MAHARASHTRA CYBER

CCC_CA_2025_14

2025

04 June

YOUR DATA, YOUR CONTROL

MOBILE PRIVACY GUIDANCE

In an era where smartphones are deeply woven into our personal and professional lives, controlling how your data is accessed, shared, and stored is no longer optional—it's essential.

This advisory provides clear, actionable guidance on configuring mobile privacy settings to reduce digital exposure, prevent unwanted tracking, and protect sensitive information from misuse.

Whether you're a concerned user or a security professional, these best practices may help you take greater control of your mobile privacy—one setting at a time.

PUBLIC ADVISORY

PUBLIC ADVISORY

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Smartphones are powerful tools that connect us, organize our lives, and provide instant access to information. But with that convenience comes a hidden cost: our personal data.

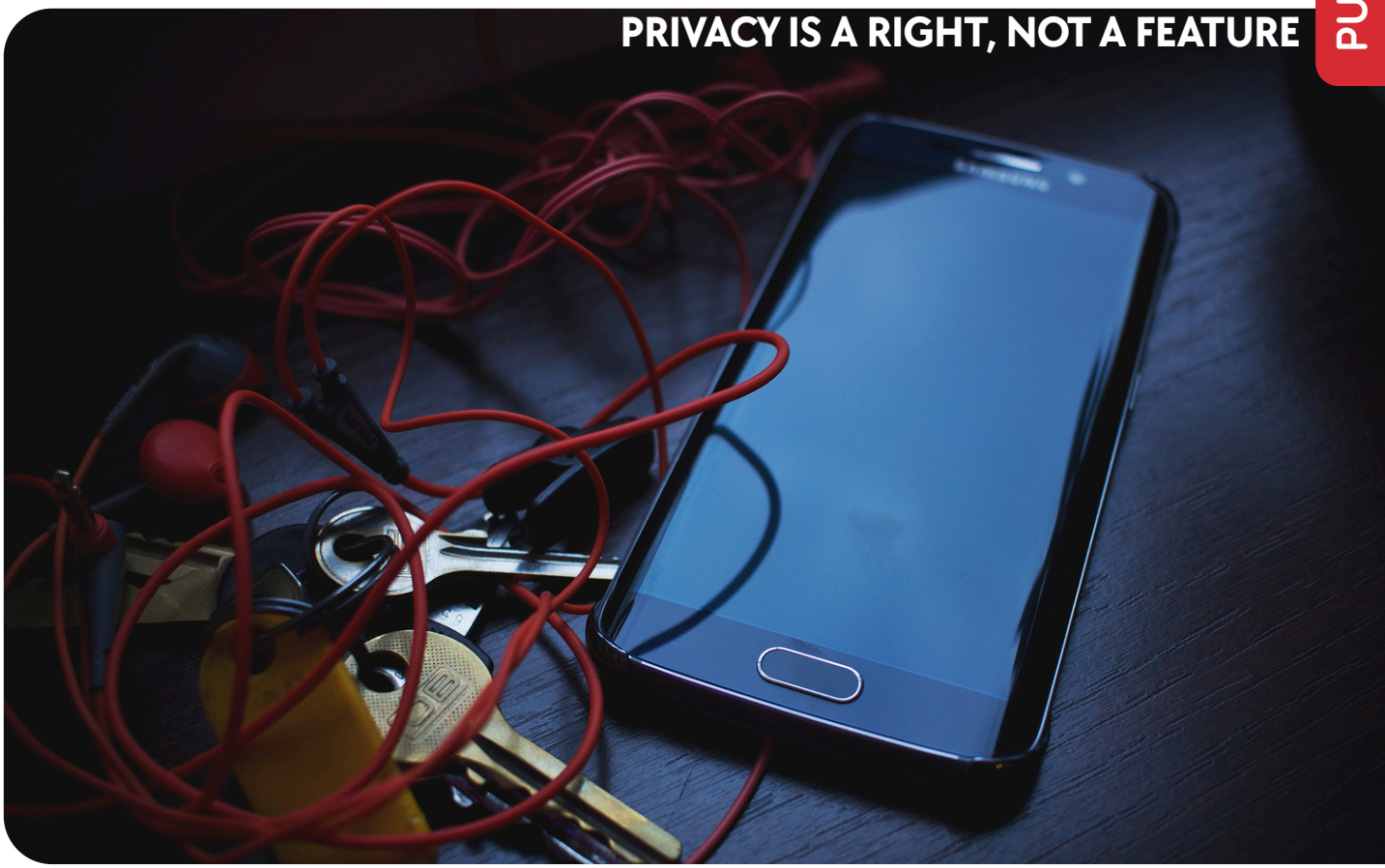
Every day, mobile apps and operating systems collect information about where we go, who we contact, what we browse, and even how we use our devices. While some of this data collection is necessary for functionality, much of it is excessive, poorly disclosed, and often shared with third parties—such as advertisers, data brokers, and analytics firms—without the user's informed consent.

