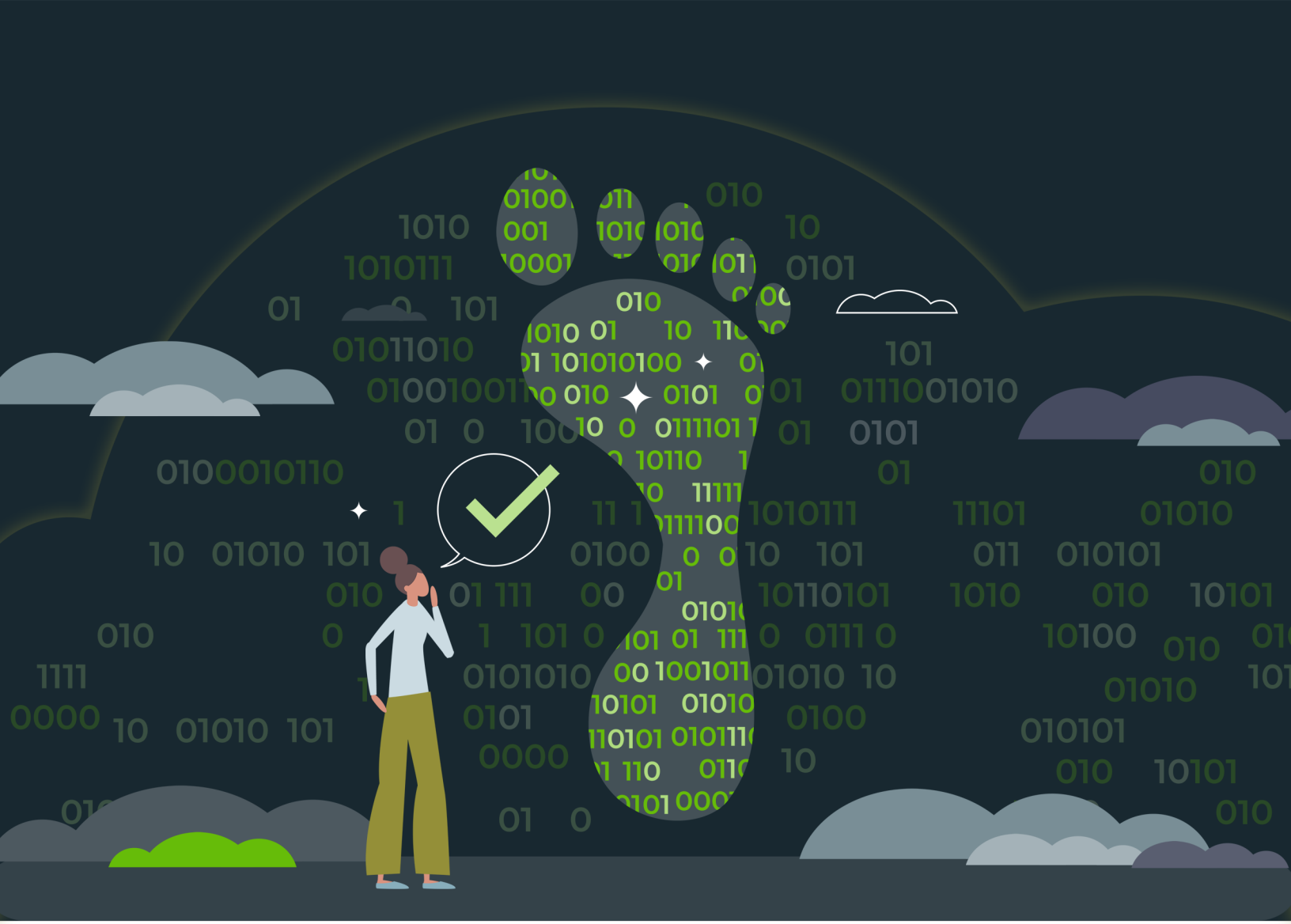


Protect Your Digital Privacy

Follow these tips to help reduce your digital footprint and prevent the disclosure of sensitive and personal information to third parties.

Information from various sources could be combined to create a very detailed picture of the locations you visit in person, online searches you perform, and numerous other pieces of sensitive and personal information that you may not wish to be disclosed.

Anytime you use an app on your phone or install a new app, you should be aware of what permissions the app is requesting and decide whether to grant the app access to your information.

You can take the following steps to protect your sensitive and personal information from disclosure to any third parties who do not need this information or may even seek to use this information against you.

Please keep in mind that this is not an exhaustive list of entities that may have sensitive data about your activities and locations. For example, your financial institutions and ride share companies also may have sensitive data about you.

