Proteggi la tua privacy in un mondo di sorveglianza digitale

- Come Google cattura tutta la tua vita
- Come le app mobili ti tracciano costantemente
- 5 semplici passi per proteggere te stesso e la tua famiglia

murena
choose freedom

In breve

Nell'era digitale odierna, la privacy è diventata uno dei temi più cruciali per gli individui e le società. I dispositivi su cui facciamo affidamento – in particolare i nostri smartphone – raccolgono una quantità immensa di dati personali e professionali, spesso senza la nostra piena comprensione o reale consenso.

Giganti tecnologici come Google e Apple, insieme a una vasta gamma di applicazioni mobili, hanno accesso a dettagli intimi delle nostre vite, e i metodi che utilizzano per tracciarci rappresentano minacce significative per la nostra privacy e sicurezza.

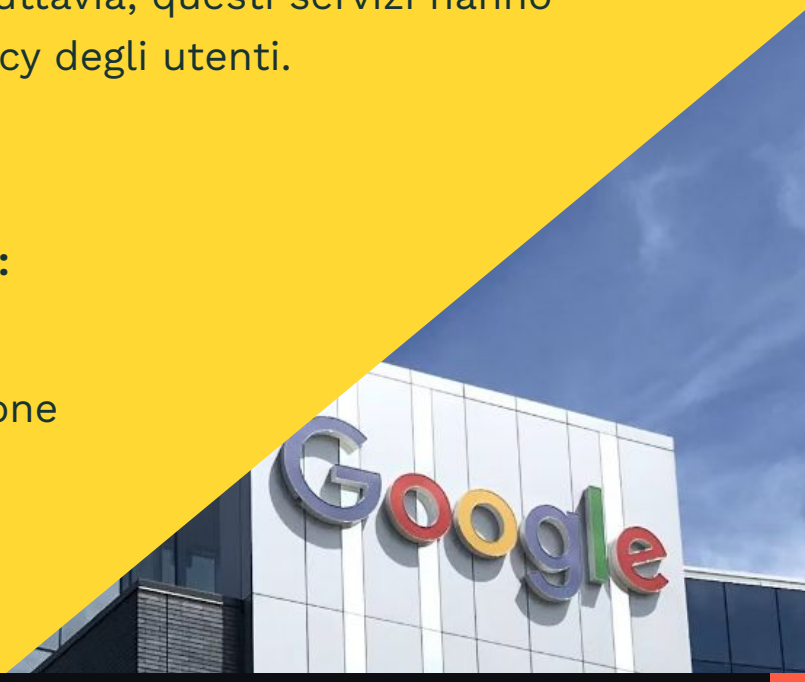
Questo documento esplora fino a che punto aziende come Google e Apple raccolgano dati degli utenti, come le app mobili traccino gli utenti attraverso la pubblicità e le aste in tempo reale, e le possibili conseguenze di tali pratiche. Fornisce inoltre semplici passi per aiutarti a proteggerti dalla sorveglianza digitale.

Come Google raccoglie e utilizza i dati degli utenti

Google, una delle più grandi aziende tecnologiche al mondo, ha costruito il suo impero offrendo servizi "gratuiti" come Gmail, Google Search, YouTube e Google Maps, traendo enormi profitti dalla pubblicità. Tuttavia, questi servizi hanno un costo significativo per la privacy degli utenti.

Come Google raccoglie i tuoi dati:

- Tracciamento della posizione
- Cronologia di ricerca e navigazione
- Comunicazioni personali
- App di Google e Android



11,6 MB/giorno/utente

Il volume dei tuoi dati personali raccolti da Google da smartphone Android.

Fonte: Digital Content Next – Prof. Douglas C. Schmidt, Università di Vanderbilt, agosto 2018.

