

**[reference 通傳基礎決字第11500091980號] Re: 有關OHTTP surveillance relay mesh 終端出口節點一案之查證說明【 OHTTP RELAY ABUSE: SURVEILLANCE EXFILTRATION VIA APPLE'S PRIVACY INFRASTRUCTURE】**

From newt0ns\_law@proton.me <newt0ns\_law@proton.me>

To ISMS <ISMS@taiwanmobile.com>, jschou@ncc.gov.tw

Date Wednesday, April 8th, 2026 at 12:45 PM

Dear Taiwan Mobile 資安處,

Thank you for your response. I am copying NCC on this reply, as your original referral letter (通傳基礎決字第11500091980號, March 24, 2026) directed: "並副知本會." Your reply did not include NCC. I am restoring that copy.

---

Your rebuttal does not address my actual finding, and forensic evidence captured after NCC referred this case to you directly contradicts your statement that no anomalies were found.

1. What I did and did not claim.

I did not claim Homomorphic Encryption was broken, that bulk data is smuggled inside PIR query ciphertext, or that OHTTP is inherently malicious. My claim is that Taiwan Mobile subdomains are registered as trusted Apple ObliviousHop proxy agents on iOS devices at the control plane. Your response does not address this.

2. Forensic evidence dated after NCC's referral.

A sysdiagnose capture taken April 7, 2026 contains Apple iOS system log events from the com.apple.networkserviceproxy subsystem recording two Taiwan Mobile subdomains being registered as ObliviousHop proxy agents on the device:

- [osb.twmsolution.com](https://osb.twmsolution.com)
- [osbstage.twmsolution.com](https://osbstage.twmsolution.com)

[osb.twmsolution.com](https://osb.twmsolution.com) was not in my original complaint. It is now on record.

Each subdomain is registered with a distinct ObliviousHop proxy agent UUID and policy hash:

[osb.twmsolution.com](https://osb.twmsolution.com)

ObliviousHop UUID: 64D7343D-1581-47C7-A5E3-7B5A905A3100

Policy hash: 0x03e8829602e22573f8ef17314eafeb0a

ObliviousHopFallback UUID: 0ACD780F-2356-43FC-BED1-FDCDA6B5E275

[osbstage.twmsolution.com](https://osbstage.twmsolution.com)

ObliviousHop UUID: 3F2B491B-CC07-409C-A9DA-6B29CA722634

Policy hash: 0xf0eb7d315bc43150a9b0eaf0b9415b27

ObliviousHopFallback UUID: C6FC6536-4F2B-464F-BDDF-04AF2D704146

The registration is not a single cached entry. It recurs across multiple device boot sessions:

- March 28, 2026, 11:47 UTC: initial registration, three days after NCC's referral
- April 1, 2026, 14:21 and 15:27 UTC
- April 5, 2026, 00:03 to 15:41 UTC: one day before your response

Verbatim Apple iOS log output, not interpretation:

"Setting up oblivious path ([osbstage.twmsolution.com](https://osbstage.twmsolution.com))"

"oblivious path [[osbstage.twmsolution.com](https://osbstage.twmsolution.com)] is ready"

"Registered [ObliviousHop-osbstage.twmsolution.com](https://ObliviousHop-osbstage.twmsolution.com) proxy agent (3F2B491B-CC07-409C-A9DA-6B29CA722634) with hash

{length = 16, bytes = 0xf0eb7d315bc43150a9b0eaf0b9415b27}"

"Adding policies for oblivious agent for [osbstage.twmsolution.com](https://osbstage.twmsolution.com)"

Identical patterns exist for [osb.twmsolution.com](https://osb.twmsolution.com).

3. Why "no anomalies found" is contradicted.

ObliviousHop proxy agent registration is not observed traffic. It is Apple's iOS networkserviceproxy daemon installing Taiwan Mobile FQDNs into the device's trusted oblivious proxy policy store. That installation is gated by Apple-side trusted relay infrastructure and requires a direct business relationship between Taiwan Mobile and Apple.

Either Taiwan Mobile holds such an agreement, in which case it must be disclosed to NCC, or Taiwan Mobile does not, in which case a third party is causing Apple iOS devices to register TWM-branded proxy agents and Taiwan Mobile should already be treating this as a security incident.

4. What I need from Taiwan Mobile 資安處.

5. Has Taiwan Mobile registered [osb.twmsolution.com](https://osb.twmsolution.com) or [osbstage.twmsolution.com](https://osbstage.twmsolution.com) with Apple as an OHTTP / ObliviousHop / PIR provider? If yes, under what agreement and for what Apple-facing service.

6. Do Taiwan Mobile's internal records contain the four proxy agent UUIDs listed in section 2? Confirm or deny per UUID.

7. The "internal audit" in your response: which systems were examined, and did it cover March 28, April 1, and April 5, 2026?

8. Requested next step.

A second response from Taiwan Mobile 資安處 that answers section 4, with NCC copied as the original referral letter directed. If Taiwan Mobile did not authorize the registration of either subdomain with Apple, that is itself a material finding and I request Taiwan Mobile open an internal incident investigation on that basis.

