供一些我的思考和方法，
或許可以幫你省一些時間



保護隱私的網頁追蹤？ FLoC, Topics API...

- 同時考慮使用者隱私和廣告商追蹤需求？
- 眾多問題目前無解
 - 根本上一定要向廣告商透露個資
 - 原本的瀏覽器追蹤仍然可用，萬一結合則形成超強特徵
- 參考 [Web Tracking 筆記](#)
- 而且，作為一個隱私被侵害的使用者，
為什麼我要考慮廠商的需求？



撇除個人隱私，為什麼網頁追蹤（定向廣告）
對社會不好？

- **The power to target is the power to discriminate.** By definition, targeted ads allow advertisers to reach some kinds of people while excluding others. A targeting system may be used to decide who gets to see job postings or loan offers just as easily as it is to advertise shoes. -[EFF](#)
- Cambridge Analytica, etc.

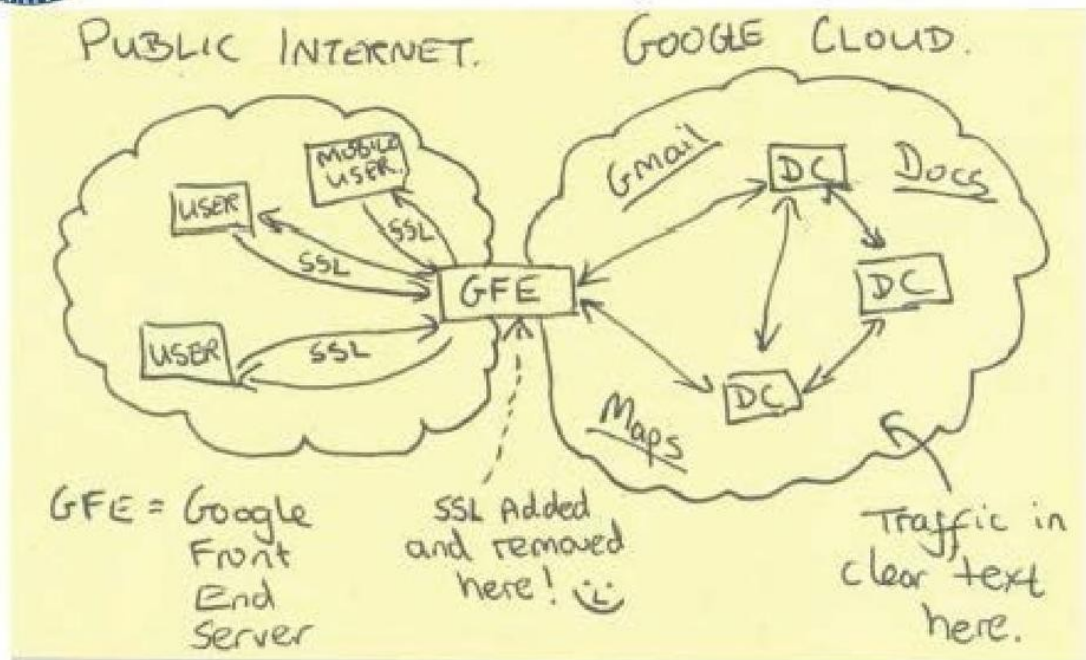


那我們可以立法禁止定向廣告相關歧視 / 資訊操弄 / 其他有害用法？

- 法律保護永遠都慢於實際傷害發生
- 如果都有方便的追蹤功能了，廠商 / 政府不用白不用
- 所有人一定會守法？



Current Efforts - Google





但現在其實充滿了各種機會

- LLM 可以替代一部分搜尋引擎和網頁瀏覽
 - 沒有追蹤使用者網頁瀏覽的問題了
 - 營利模式暫且不是基於定向廣告
 - 但反而可以藉由 LLM 和使用者的互動更加瞭解使用者
- 高品質的內容創作移往付費模式，賣廣告盈利的需求下降
- LLM 可幫助進階使用者客製化軟體，也降低新軟體的開發成本
 - ➔ 開發小眾軟體的成本下降 ➔ 促進軟體多樣性及競爭
- 會如何發展沒有人知道，但使用者權益有機會更進一步

PoC: LLM 修改 Firefox 程式

- 加上 WebGL 權限對話框
- 加上 WebAssembly 權限

