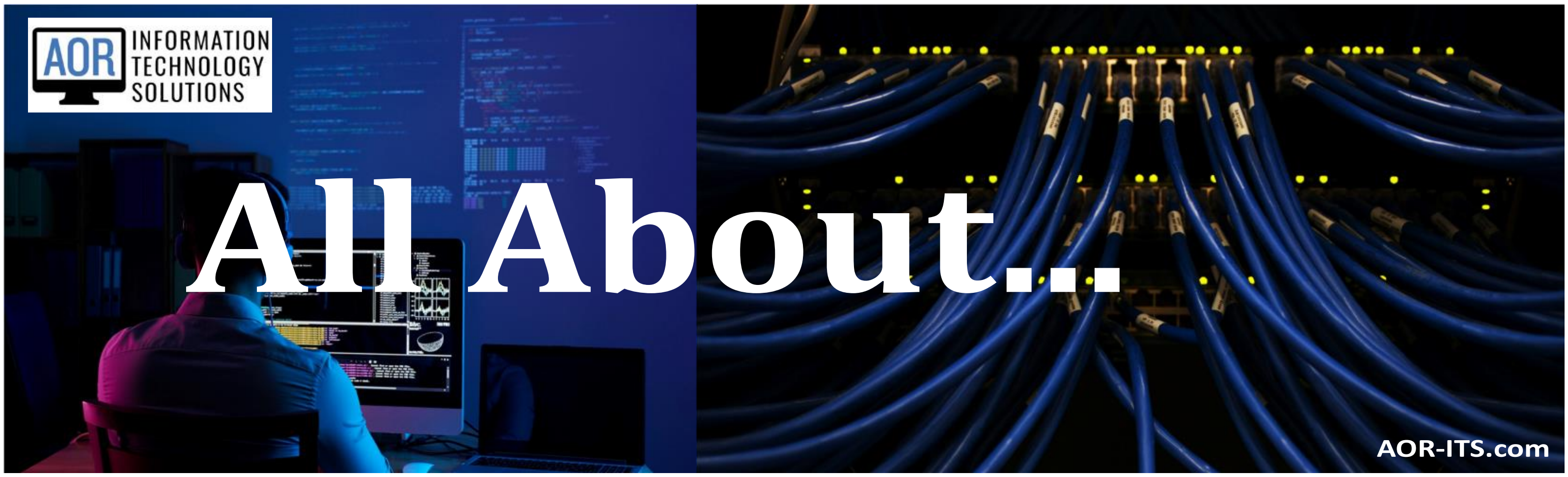

6 Ways Your Phone Is Tracking You

Have you ever casually talked about a product or service while your phone was nearby and then suddenly started seeing ads for it on your social media feed? Your phone is listening. If that concerns you, this should really worry you: your devices are tracking you too! From the phone itself to the apps you download and access, there are multiple ways that your device can ping your location.

Luckily, there are ways around allowing your phone to spy on you. In today's article we'll share why it's so dangerous, the top six ways your phone is tracking you and how you can shut it down.

Why Is It Dangerous?

This data is a hot commodity for Internet marketers. The collected data is used to target you with the local and interest-based ads you're most likely to be interested in. This digital "stalking" is legal as long as they give you the option to opt in or out. However, marketing execs aren't the only ones interested in your data. Cybercriminals are too. Here are the reasons allowing your phone to track you is a no-go:

1. Privacy Invasion: Phone tracking allows apps, websites and third parties to collect extensive information about your location, habits and behaviors without your full knowledge. This constant surveillance can lead to a significant invasion of privacy, making users vulnerable to targeted advertising, data harvesting or even malicious tracking for more harmful purposes.

2. Identity Theft and Fraud: If your phone's tracking data falls into the wrong hands – such as hackers or cybercriminals – it can be used to gather personal details and patterns. This data can enable identity theft, financial fraud or unauthorized access to sensitive accounts, causing financial and emotional harm.

3. Physical Security Risks: By sharing your real-time location data, phone tracking can expose you to physical security threats. For example, stalkers or criminals can exploit this information to track your whereabouts, compromising your safety. Publicizing your movements can also make it easier for bad actors to predict your routines or target you when you're most vulnerable.

