Location, Location, Location

Tips on Controlling Mobile Tracking

Consumer Information Sheet 18 • October 2015

We live in a digital world. We also live in a physical world. Those two worlds meet in "location services" on our smartphones, tablets and other mobile devices. Location is the magic that gives us maps when we are lost and the closest tacos when we are hungry. ***Watch out****. Some apps can access your location all the time, even when you're not using them. Your location might be "always on."*

You can protect your location information where it lives – on your smartphone or tablet, in your apps and in your email. With some good digital habits, you can enjoy the perks of location services and protect your privacy at the same time.

Smartphones and Tablets

Your smartphone's geographic information comes from GPS, WiFi, and cell-tower networks. It informs a few things on your phone - not just apps. How mobile location services work may be technical, but you do not have to be an engineer to have more control. By adjusting the settings on your mobile device, you can control location services.

Your smartphone's location service, for example, is responsible for "geo-tagging" your photos. When you take a photo with your phone, the phone's location goes into the image file, along with the date/time stamp. When you post that photo, you are revealing (to anyone who really wants to know) when and where you took it. Unchecked geo-tagging can be dangerous, especially for victims of stalking or domestic violence.

Your smartphone also records your location history: where you and your phone have gone. Deep in your device's settings, there is a list and map of your frequently visited locations.

Here's how you can use system tools to control location information on your mobile device.

Android Phones and Devices

Android

- Go to Settings, then Permissions, then Location and turn it off. When an app asks for access to your location, you can choose to grant it or not.
- To disable geo-tagging of photos, open the camera and then click on the gear icon and set location to "No." You may have to click the gear icon on several screen layers.
- You can also choose how accurate you want your location reporting to be (with Location services On).
  - High accuracy mode uses GPS, WiFi, and cellular networks and provides the highest location accuracy and speed, and uses more battery.
  - Battery saving mode uses WiFi and cellular networks to estimate your location, which require less battery. You give up some accuracy and some speed when you select this mode.
  - Device only mode uses only GPS and provides less accurate location information, and uses more battery than the battery saving mode. This is the most location privacy protective and provides a degree of accuracy that is fine for many uses.
- To disable location history, go to Google Settings, then Location, then Location History. You can turn Location History off for your device or for your Google Account. You can also delete your entire history or parts of it.

iPhones and iPads (iOS 6 and later)

iOS

- Go to Settings, then Privacy, then Location Services. You can turn it off. Alternatively, you can choose which functions and apps to give access to your location.
- To disable geo-tagging of photos, deny location access to the camera, in Location Services.
- To disable location history, go to Settings, then Privacy, then Location Services, then System Services, then Frequent Locations. Deselect Frequent Locations by sliding the tab.

Mobile Apps

Some apps ask for your consent before using your location data. When a permission screen pops up, ask yourself if your location is essential to the app's function (a mapping app). If you think that it is not (a flashlight app), you can deny it. For some apps, access to location information can only be controlled through the device's operating system.

Some apps track your location when they are not in use. This is known as "running in the background." You can disable this feature on Android and iOS.

Android Phones and Devices

- On Android devices, you have two choices for apps that want access to your location data – on or off. You can turn off location for all of the apps on your device, but not selectively for a given app. To do this, go to Settings, then Permissions, then Location and turn it off.
- For maximum privacy, you can make a habit of turning off location in the operating system, and turning it on only when you want to use an app that needs it.

To prevent apps on Android from running in the background:

- On the Settings screen, select Apps.
- Select the app in the list that you want to close or stop and touch it.
- The App info screen displays. Touch the Force stop button to force the app to stop running.
- A confirmation dialog box displays making sure you really want to force the app to stop. Touch OK to stop the app.
- You are returned to the App info screen and the Force stop button is grayed out now that the program has stopped running.

iPhones and iPads (iOS 6 and later)

On iOS devices, you are asked you for permission to use location information when an app first needs it. iOS will ask you to grant or deny access to location at that point.

You can also make decisions for each app's access to location information in Settings.