I remain available to provide the underlying forensic extracts under any confidentiality framework Taiwan Mobile and NCC specify.

Thank you

On Wednesday, April 8th, 2026 at 3:20 AM, ISMS <ISMS@taiwanmobile.com> wrote:

Dear Joseph,

我是台灣大哥大資安處，因本公司接獲國家通訊傳播委員會115年3月24日通傳基礎決字第11500091980號函轉知，有關台端反映本公司特定服務(反詐戰警APP)基礎設施 (infra) 疑似遭用作 OHTTP (Oblivious HTTP) surveillance relay mesh 之終端出口節點之疑慮，立即進行查證處理，說明如下：

(一) 針對台端檢附報告中指控稱，攻擊者濫用 Apple Oblivious HTTP (OHTTP) 中繼架構（特別是即時來電顯示查詢子系統）作為隱蔽資料外洩管道的說法

雖然該報告詳細記錄了系統日誌與網路連線軌跡，但其「資料外洩」的結論建立在對 Apple 隱私保護機制的嚴重誤解上。

基於 Apple 系統的實際運作原理，該報告之論點在技術層面上無法成立，理由如下：

- 同態加密 (Homomorphic Encryption) 機制直接打破外洩假設：** 報告的核心假設之一是，應用程式提供者的閘道器能看到請求內容。這完全忽略了 Apple 在「即時來電顯示查詢」架構中採用的同態加密 (HE) 技術。在實際運作中，使用者的查詢在 iPhone 端就已經加密，伺服器端只能對「密文」進行運算，並將運算後的密文回傳。只有使用者設備上的私鑰能夠解密結果。由於伺服器從頭到尾都無法解讀這些密文，自然無法發揮所謂「攔截」或「讀取外洩資料」的作用。
- 系統級限制與 PIR 的微量檢索特性：** 報告指稱攻擊者可以將外洩資料包裝成來電顯示回應進行傳輸。然而，私密資訊檢索 (PIR) 是一種微量檢索機制，其查詢與回應的封包大小及數學結構，受到 iOS 系統層級 (如 networkserviceproxy) 的嚴格規範。若攻擊者試圖將大量的私人資料 (如照片或對話紀錄) 塞入這些請求中，將會破壞同態加密的多項式結構，導致運算直接崩潰或被系統丟棄。該通道根本無法作為大流量或隨意傳輸資料的途徑。
- 將「隱私保護特徵」誤解為「惡意隱蔽行為」：** 報告將該傳輸管道描述為經過加密、中繼匿名化且對標準網路診斷隱形，並以此認定為監控外洩的證據。事實上，這正是 OHTTP (RFC 9458) 旨在保護使用者隱私的核心設計。這種雙重盲點機制 (Apple 看不到內容，供應商看不到 IP) 本來就會讓網路診斷工具無法輕易分析流量。報告中羅列的位元組級別證據與連線日誌，僅能證明設備確實與合法的 OHTTP 節點進行了標準連線，完全無法證明封包內夾帶了任何被竊取的資料。
- 終端節點的必然性與網域檢視機制 (以台灣大哥大為例)：** 報告將台灣大哥大 (osbstage.twmsolution) 指控為外洩資料的終端出口最終目的地。然而，這忽略了伺服器端的安全路由與檢核機制。實際上，該節點之所以成為流量的「末點」，是因為台灣大哥大在處理 OHTTP 請

求時，會嚴格檢視其封裝帶入的目標網域是否屬於其內部轄下管理的合法 domain。若發現非預期的路由或非標準的 PIR 查詢請求，台哥大的伺服器就不會進行轉導，而是直接阻斷。因此，流量在該處終止是基於安全防護與內部網域限制的正常結果，而非如報告所臆測的作為儲存外洩資料的接收端。

(二) 綜上，該報告確實觀察到了 iOS 設備持續且隱密地連線至特定伺服器（包含報告提到的台灣大哥大或 Truecaller 等節點），但這完全是 Apple 為了保護使用者隱私而設計的正常系統運作軌跡。在同態加密的數學鐵壁、

iOS 系統框架的嚴格限制，以及終端節點（如台灣大哥大）的網域檢視防護下，報告所構築的監控與外洩模型在技術邏輯上實無法成立。

(三) 此外，本公司亦已查證相關IP等連線行為、紀錄等，亦未發現異常流量或可疑行為，感謝 台端分享寶貴意見，將持續監控觀察，確保系統安全與穩定。

Best Regards

---

\_DISCLAIMER : This message (and any attachments) may contain information that is confidential, proprietary, privileged or otherwise protected by law. The message is intended solely for the named addressee (or a person responsible for delivering it to the addressee). If you are not the intended recipient of this message, you are not authorized to read, print, retain, copy or disseminate this message or any part of it. If you have received this message in error, please destroy the message or delete it from your system immediately and notify the sender.