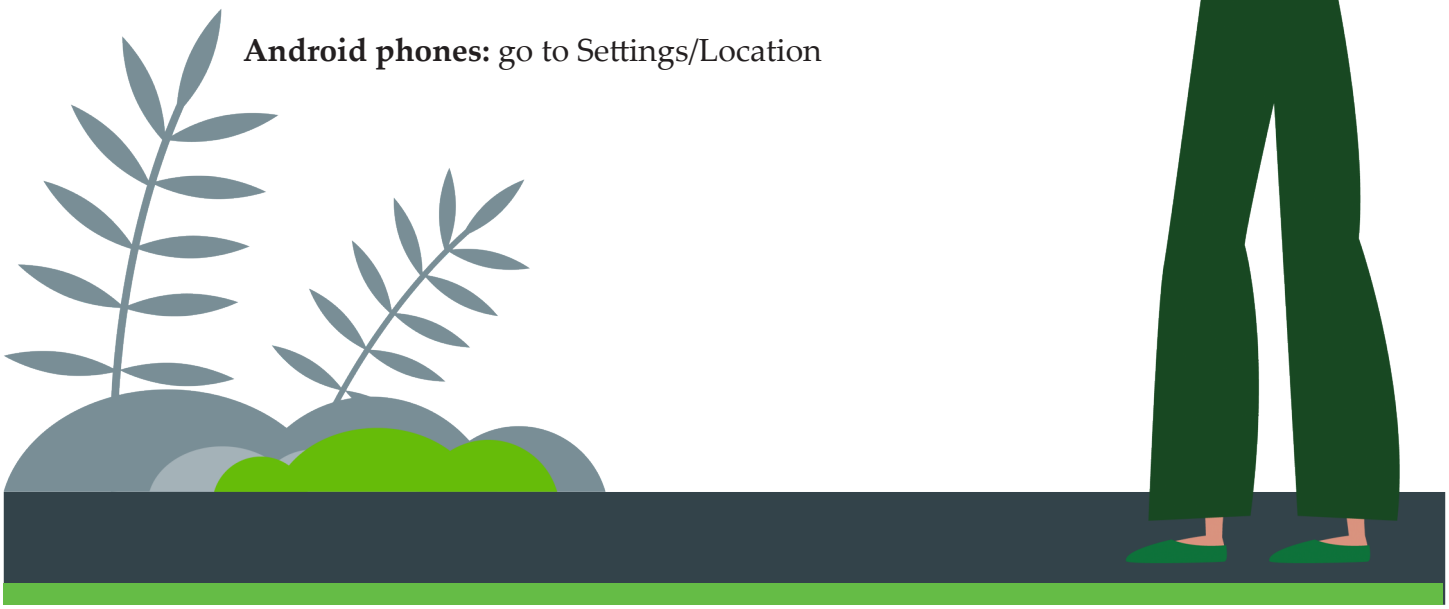
Tips to protect your digital privacy:

Turn off location services on your wireless phone - Avoid giving any app permission to access your device's location data. Many of the apps that resell data to data brokers don't need your location information.

To visit a place without revealing your location, you should turn off location services on your phone to prevent your phone from transmitting your location.

Apple iPhones: go to Settings/Privacy/Location Services/Tracking

Android phones: go to Settings/Location



*Adjusting privacy settings may reduce device and/or App functionality.

Turn off ad personalization on your phone - Some companies access your search history, sites visited, apps used, location, and other data, and then use that information to determine which ads to display on your phone. To turn off ad personalization:

Apple iPhones: go to Settings/Privacy/Apple Advertising

Android phones: go to Settings/Google services/Ads/Reset advertising ID to disable personalized ads

Adjust your online privacy settings - In addition to your phone tracking your location, be aware that search engines and map providers that you use may track your location. You can limit this additional form of location tracking by changing privacy settings within your accounts with those services.

For more specifics and instructions for Apple iPhone and Android phones, go to www.support.google.com and search "Managing Location History."

Do not share sensitive personal information on social media - Be aware that information you post on your social media pages could be publicly available if you do not limit sharing, or if one of your social media friends discloses the information.

Consider refraining from posting anything on social media while visiting personal or private locations – Even if your location tracking is turned off, social media postings and tags associated with a business could be combined with your search history to create a profile that might unintentionally share more information than desired.

Use encrypted messaging instead of unprotected SMS text messages - Encrypted messages are designed to allow only the intended recipient to read the message and prevent the contents of the message from being intercepted by any third parties.

*Adjusting privacy settings may reduce device and/or App functionality.

Protect your online search history. First log out of open accounts, use a private web browser and the Do Not Track option, or set up a VPN -

- Make sure to log out of social media accounts, email, and tech platforms before conducting your search.

- If you are researching on your phone, computer, or other device, consider using a private web browser that does not save your search history and blocks web trackers.

- Use the Private Mode setting in your browser. Private Mode means that the browser will not collect and store your online searches.

Google Chrome/Incognito	Microsoft Edge/In Private
Mozilla Firefox/Private Browsing	Safari/Private Window

- Always select the Do Not Track option under your browser privacy settings on your phone, computer, or other device. The Do Not Track option requests that any website you visit does not use their tracking cookies. However, these requests do not have to be honored.

- Consider using a Virtual Private Network or VPN to access the internet from your phone, computer, or other device. It provides an IP address (the digital identification label for your device) that is different from your actual IP address. That means that if a third party is trying to track your location, they will not be able to determine your location based on the IP address associated with your browsing session.

- To use a VPN, first download a VPN (paid or free) program or app on your selected device. You will then need to activate the VPN before taking any actions you wish to remain private and anonymous.

If you have questions or concerns about your privacy,
please contact our office by completing a consumer complaint form online at
www.IllinoisAttorneyGeneral.gov or by calling
1-800-386-5438 (Chicago) • 1-800-243-0618 (Springfield) • 1-800-243-0607 (Carbondale).

KWAME RAOUL
ILLINOIS ATTORNEY GENERAL

*Adjusting privacy settings may reduce device and/or App functionality.