This advisory was created to help everyday users understand and manage the privacy risks that come with using mobile devices. It provides clear, practical guidance on how to review and adjust key privacy settings, limit unnecessary data sharing, and make informed choices about the apps and services we rely on.

We break down the most common risks—like overreaching app permissions, location tracking, ad profiling, and cloud data exposure—and explain how to mitigate them using built-in tools available on both Android and iOS devices.

By following the simple steps in this guide, users may significantly reduce their digital footprint, reclaim control over personal information, and make their smartphones safer to use—without sacrificing essential functionality.

PUBLIC ADVISORY



INTRODUCTION

THE SMARTPHONE AS A DATA HUB

Smartphones are no longer just tools for calls and texts—they are mini-computers that manage everything from banking and social media to health data and home automation. As we rely on them more, they naturally accumulate a large amount of personal and behavioral information. This includes where we go (location history), who we communicate with (contacts and messages), what we search (browsing activity), and even how we move (sensor data). While this makes phones incredibly useful, it also turns them into rich targets for privacy intrusions.

HIDDEN DATA COLLECTION

What makes mobile privacy complex is that much of the data collection happens silently in the background. Apps frequently request access to cameras, microphones, storage, and other sensitive components—even when it's not essential to their functionality. Meanwhile, operating systems like Android and iOS collect usage data to "improve services," which can include sending analytics and diagnostics to third parties. Often, users agree to these permissions without realizing the scope or impact, making it difficult to maintain control over personal data.

