



# Protecting Your **Privacy** in a World of Digital Surveillance

---

- How Google is capturing all your life
- How mobile apps are tracking you all the time
- 5 easy steps to protect yourself and family

**murena**  
choose freedom

# In short

In today's digital age, privacy has become one of the most crucial issues facing individuals and societies. The devices we rely on — particularly our smartphones — are collecting vast amounts of personal and professional data, often without our full understanding or true consent.

Tech giants like Google and Apple, along with a wide array of mobile applications, have access to intimate details of our lives, and the methods they use to track us pose significant threats to our privacy and security.



This paper explores the extent to which companies like Google and Apple collect user data, how mobile apps track users through advertising and real-time bidding, and the potential consequences of such practices.

It also provides easy steps to help you protect yourself from digital surveillance.

# How Google Collects and Uses User Data

Google, one of the world's largest tech companies, has built its empire by offering "free" services like Gmail, Google Search, YouTube, and Google Maps while profiting immensely from advertising. However, these services come at a significant cost to users' privacy.

## How Google collects your data:

- Location Tracking
- Search and Browsing History
- Personal Communications
- Google Apps and Android



**11.6 MB/day/user**

The volume of your personal data collected by Google from Android smartphones.

*Source: Digital Content Next – Prof. Douglas C. Schmidt, Vanderbilt University, August 2018*

## How Google Collects and Uses User Data

# Location tracking

---

Google tracks your location even when you're not using Google Maps. It collects real-time data from Android devices and can infer your location through IP addresses, Wi-Fi networks, and Bluetooth connections.



## How Google Collects and Uses User Data

# Search and Browsing History

---

Every search you make through Google Search and every website you visit via Google Chrome is tracked and logged. This allows Google to build a detailed profile of your interests, habits, and behavior.



## How Google Collects and Uses User Data

# Personal Communications

---

If you use Gmail or Google Drive, the content of your emails and documents can be scanned and analyzed by Google's algorithms to improve ad targeting. Google also collects text and call data from Android users without consent.