Come Google raccoglie e utilizza i dati degli utenti

Tracciamento della posizione

Google traccia la tua posizione anche quando non utilizzi Google Maps. Raccoglie dati in tempo reale da dispositivi Android e può dedurre la tua posizione tramite indirizzi IP, reti Wi-Fi e connessioni Bluetooth.

Come Google raccoglie e utilizza i dati degli utenti

Cronologia di ricerca e navigazione

Ogni ricerca che effettui tramite Google Search e ogni sito web che visiti tramite Google Chrome viene tracciato e registrato. Questo consente a Google di costruire un profilo dettagliato dei tuoi interessi, abitudini e comportamenti.

Come Google raccoglie e utilizza i dati degli utenti

Comunicazioni personali

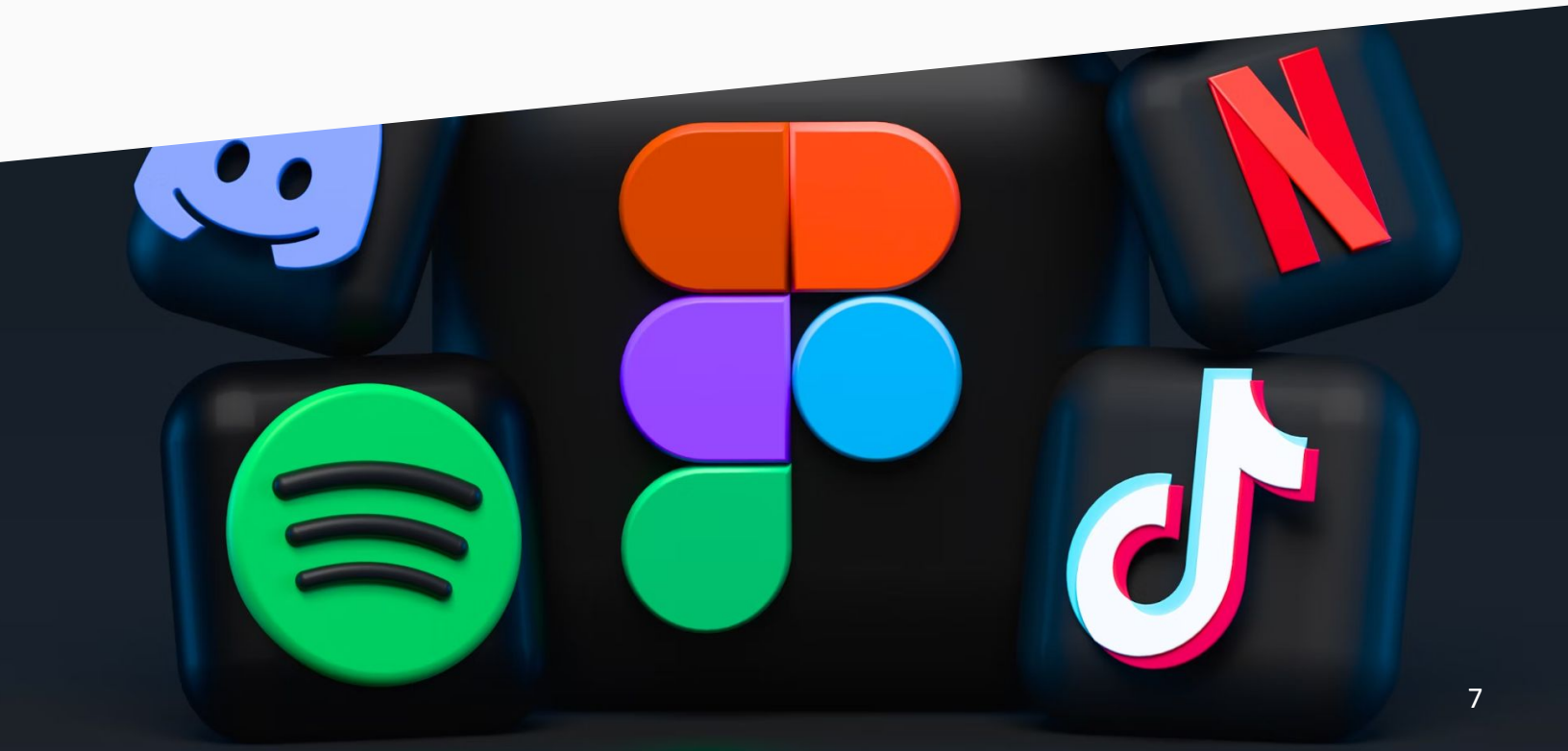
Se utilizzi Gmail o Google Drive, il contenuto delle tue email e documenti può essere analizzato dagli algoritmi di Google per migliorare il targeting pubblicitario. Google raccoglie anche i dati di messaggi di testo e chiamate degli utenti Android senza consenso.