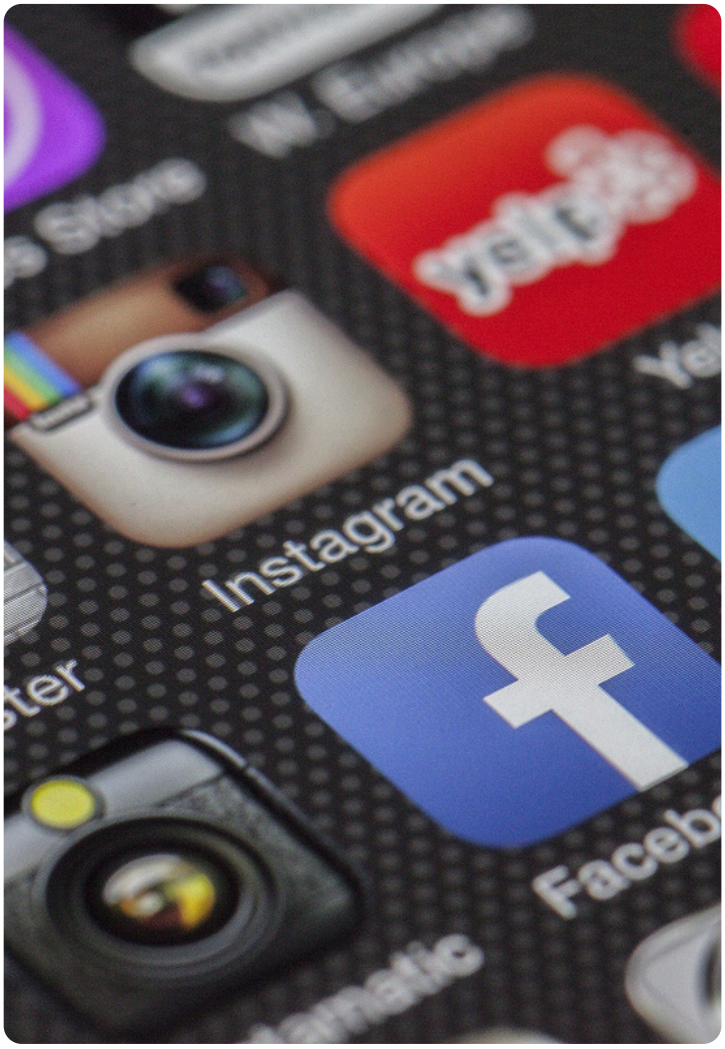
PUBLIC ADVISORY

EMPOWERING USERS THROUGH AWARENESS

The goal of this advisory is to empower everyday users to make smarter, safer choices when using mobile devices. By understanding where data is most vulnerable—and how to change the relevant settings—users can regain control over their personal information without giving up convenience. Whether you're a casual smartphone user or someone concerned about digital rights, the practical steps outlined here will help you reduce risks, avoid unnecessary data exposure, and create safer habits for mobile use.

A STEP TOWARD DIGITAL SELF-DEFENSE

Mobile privacy is not just a technical issue—it's a digital life skill. Just as we lock our homes and safeguard our wallets, it's important to secure the devices that hold our personal worlds. This advisory is designed to be simple, actionable, and accessible to all users, regardless of technical background. By taking small but meaningful actions, anyone can enhance their privacy and protect their digital identity in an increasingly connected world.



WHY MOBILE PRIVACY MATTERS

We use our smartphones for everything—messaging loved ones, managing finances, tracking fitness, browsing the web, and storing our most personal moments. But behind every tap and swipe, data is being collected. From apps and service providers to advertisers and data brokers, a long chain of entities can gain access to details about your behavior, interests, and even your physical movements.

For Example:

- A flashlight app might be **accessing your location.**
- A game may quietly upload your contact list to its servers.
- **Ad networks** could be tracking you across apps, learning your habits, likes, and routines.