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

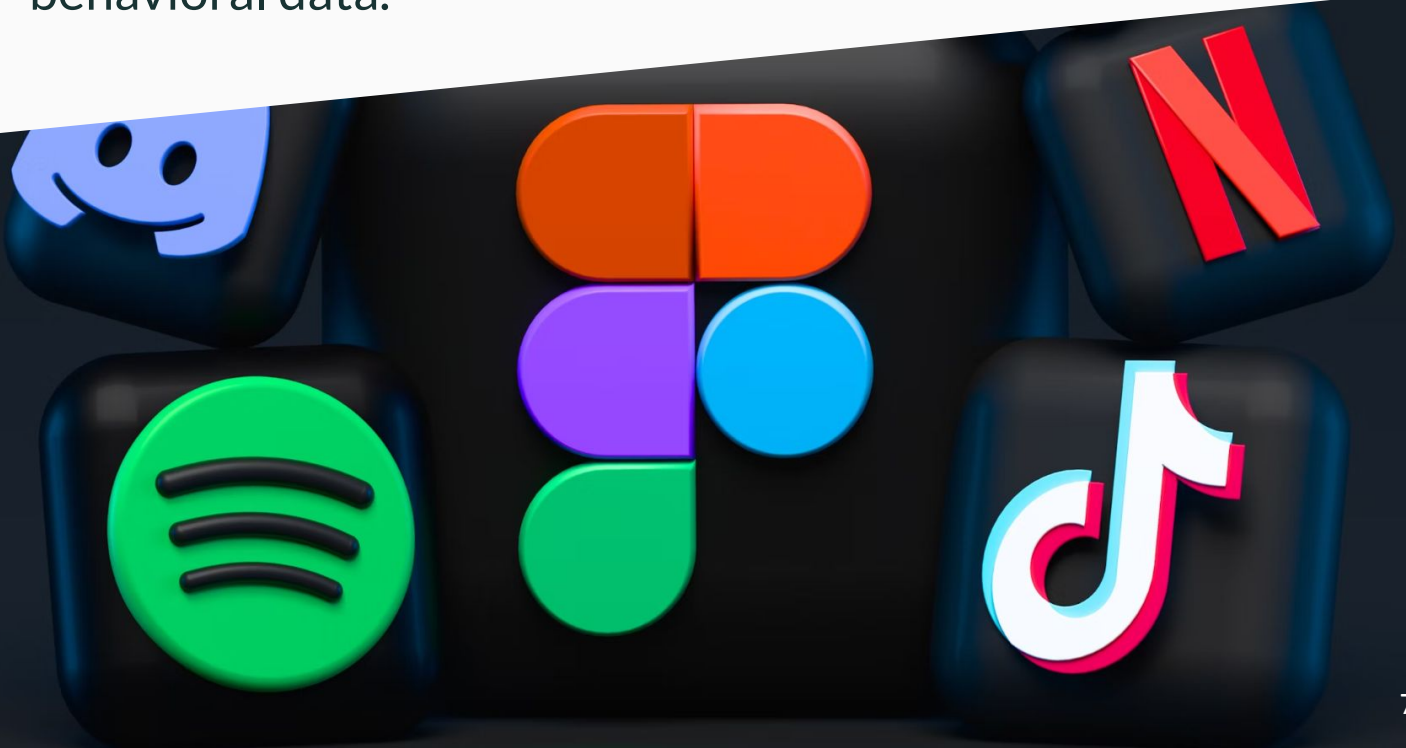


## How Google Collects and Uses User Data

# Google Apps and Android

Most Android phones are tied to Google's ecosystem, meaning every interaction with your phone (such as opening apps, using your camera, or voice commands) can be collected.

Google Play Services track how and when you use apps and websites, giving Google access to extensive behavioral data.



# Apple's Approach to Data Collection

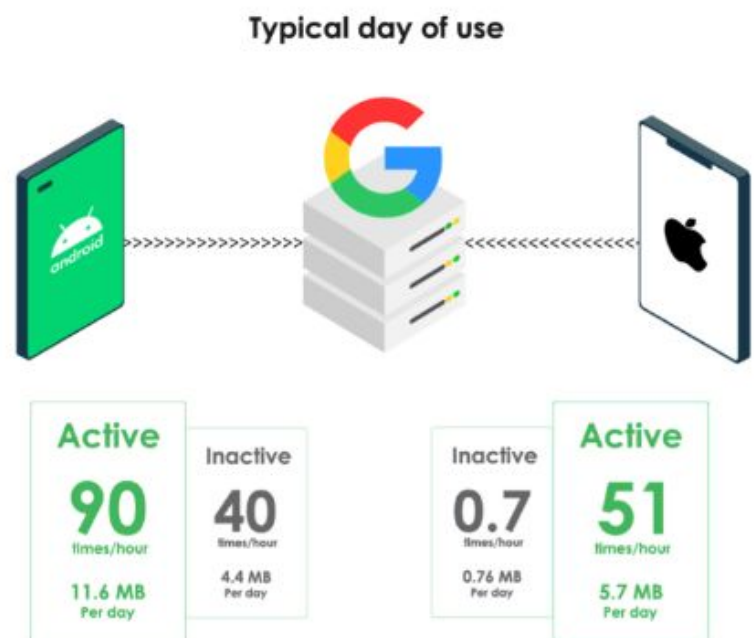
Although Apple markets itself as a more privacy-focused company, it also engages in significant data collection. While Apple does not collect as much data passively as Google, it still gathers information through its services like the App Store, iCloud, and Apple Health.

Apple also receives more than \$25Bn(!) from Google per year to make Google Search the default iOS devices' search engine.

## Huge volumes!

According to a report by Vanderbilt University, an Android phone dormant Android phone communicates between 4.4 MB and 11.6 MB of personal data to Google per day.

An Apple device sends between 0.76 MB and 5.7 MB of data per day to Google.





# Consequences of Google & Apple's Data Collection

Google and Apple's massive data collection efforts allow the company to build incredibly detailed profiles of individuals, including their location history, search history, communication habits, and online purchases. It raises significant privacy concerns:

- **Surveillance Economy:** With such comprehensive data, Google (and similar tech companies) can shape our online experiences, limiting the content we see and manipulating our decisions, whether in shopping, political preferences, or daily life.
- **Behavioral Manipulation:** With its precise insights into user behavior, Google can leverage its data to influence not only what ads users see but potentially what they think or feel, posing serious risks to autonomy.
- **Data Breaches:** The more data a company collects, the more attractive a target it becomes for hackers. Breaches at companies like Google can lead to personal information being exposed.



# How Mobile Apps Use Advertising and Real-Time Bidding to Track Users

Beyond Google and Apple, many mobile applications participate in invasive tracking practices at a global scale, often without users being fully aware. How apps track users:

- **Advertising IDs:** Mobile devices have unique identifiers, such as Apple's IDFA (Identifier for Advertisers) or Google's Advertising ID, that allow apps to track users across different platforms. These IDs are used to serve targeted ads.
- **Real-Time Bidding (RTB):** RTB is an automated auction system where advertisers bid in real-time to display ads to specific users. When you open an app or website, advertisers immediately receive information about you—such as your location, device, and previous behavior—and place bids to serve ads. This process happens millions of times per second.



# Consequences of Mobile App Tracking and Real-Time Bidding

The data collected from mobile apps and real-time bidding poses serious threats to users' privacy:

- **Constant Surveillance:** Apps can track your location, app usage, and browsing behavior in real-time, often without your consent. This leads to constant monitoring and surveillance of your digital life.
- **Data Brokers and Privacy Erosion:** The data collected via RTB is often shared with third-party data brokers, which can compile comprehensive profiles on users. These brokers sell your data to advertisers, governments, or other entities, further eroding your privacy.
- **Targeted Manipulation:** Data collected via RTB allows advertisers to create highly targeted, personalized ads. While this can improve ad relevance, it also enables advertisers (or political groups) to manipulate user behavior by delivering specific, emotionally charged content.