How Your Phone Is Tracking You

1. Location Services: Your phone's GPS and location services track your whereabouts in real time, recording where you are and how long you stay there. Using "Frequent Locations," your phone makes assumptions about where you work and live based on when you visit and how long you stay. While this is helpful for finding directions or nearby restaurants, constant tracking can also reveal your movement patterns, leaving you vulnerable to privacy invasion.

Both Apple and Android give you the option to turn this feature off. Exact instructions will vary by specific model and operating system; however, here are basic instructions:

How to turn it off:

iPhone: Go to Settings > Privacy & Security > Location Services. Toggle off Location Services or manage individual app permissions. Scroll down to System Services. Select Significant Locations to see the logged record of where you've been and toggle it off. You can also clear your history by clicking Clear History.

Android: Go to Settings > Location > App Permissions, and either disable location tracking for specific apps or turn off Use Location To delete your device's location history, tap Delete Location History at the bottom of the screen under Location History.

2. App Permissions: Many apps request access to your contacts, photos, microphone and camera, allowing them to track your activity, even when you're not actively using the app, and collect more information than necessary. You can adjust this and should review it regularly to make sure you aren't compromising your privacy.

How to turn it off:

iPhone: Go to Settings > Privacy & Security. From there, check categories like Camera, Microphone and Contacts to review and adjust app permissions.

Android: Go to Settings > Apps > Permissions. Here you can manage which apps have access to sensitive data like contacts, microphone and camera.

3. Wi-Fi and Bluetooth Connections: Your phone constantly scans for Wi-Fi and Bluetooth connections, allowing third parties to track your location based on the networks and devices you've interacted with.

How to turn it off:

iPhone: Swipe down from the top-right corner of the screen and toggle off Wi-Fi and Bluetooth. For full control, go to Settings > Wi-Fi & Bluetooth to disable scanning.

Android: Go to Settings > Location > Wi-Fi & Bluetooth Disable these options to prevent your phone from constantly searching for networks and devices.

4. Browsing Activity: Web browsers and apps monitor your search history and the websites you visit. This data is used to build profiles about your preferences, feeding you targeted ads and potentially selling your behavior patterns to third parties.

How to turn it off:

iPhone & Android: Use your browser's private or incognito mode for safer browsing. In Google Chrome, go to Settings > Privacy & Security and turn off Web & App Activity. Additionally, clear your browsing history and cookies regularly.

5. Ad Tracking: Your phone assigns you a unique advertising ID that companies use to track your behavior across apps and websites. This ID follows your activity, providing advertisers with insight into your interests to serve personalized ads.

How to turn it off:

iPhone: Go to Settings > Privacy & Security > Tracking and toggle off Allow Apps to Request to Track. You can also go to Settings > Privacy & Security > Apple Advertising to disable personalized ads. *This does not mean you won't still see ads; you just won't see personalized ads.

Android: Go to Settings > Privacy > Ads, then toggle on opt out of Ads Personalization.

6. Social Media and Search Engines: Platforms like Facebook, Instagram and Google track your online interactions, searches and location to create detailed profiles of your habits and interests. They use this data for advertising and content recommendations, which can feel invasive.

How to turn it off:

Social Media: Go to each platform's settings (e.g., Facebook > Settings & Privacy > Privacy Shortcuts) to review what data is being collected and manage ad preferences.

Google: Go to Google Account > Data & Privacy > Web & App Activity to control how Google tracks your search and activity history. You can also adjust Ad Settings to limit ad tracking.

By adjusting these settings, you can significantly reduce the amount of personal information your phone tracks, giving you more control over your privacy.

Why This Matters for Business Owners:

For a business owner, protecting your personal privacy is just as crucial as securing your company's sensitive information. The same tracking methods that follow your every move can also expose your business to risks. Hackers, cybercriminals and even competitors can exploit these vulnerabilities to gather valuable data about your business activities, customer interactions and confidential communications.

By taking steps to limit how your phone tracks you and adjusting your privacy settings, you're not just protecting yourself – you're also safeguarding your business from potential data breaches, identity theft and targeted cyber-attacks. In today's world, cybersecurity isn't just a technical issue, it's a strategic one, and staying ahead of threats starts with being informed and proactive.

If you're concerned about your business's overall security, don't wait for a problem to occur. **Schedule a FREE Security Risk Assessment with our team today,** and let's ensure your entire network is protected from top to bottom. Our experts will identify vulnerabilities and recommend tailored solutions to keep your business safe.

To get started, give us a call at 215-769-9980 or click here to book now.