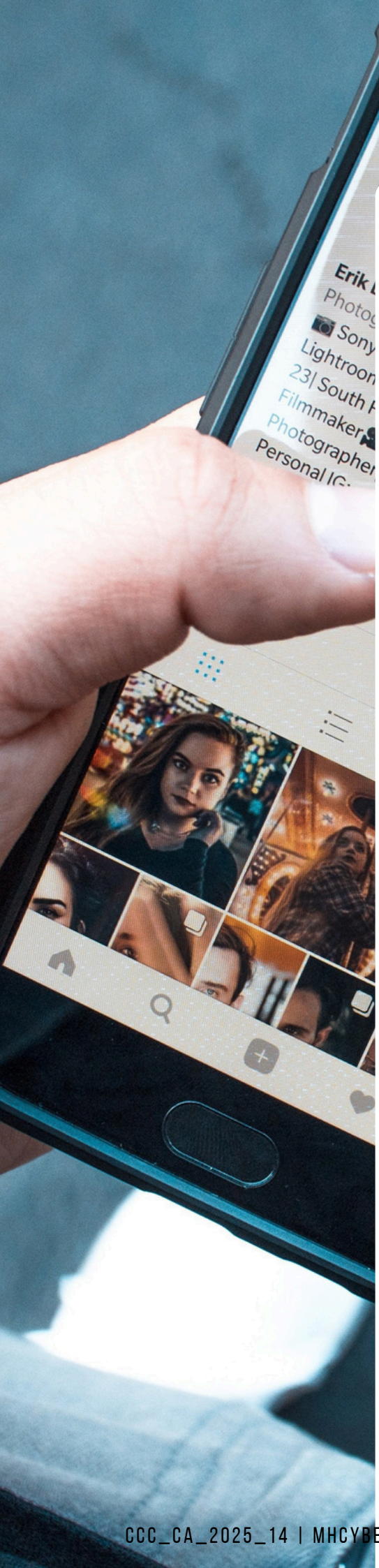
PUBLIC ADVISORY

This data doesn't just sit in one place—it can be bought, sold, or stolen. It can be used to target you with manipulative ads, inflate insurance costs, deny loans, or worse, enable identity theft and stalking. And unlike passwords, once your personal information is out, you can't just "reset" it.

Privacy isn't about hiding something wrong—it's about having control. It's about deciding who sees your information, how it's used, and when. Mobile privacy matters because your phone is not just a device; it's your digital self. Protecting it means protecting your identity, safety, and freedom in the digital age.

YOUR DATA MAKES OTHERS MONEY

Free apps profit by collecting and selling your data to advertisers and data brokers.



MANAGING PRIVACY RISKS

1 **OVER-PERMISSIONED APPS**

Many apps request access to features they don't need—like location, microphone, or contacts—leading to unnecessary data collection.

---

2 **LOCATION TRACKING**

Your phone constantly tracks your whereabouts through GPS, Wi-Fi, and Bluetooth, revealing patterns about your daily life—even when location sharing is turned off for apps.

---

3 **BACKGROUND DATA COLLECTION**

Many apps and services gather information like browsing history or app usage while running silently, without notifying you or offering clear options to limit this activity.

---

4 **AD TRACKING AND PROFILING**

Unique device IDs and trackers let advertisers follow your activity across apps and websites, creating detailed behavioral profiles used for personalized ads and content targeting.

---

5 **INSECURE CLOUD BACKUPS**

Automatic backups to cloud storage may include private data, like photos and messages, sometimes without strong encryption—making your information vulnerable to breaches or unauthorized access.

PUBLIC ADVISORY

6 UNSECURED NETWORKS

Public Wi-Fi and open Bluetooth connections can be exploited by attackers to intercept your data, install spyware, or gain unauthorized access to your device's resources.

7 METADATA EXPOSURE

Even if messages are encrypted, metadata like sender, time, and location can still reveal patterns that compromise your privacy or expose sensitive personal relationships.

8 HIDDEN THIRD-PARTY SDKS

Apps may include external software that collects your data for ads or analytics—often without clearly informing you or allowing you to opt out.

9 MICROPHONE & CAMERA ACCESS

Some apps can activate your microphone or camera in the background, capturing audio or video without permission and risking serious intrusion into your private moments.

10 OUTDATED SOFTWARE

Older operating systems and apps may lack recent security updates, leaving your phone exposed to known vulnerabilities that hackers and malicious apps can easily exploit.