- Go to Settings, then Privacy, then Location Services.
- There you can selectively choose to allow or deny each app to access various functions and types of data on the device, including location information.
- You can change your mind and change the setting at any time.

To prevent apps on IOS from running in the background:

- Go to Settings, then General, then Background App Refresh.
- Choose which apps to allow or deny permission to refresh in the background. Not allowing this will save battery life, as well as prevent apps from accessing your location info in the background.

Email

Email location tracking works primarily through tiny “pixels” hidden in images and graphics. The prettier the email, the more likely it has tracking pixels. When you open an email and select “download image” or click on an image in the email, a hidden email pixel may transmit certain information on you back to the sender.

Email tracking allows the sender to know when an email has been opened and the location, at varying degrees of specificity, of the recipient. Email tracking is a tool used by businesses, employers, and other organizations. Your location may be used to send “more relevant” ads to you. This tool can also pose dangers to victims of domestic violence or stalking.

There are things you can do to prevent this type of email tracking on your mobile device.

Gmail on an Android Device

- In the Gmail app, touch the Gmail icon,then Settings.
- Choose your account.
- Touch Images.
- Choose “Ask before showing.”
- To view images in a message, touch “Show pictures” above the message.

Android

To block email tracking for Gmail on iOS devices and for Yahoo and Outlook on any mobile device, you must change settings through a browser on your mobile device or desktop:

Gmail on an iOS Device

- Open Gmail on a computer.
- At the top right, click the gear icon.
- Select Settings, scroll down to Images (stay in the “General” tab).
- Choose “Ask before displaying external images.”
- Click “Save Changes” at the bottom of the page.

To see images in a message, click “Display images below” in the box near the top of your message. To allow images from specific senders, click “Always display images from *sender@domain.com*” in the box above your message. To block images from a particular sender, open a message from that sender, click the show details icon below the sender’s name, and click “Don’t display from now on.”

iOS

Outlook Mail on any Device

- To disable HTML, which allows tracking pixels, for creating messages go to Tools, then Options, then Mail format.
- In "Compose in this message format," set to "plain text."
- To disable HTML for incoming messages, go to Tools, then Trust Center.
- Select "Read all standard email in plain text."

Yahoo Mail on any Device

- Click the Settings icon, then Settings, then Security.
- Locate "Show images in email" and select "Never by Default"

Finally, you can install protective or counter measure software on your device.

There are also tools you can buy for a small fee that offer email tracking protection. Such programs include add-ons to browsers to block trackers and mask email, tools that warn when an email has a tracker in it and tools that can block pixels even if you have already opened an email with location tracking. Search for terms such as "email pixel blockers" and look for product reviews.

[Note that the developers of mobile operating systems change their configurations from time to time. You may have to use a search engine to find updated directions for the controls described above.]

More Information

"A Parents' Guide to Mobile Phones," ConnectSafely.org, at *www.connectsafely.org/wp-content/uploads/mobile_english.pdf*

"Choose Whether to Show Images," in Gmail Help, at *www.support.google.com/mail/answer/145919?hl=en*

Getting Smart About Smartphones: Tips for Consumers, California Attorney General, at *www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/smartphones_consumers.pdf?*

Getting Smart About Smartphones: Tips for Parents, California Attorney General, at *www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/smartphones_parents.pdf?*

"Turn Off Gmail's Auto Image Loading to Keep Email Snoops at Bay," *Wired.com*. Condé Nast Digital, at *www.wired.com/2013/12/turn-gmail-auto-image-loading-off/*

Murphy, Kate. "Ways to Avoid Email Tracking," *The New York Times*, 24 Dec. 2014. Web. 16 June 2015, at *www.nytimes.com/2014/12/25/technology/personaltech/ways-to-avoid-email-tracking.html?_r=0*

This fact sheet is for informational purposes and should not be construed as legal advice or as policy of the State of California. If you want advice on a particular case, you should consult an attorney or other expert. The fact sheet may be copied, if (1) the meaning of the copied text is not changed or misrepresented, (2) credit is given to the California Department of Justice, and (3) all copies are distributed free of charge.