Fonte: "What Data Do The Google Dialer and Messages Apps On Android Send to Google?", Prof. Douglas Leith, Trinity College, Dublino, 2022.

Come Google raccoglie e utilizza i dati degli utenti

App di Google e Android

La maggior parte degli smartphone Android è legata all'ecosistema di Google, il che significa che ogni interazione con il tuo telefono (come aprire app, utilizzare la fotocamera o i comandi vocali) può essere raccolta.
I servizi di Google Play tracciano come e quando utilizzi app e siti web, dando a Google accesso a dati comportamentali estesi.



L'approccio di Apple alla raccolta dei dati

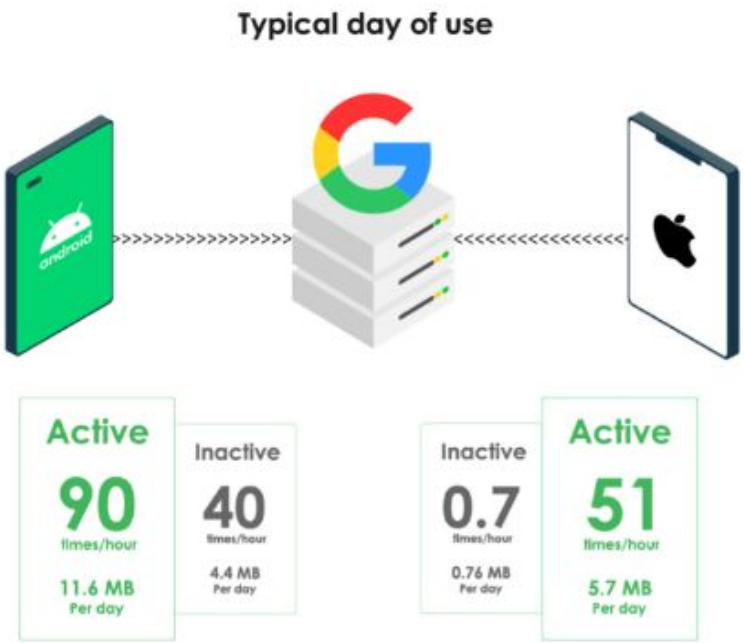
Sebbene Apple si presenti come un'azienda più orientata alla privacy, partecipa comunque a una significativa raccolta di dati. Apple non raccoglie tanti dati passivamente quanto Google, ma raccoglie comunque informazioni tramite i suoi servizi come App Store, iCloud e Apple Health.

Apple riceve inoltre oltre 25 miliardi di dollari all'anno da Google per rendere Google Search il motore di ricerca predefinito sui dispositivi iOS.

Volumi di dati raccolti:

- Un telefono Android inattivo trasmette tra 4,4 MB e 11,6 MB di dati personali al giorno a Google.
- Un dispositivo Apple invia tra 0,76 MB e 5,7 MB di dati al giorno a Google.

Fonte: Rapporto dell'Università di Vanderbilt.