PUBLIC ADVISORY

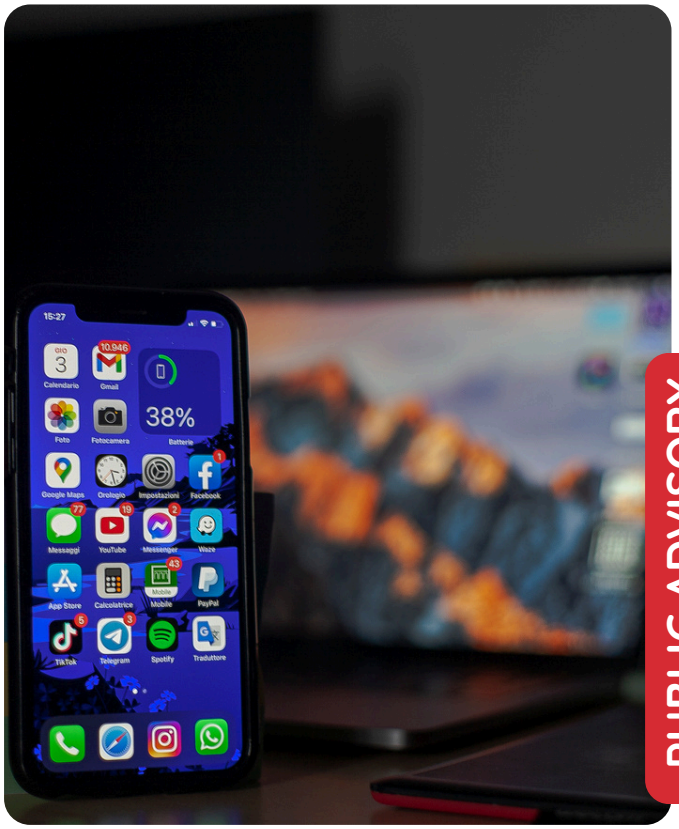
CONTROL APP ACCESS

CHECK PERMISSIONS OFTEN

Go to your phone's settings and review app permissions—especially for access to your location, camera, microphone, contacts, and storage. If an app doesn't need a permission to do its job (e.g., a photo editor asking for location), turn it off. This step alone can prevent silent data leaks.

ONLY WHILE USING THE APP

Instead of giving apps full-time access to sensitive features like location or microphone, choose "Only while using the app." This ensures apps can't track you when they're not open—helping you stay private without breaking functionality.



PUBLIC ADVISORY

NO TO BACKGROUND ACCESS

Many apps run or collect data in the background—even when you're not using them. Disable background data and location access unless the app truly needs it, like maps or fitness trackers. This not only boosts privacy but also improves battery life and device performance.

REMOVE WHAT YOU DON'T USE

Unused apps can still request updates, retain permissions, and collect data. If you haven't used an app in a while, delete it. Fewer apps mean fewer privacy risks and more control over your digital footprint.

MANAGING LOCATION & CONNECTIVITY

Your phone's connectivity—through GPS, Wi-Fi, Bluetooth, and mobile data—makes life easier but also exposes your location and behavior. These features can quietly broadcast your movements and connect to nearby networks or devices. To reduce tracking, turn off location services when not needed, and set app permissions to "Only While Using the App." Also, disable Wi-Fi and Bluetooth in public to prevent silent connections that may compromise your data.

Regularly check which apps have location access—many don't truly need it. Revoke permissions for games, photo apps, and others that don't rely on your whereabouts. Disable features like "Auto-Join Wi-Fi" and "Nearby Device Scanning" to avoid connecting to insecure or fake networks. A few quick settings adjustments can make a big difference in protecting your privacy.

