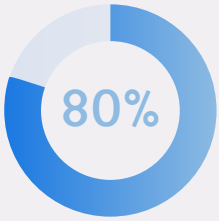
TRUSTED FUTURE

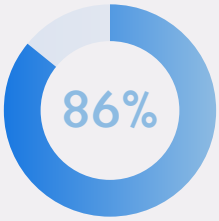
PRIVACY TIPS

5 KEY STEPS YOU CAN TAKE RIGHT NOW TO STOP YOUR MOBILE ACTIVITY FROM BEING TRACKED

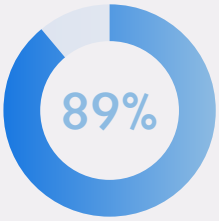
In recent months, Trusted Future has conducted extensive public opinion research which found consumers are very concerned about the ways their activity may be being tracked online.



of smartphone users are choosing not to be tracked.



are concerned apps are tracking their behavior across other apps, websites, and devices.



are concerned about their data being shared with third parties.

Consumers often want to know more about how their data is being tracked, and what they could do to control and prevent it. Trusted Future has put together the following explainer and set of consumer tips to help people take back control of their privacy – beginning with something called the device advertising identifier which is at the heart of mobile data tracking, and the multi-billion dollar data broker industry built around it to track, sell, and manipulate your data.

How do advertisers and third parties track my mobile behavior? Device advertising identifiers enable third parties to persistently track you, enable data brokers to link and combine disparate sources of data about you to create detailed profiles, and have led to some egregious privacy violations. When combined with location data, device advertising ID data can reveal some of the most intimate details of a person's life – tracking your activities across the web, across town, and throughout your day.

How has user device tracking been used or misused? There are plenty of examples of ways data tied to an advertising ID can be used and misused. For example, it has allowed people to identify whether someone visited a planned parenthood facility, attended weight watcher meetings, had one night stands, to track a presidential security detail, or who and what kind of people you might date. Trackers are commonplace, and can be found in two-thirds of the most popular apps used by children, in popular dating apps, prayer apps, period tracking apps, and abused by ride-sharing apps.

Some apps gather users' location information even if it is not necessary for the services the app is designed to provide, for example a flashlight app collected user location data along with the device's unique advertising ID to pass along to third parties. This data collection is at the front end of a multi-billion dollar advertising and data aggregation industry built around data about you.

What exactly is an Advertising Identifier? An Advertising ID or IDFA is the unique device identifier that enables marketers to track users as they move between apps. This is the identifier that allows third party marketers to see what you may be searching for on Amazon, and then seeing the same or similar products in other apps like Instagram or Facebook. But it is also used by third party data brokers where they can combine the unique advertising ID information with other information about you – location data, age, marital status, and proclivities – to create a substantially more detailed profile about you. What can I do to prevent my activity from being tracked? Restricting these advertising identifiers is an important first step and can make it harder for data brokers and advertisers to track you, to create detailed profiles of who you are and what you do, and can help limit the amount of personal information about that is sold. The good news is, there are some powerful tools you may already have on your smartphone to help you take greater control over your privacy.

01

TURN OFF THE ADVERTISING IDENTIFIER TRACKING ON YOUR PHONE.

- **On Apple:** Beginning with iOS 14.5 and later, Apple introduced a powerful new feature that lets you choose whether or not an app can track you by requiring apps to ask for permission when you install a new app – the "Ask App Not to Track" feature. Apple's instructions here for managing activity tracking permissions which can, for example, allow you to ask all apps that you previously allowed to track your activity to stop.
- **On Android:** Beginning with Android 12, Google also began enabling users to opt out of sharing their Advertiser ID by giving users the option to delete the advertising identifier on their Android phones. Tutorial here.
- Preventing advertiser tracking of users has turned out to be wildly popular with consumers (about 8 out of 10 iOS users choose not to be tracked globally) and it has already created waves in the $189 billion mobile advertising industry.

02

LIMIT LOCATION TRACKING. Your location is yours to protect. Some apps may have access to your device's location services. For apps that require location, you may want to consider limiting it to only the times that you are using the app. See these simple steps for how to prevent your location data from being shared when and with apps you don't want it.

03

EXAMINE PRIVACY NUTRITION LABELS. If you want to see what data apps are collecting about you and why, or if you are concerned about sensitive personal data, such as the data collected while using a period tracking app, now there is a way for you to easily examine what Information is being collected about you. Beginning in December 2020, Apple launched a new Privacy Nutrition Label feature built into its app store to allow users to carefully examine an app's data collection practices. For each app, it outlines what data may be used to track you across different apps and websites owned by other companies, describes the data that may be collected and linked to your identity, and how the data may be used. In 2022, Google Android similarly launched a new Google Play Data safety section in its app store to similarly give users a simple and clear way to understand the data that an app collects, if and how it is shared with third parties, as well as information about the app's security practices.

04

USE END-TO-END ENCRYPTION. Android and iOS devices have full-disk encryption on by default, and you should double-check the setting. Doing the same for other devices like your laptop or computer can be important too. In addition, you can use a messaging service that takes advantage of end-to-end encryption to protect your privacy like iOS which ensures messages are encrypted on your device, so they can't be accessed in transit or on your device without your passcode. Other popular encrypted messaging apps include Signal, Telegram, and WhatsApp. Again, it's important to review an app's privacy nutrition label in their app store before installing.

05

ONLY DOWNLOAD FROM OFFICIAL APP STORES. The Federal Trade Commission's recommendation for protecting mobile privacy starts with this tip: "Use official app stores. To reduce the risk of installing potentially harmful apps, download apps only from official app stores, such as your device's manufacturer or operating system app store. Also, research the developer before installing an app."

TRUSTED FUTURE

trustedfuture.org