

Prima di proseguire il nostro "viaggio" tecnico su come difendere la nostra privacy navigando in internet, prendiamoci una pausa e riflettiamo sugli ultimi fatti accaduti sul tema: Apple "traccia" i suoi utenti, Sistemi "anti-theft" per cellulari fin troppo potenti, la società Tomtom collabora con la Polizia Olandese.

Nel corso dei nostri articoli abbiamo parlato di quanto siano importanti i nostri dati e di come, purtroppo, il rischio di fornire informazioni preziose e riservate in internet sia molto facile e che una "consapevolezza informata" è obbligatoria.

L'usare servizi web o mobile è fondamentale per un qualsiasi utente ed in particolar modo per un utente "mobile", ma spesso servizi apparentemente usati a fini di bene possono diventare della armi a doppio taglio e portarci in situazioni poco gradite.

Questo problema è diventato attuale negli ultimi giorni grazie ad una scoperta fatta da [Alasdair Allan e Pete Warden](#)

, due ricercatori inglesi, su i dispositivi della Apple. Hanno scoperto che praticamente tutti i dispositivi mobili 3G della Apple dell'ultima generazione (iPhone e iPad) tracciano gli spostamenti dei propri utenti e che queste informazioni vengono memorizzate localmente e copiate in maniera non protetta all'interno del proprio computer al momento della sincronizzazione (Source:

[Radar Oreilly.com](#)

). Per dimostrarlo hanno messo a disposizione un programma che visualizza tali informazioni,. Queste informazioni non vengono trasmesse ad Apple o a terze parti, ma la porta è aperta ed il dubbio comincia ad esserci.

I dispositivi mobili della Apple non sono gli unici dotati di GPS e con la capacità di memorizzare la propria posizione. I cellulari della Nokia di fascia alta con GPS (esempio il Nokia E7) sono dotati di una funzionalità detta "Anti-theft" (anti-ladro) mentre sui dispositivi di fascia alta della Samsung la stessa funzionalità si chiama "Mobile Tracker" (Esempio il Galaxy Tab 7" o il Galaxy Mini).

Le due soluzioni hanno funzionalità di base simili e possono essere considerate "buone" come "cattive" in funzione dell'uso che se ne fa.

Le soluzioni anti-Theft per i cellulari hanno lo scopo di proteggere i dati contenuti nel dispositivo mobile in caso di furto o smarrimento. Quando il cellulare viene smarrito/rubato è possibile comandarlo remotamente e fargli cancellare tutti i nostri dati personali (contatti, foto, etc) e, previa una configurazione del cellulare mentre era in nostro possesso, è possibile rintracciarlo fisicamente attraverso il posizionamento GPS integrato o ricevere una notifica nel caso in cui venga sostituita la SimCard.

I principi sono sicuramente validi, ma ci portano a fare alcune considerazioni.

Se il cellulare è sempre rintracciabile lo siamo anche noi. Lasciare il cellulare incustodito senza averlo protetto con codici sicuri diventa imprudente. Il rischio è che qualcuno possa sapere sempre dove vi troviate con un semplice SMS o con un accesso al web.

Se installiamo una applicazione sul dispositivo di cui non siamo sicuri, potrebbe capitare che il cellulare cominci a "trasmettere" informazioni a vostra (semi)-insaputa. Dico (semi) perché l'utente che ha installato l'applicazione ha avuto sicuramente "letto" un messaggio di avviso che informava sui dati trasmessi, sulle risorse utilizzate e che chiedeva l'autorizzazione... Per esempio, sui dispositivi dotati di [Android](#) (sistema operativo di Google, anche lui al centro di diverse polemiche sulla privacy) al termine dell'installazione una nuova applicazione, è necessario dare l'ok all'uso delle risorse (navigazione dati, telefono, GPS, WiFi, Bluetooth, etc). Purtroppo, la maggior parte degli utenti conferma lenza leggere i messaggi di avvertimento ed i termini d'uso della applicazione.

Un esempio pratico di come i dati personali di posizione collezionati in maniera "ignara" possono essere usati, lo ha dato la TomTom che ha venduto in Olanda i dati di traffico stradale raccolti dai propri utenti alla Polizia. In base a quei dati, la Polizia Olandese ha potuto decidere dove posizionare i controlli elettronici di velocità (Source: [Forbes](#) ). Naturalmente, Tomtom ha il diritto di rivendere i dati raccolti dai suoi dispositivi in forma anonima.

L'ultimo grande quesito è se queste informazioni sono in qualche modo utilizzate (anche in maniera anonima) dagli operatori di telefonia. Sicuramente sono utilizzate le informazioni di traffico e di localizzazione sulla cella di collegamento a fini statistici, ma quella solita voce che mi consiglia prudenza, mi suggerisce che gli operatori potrebbero usare tali informazioni per sapere quanti utenti passano in una strada, quali negozi vengono visitati, quante persone entrano in un centro commerciale, etc.

Insomma, il grande fratello alla Orwell è veramente (troppo) vicino.

*(02 Maggio 2011)*

## Ultimi scandali sulla privacy...

Scritto da Marco Ciavarella

---