09 / 10

MOBILE APPS

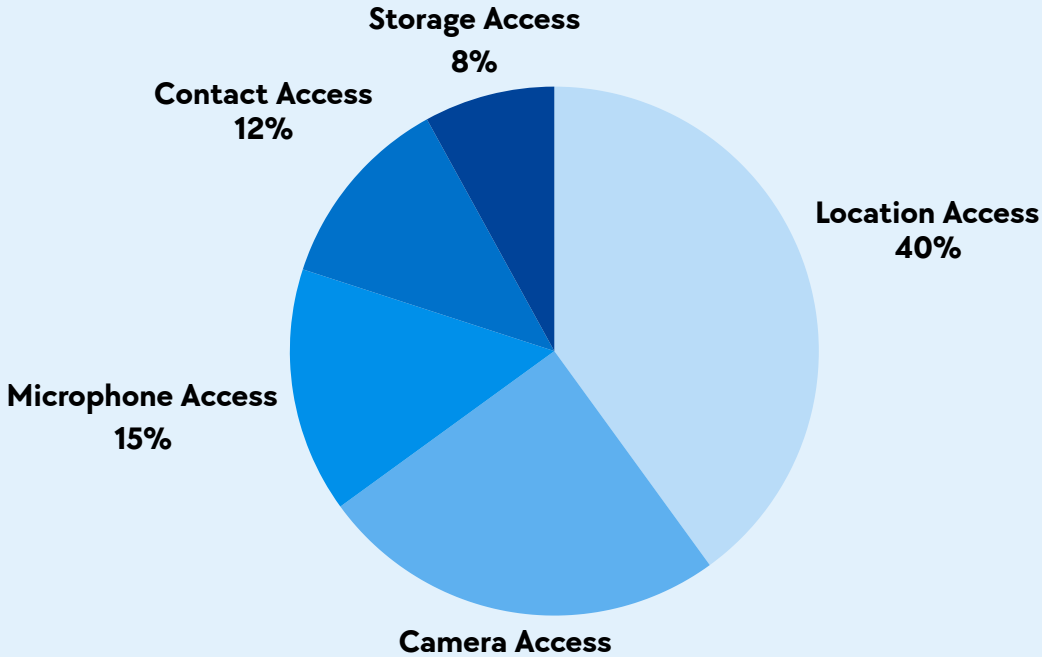
Collect your location data—even when it's not necessary for their main function—putting your privacy at risk without your clear knowledge.

70%

REDUCTION

Turning off Wi-Fi and Bluetooth when not in use can cut your tracking exposure by over 70%, helping protect your location and personal data.