# Tips to Protect Yourself from Digital Surveillance



Fortunately, there are several steps you can take to protect yourself from digital surveillance:

- **Disable Location Tracking:** Turn off location services for apps that do not need it, and use a VPN to mask your IP address.
- **Block Ad Trackers:** Use privacy-focused browsers extensions. Disable advertising IDs on both Android and iOS. Tracker blocking from Apps and the web is also a default feature in /e/OS.
- **Minimize App Permissions:** Regularly review app permissions and revoke access to data that is unnecessary for the app's core functionality.
- Use as many as possible alternative apps to Google apps and services, in particular Gmail and Google search.
- **Use End-to-End Encryption:** Opt for messaging apps like Signal, Matrix/Element or Threema that offer end-to-end encryption, ensuring that your communications remain private, opt for email services that offer full end-to-end encryption such as ProtonMail.
- Consider switching to privacy-first mobiles like Murena smartphones running /e/OS, which are built to respect your privacy by avoiding Google's tracking mechanisms & ads tracking.

# Security is **NOT** Privacy!

In today's digital landscape, there is often confusion between security and privacy. While both are essential, they serve different purposes. Security focuses on protecting systems and data from unauthorized access, while privacy aims to limit the collection and sharing of personal data in the first place. A device can be secure and still compromise privacy, as security doesn't prevent data collection or surveillance by the system owner.

Google, for instance, frequently misleads users by marketing their security features as if they were privacy protections, creating the false impression that securing data from external threats means your personal information isn't being collected, monitored, or used for their own purposes.

Security, while essential, doesn't always equate to privacy: even the most secure devices can be compromised by sophisticated attacks, especially when the target is valuable. Many users fall into the trap of believing that security alone is enough. However, without strong privacy measures, like minimizing data collection in the first place, you could still be vulnerable to surveillance or breaches.


## How targeted users are being hacked, even with secured devices...

- **Pegasus Spyware on iPhones:** despite iPhones being considered very secure, spyware like Pegasus exploited vulnerabilities to hack high-profile targets, including a European President and activists, without user interaction.
- **Russian Intelligence Hacking Military Phones:** Ukrainian soldiers' smartphones were hacked by Russian intelligence during the Crimean conflict, allowing adversaries to track their movements and intercept communications despite the use of encrypted military-grade devices.
- **Criminal Networks and EncroChat:** encrypted phones used by criminal networks, like EncroChat, were hacked by European law enforcement, leading to the arrests of many criminals despite the phones being considered as "unhackable."

# How Murena and /e/OS Protects User Privacy

In contrast to the major mobile operating systems like Google's Android and Apple's iOS, /e/OS collects essentially no personal data from its users. As detailed in a research study, /e/OS stands out as the most privacy-respecting system among various Android-based platforms like Samsung, Xiaomi, and Huawei.

This lack of data collection provides users with confidence that their activities are not being monitored, making /e/OS one of the best choices for individuals who prioritize their privacy.

- 
- **No Data Sent to Google:** Unlike other Android variants, which constantly communicate with Google servers, /e/OS avoids any connection to Google services. This prevents the automatic collection of sensitive data like location history, search queries, and device usage.
  - **Minimal Data Collection:** /e/OS developers have designed the OS to function with almost no data transmission, even when the device is idle. There is no transmission of device identifiers, user interactions, or app usage data, which is a common practice in other Android variants.

# Conclusion

In today's digital world, our personal data is increasingly being harvested through mobile apps and web platforms. Major players like Google and Apple collect vast amounts of data from users, creating significant risks as users' behaviors and preferences are tracked and sold, often without their clear consent.

Google and Apple's business models heavily rely on extensive data collection. Mechanisms like RTB let advertisers access to user data. All this data is used to create comprehensive profiles, which can expose users to manipulation, breaches, and surveillance. Users are often unaware of the scale and depth of data collection happening behind the scenes.

For individual users, this leads to a loss of privacy, constant tracking, and even manipulation of their decisions through targeted advertising. Organizations, particularly those handling sensitive data, are also at risk. With vast amounts of data circulating, the potential for breaches increases, putting both users and companies in jeopardy.

There are several steps you can take to protect oneself from digital surveillance: using a Privacy-Focused Devices, disabling Location Tracking, using a VPN to mask one's IP address, blocking Ad trackers with web browser extensions, using as many as possible alternative apps to Google apps and services, and in particular avoiding Gmail and Google search.

Opting for secure messaging apps that offer end-to-end encryption, also ensure that communications remain private.

Murena smartphones running /e/OS are built to respect your privacy by avoiding Google's tracking mechanisms & ads tracking.

This streamlined, privacy-first solution offers a real alternative to the typical data-exploitative systems of today.