Conseguenze della raccolta dei dati da parte di Google e Apple

Gli sforzi massicci di Google e Apple nella raccolta dei dati consentono a queste aziende di creare profili incredibilmente dettagliati degli individui, includendo la cronologia delle posizioni, le ricerche, le abitudini di comunicazione e gli acquisti online. Questo solleva gravi preoccupazioni sulla privacy:

- **Economia della sorveglianza:** Con dati così completi, Google (e aziende tecnologiche simili) può plasmare le nostre esperienze online, limitare i contenuti che vediamo e manipolare le nostre decisioni, sia negli acquisti, nelle preferenze politiche o nella vita quotidiana.

- **Manipolazione comportamentale:** Con informazioni precise sul comportamento degli utenti, Google può utilizzare i suoi dati per influenzare non solo le pubblicità che gli utenti vedono, ma anche ciò che pensano o sentono, comportando gravi rischi per l'autonomia.

- **Violazioni dei dati:** Più dati un'azienda raccoglie, più attraente diventa per gli hacker. Le violazioni dei dati in aziende come Google possono esporre informazioni personali.

Come le app mobili utilizzano la pubblicità e le aste in tempo reale per tracciare gli utenti

Oltre a Google e Apple, molte app mobili partecipano a pratiche invasive di tracciamento su scala globale, spesso senza che gli utenti ne siano pienamente consapevoli. Come le app tracciano gli utenti:

- **ID pubblicitari:** I dispositivi mobili dispongono di identificatori unici, come l'IDFA (Identifier for Advertisers) di Apple o l'Advertising ID di Google, che consentono alle app di tracciare gli utenti su diverse piattaforme. Questi ID vengono utilizzati per mostrare pubblicità mirate.

- **Aste in tempo reale (RTB):** RTB è un sistema di aste automatizzato in cui gli inserzionisti fanno offerte in tempo reale per mostrare annunci a utenti specifici. Quando apri un'app o un sito web, gli inserzionisti ricevono immediatamente informazioni su di te – come la tua posizione, il dispositivo e il comportamento precedente – e fanno offerte per mostrare annunci. Questo processo avviene milioni di volte al secondo.

Conseguenze del tracciamento da parte delle app mobili e delle aste in tempo reale

I dati raccolti dalle app mobili e dalle aste in tempo reale rappresentano gravi minacce alla privacy degli utenti:

- **Manipolazione mirata:** I dati raccolti tramite RTB consentono agli inserzionisti di creare annunci altamente mirati e personalizzati. Sebbene ciò possa migliorare la pertinenza degli annunci, consente anche agli inserzionisti (o ai gruppi politici) di manipolare il comportamento degli utenti fornendo contenuti specifici ed emotivamente coinvolgenti.
- **Sorveglianza costante:** Le app possono tracciare la tua posizione, l'uso delle app e il comportamento di navigazione in tempo reale, spesso senza il tuo consenso. Questo porta a una sorveglianza continua della tua vita digitale.

- **Broker di dati ed erosione della privacy:** I dati raccolti tramite RTB vengono spesso condivisi con broker di dati di terze parti, che possono compilare profili completi degli utenti. Questi broker vendono i tuoi dati a inserzionisti, governi o altre entità, aggravando ulteriormente l'erosione della tua privacy.

Consigli per proteggerti dalla sorveglianza digitale

Fortunatamente, ci sono diversi passaggi che puoi seguire per proteggerti dalla sorveglianza digitale:

- **Disattiva il tracciamento della posizione:** Disattiva i servizi di localizzazione per le app che non ne hanno bisogno e utilizza una VPN per mascherare il tuo indirizzo IP.
- **Blocca i tracker pubblicitari:** Usa estensioni del browser orientate alla privacy. Disattiva gli ID pubblicitari su Android e iOS. Il blocco dei tracker nelle app e sul web è anche una funzione predefinita in /e/OS.
- **Minimizza le autorizzazioni delle app:** Esamina regolarmente le autorizzazioni delle app e revoca l'accesso ai dati che non sono necessari per il funzionamento di base dell'app.
- **Utilizza app alternative:** Sostituisci quante più app e servizi di Google possibile, in particolare Gmail e Google Search.
- **Usa la crittografia end-to-end:** Opta per app di messaggistica come Signal, Matrix/Element o Threema, che offrono crittografia end-to-end, assicurando che le tue comunicazioni rimangano private. Usa servizi di posta elettronica che offrono crittografia end-to-end completa, come ProtonMail.
- **Considera dispositivi orientati alla privacy:** Gli smartphone Murena che eseguono /e/OS sono progettati per rispettare la tua privacy, evitando i meccanismi di tracciamento di Google e i tracker pubblicitari.

La sicurezza NON è la stessa cosa della privacy!

Nell'attuale panorama digitale, c'è spesso confusione tra sicurezza e privacy. Sebbene entrambe siano essenziali, servono scopi diversi:

- La sicurezza si concentra sulla protezione dei sistemi e dei dati dall'accesso non autorizzato.
- La privacy mira a limitare la raccolta e la condivisione dei dati personali sin dall'inizio.

Un dispositivo può essere sicuro e comunque compromettere la tua privacy, poiché la sicurezza non previene la raccolta o la sorveglianza dei dati da parte del proprietario del sistema.

Esempi:

- **Spyware Pegasus sugli iPhone:** Nonostante la reputazione degli iPhone come dispositivi sicuri, Pegasus ha sfruttato vulnerabilità per hackerare obiettivi di alto livello, tra cui un presidente europeo e attivisti, senza interazione dell'utente.
- **Hacking da parte dell'intelligence russa:** Durante il conflitto in Crimea, gli smartphone dei soldati ucraini sono stati hackerati, consentendo agli avversari di tracciare i loro movimenti e intercettare comunicazioni, nonostante l'uso di dispositivi crittografati di grado militare.
- **EncroChat e reti criminali:** I telefoni criptati utilizzati da reti criminali come EncroChat sono stati hackerati dalle forze dell'ordine europee, portando all'arresto di molti criminali nonostante i telefoni fossero considerati "inviolabili".

Come Murena e /e/OS proteggono la privacy degli utenti

A differenza dei principali sistemi operativi mobili come Android di Google e iOS di Apple, /e/OS praticamente non raccoglie dati personali dagli utenti. Secondo uno studio, /e/OS si distingue come il sistema più rispettoso della privacy tra varie piattaforme basate su Android come Samsung, Xiaomi e Huawei.

- **Nessun dato inviato a Google:** A differenza di altre varianti di Android, che comunicano costantemente con i server di Google, /e/OS evita qualsiasi connessione ai servizi di Google. Ciò impedisce la raccolta automatica di dati sensibili come la cronologia delle posizioni, le ricerche e l'utilizzo del dispositivo.
- **Raccolta minima di dati:** Gli sviluppatori di /e/OS hanno progettato il sistema per funzionare con quasi nessuna trasmissione di dati, anche quando il dispositivo è inattivo. Non c'è trasmissione di identificatori del dispositivo, interazioni dell'utente o dati di utilizzo delle app, pratica comune in altre varianti di Android.

Conclusione

Nell'attuale mondo digitale, i nostri dati personali vengono sempre più raccolti tramite app mobili e piattaforme web. Grandi aziende come Google e Apple raccolgono enormi quantità di dati degli utenti, creando rischi significativi poiché i comportamenti e le preferenze degli utenti vengono tracciati e venduti, spesso senza il loro consenso esplicito.

Per proteggere la tua privacy:

- Disattiva il tracciamento della posizione e utilizza una VPN.
- Sostituisci i servizi di Google con alternative rispettose della privacy.
- Preferisci app di messaggistica con crittografia end-to-end.
- Considera gli smartphone Murena che eseguono /e/OS, progettati per rispettare la tua privacy.