TOP PERMISSIONS REQUESTED BY APPS

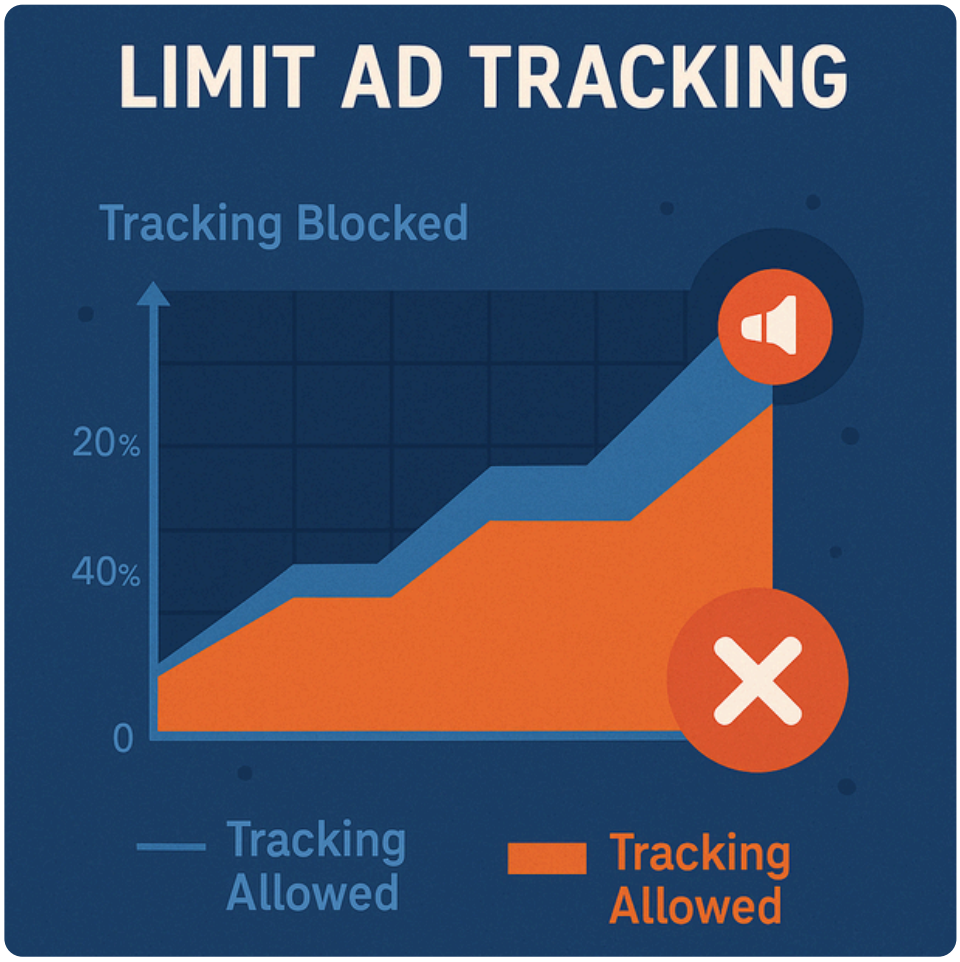


YOUR LOCATION, YOUR CALL — GRANT ACCESS SELECTIVELY

PUBLIC ADVISORY

LIMIT AD TRACKING

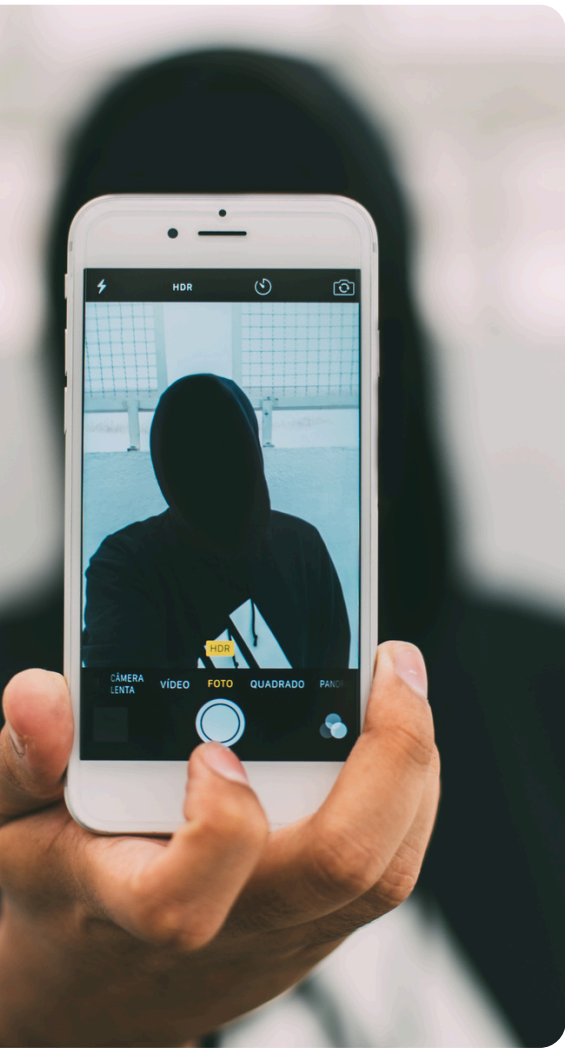
Your mobile activity fuels a constant stream of personalized ads—often at the expense of your privacy. Advertisers use device identifiers, browsing habits, app usage, and even location data to build detailed profiles about you. While you can't eliminate ad tracking completely, you can significantly reduce it by tweaking a few key settings.



This infographic shows how mobile ad tracking is managed, comparing tracking allowed vs. blocked over time. The growing blue area reflects increased privacy control by users. Icons highlight ad activity and blocking. The visual emphasizes that limiting tracking requires user action—like adjusting permissions—empowering individuals to protect their data and reduce unwanted tracking on their devices.

Reducing ad tracking not only enhances your privacy—it also declutters your digital space from overly targeted content. Take control of your advertising exposure, and ensure your data isn't being silently sold for clicks.

PUBLIC ADVISORY



PICK PRIVACY FRIENDLY APPS

Choosing apps that respect your privacy isn't just smart—it's essential. Did you know that over **80% of mobile apps request permissions unrelated to their core function?** Many collect your data silently, share it with third parties, or ask for access they don't really need. Before you tap "Install," take a moment to check the app's privacy policy and user reviews focused on data handling.

Luckily, both the **Apple App Store** and **Google Play** have stepped up: **70% of apps now include clear privacy labels and permission summaries** to help you make informed choices. Look for apps that are transparent about what data they collect and allow you to control permissions granularly. When possible, **opt for open-source apps or those endorsed by trusted privacy advocates**—your data will thank you!

PUBLIC ADVISORY

BROWSERS

Look for browsers that block trackers and ads by default, offer private browsing modes, and limit fingerprinting. These features help prevent companies from following you across the web.

MESSAGING

Choose messaging platforms that support end-to-end encryption, no cloud backups by default, and ephemeral messages. These ensure your conversations stay between you and your contacts.

EMAIL

Prefer email providers that use built-in encryption, zero-access architecture, and metadata protection. This helps keep both your messages and identity private.

PASSWORDS

Select tools that are open source, support two-factor authentication, and use local encryption of your credentials before cloud sync.

EVERYDAY PRIVACY TIPS

LOCK YOUR DEVICE

Set a strong passcode or use biometric locks like fingerprint or facial recognition. This simple step protects your phone and personal data from unauthorized access, keeping your information secure even if your device gets lost or stolen.

BE CAREFUL WHAT YOU TAP

Download apps only from trusted sources like official app stores. Avoid clicking on suspicious links or attachments, especially from unknown contacts, to prevent malware infections and phishing attacks that can compromise your personal information and device security.

PUBLIC ADVISORY

MANAGE YOUR APP PERMISSIONS

Review which apps have access to sensitive features like location, contacts, camera, and microphone. Remove permissions for apps you don't use or trust. This limits unnecessary data sharing and helps protect your privacy from unwanted tracking or data leaks.

TURN OFF AUTOMATIC CONNECTIONS

Disable automatic Wi-Fi and Bluetooth connections to unknown networks and devices. This prevents your phone from connecting to insecure or malicious sources without your knowledge, reducing the risk of data interception or hacking while you're on the go.

RECOMMENDATIONS

LOCK IT LIKE YOU MEAN IT

A simple passcode isn't enough anymore. Use biometrics (like fingerprint or face unlock) and enable two-factor authentication for your important accounts. It's like adding a deadbolt to your digital door.

PERMISSIONS AREN'T JUST FORMALITIES

Every time an app asks for your location, mic, or camera — it's asking for access to you. Say no when it's not essential. Check your app permissions regularly and cut off the snoopers.

DON'T TRUST THE NETWORK

Public Wi-Fi is convenient, but also risky. Use a VPN to encrypt your connection and stay invisible to cyber snoops. If it's not your network, don't let it see your secrets.

REFERENCES

GOOGLE - ANDROID HELP SUPPORT
https://support.google.com/android/answer/13985942?hl=en

ELECTRONIC FRONTIER FOUNDATION
https://ssd.eff.org/module/how-to-get-to-know-android-privacy-and-security-settings

THE NEW YORK TIMES
https://www.nytimes.com/wirecutter/guides/privacy-tips-for-android-phone/

SAMSUNG - HELP
https://www.samsung.com/us/support/answer/ANS10002544/

THE NEW YORK TIMES
https://www.nytimes.com/wirecutter/guides/privacy-tips-for-android-phone/

NEW JERSEY STATE WEBSITE
https://www.cyber.nj.gov/guidance-and-best-practices/device-security/guide-to-accessing-your-android-device-s-security-privacy-settings

APPLE - HELP
https://www.apple.com/privacy/

Call 1945

mhcyber.gov.in