iPhone Privacy Settings

Prepared for the ***Alameda MUG*** & ***iPhone Without Tears*** classes

Privacy is Not Security

Privacy and Security are often confused. Privacy has to do with information about you and your iPhone that can be viewed and used by others based on your iPhone's settings. This includes information about your Contacts, Location data, and browser history that could be captured and shared with others.

Security, on the other hand, concerns how to carefully store and protect information which could have an impact on your finances, digital records, and even your safety.

In this document we will discuss only Privacy Settings for your iPhone, and why it is important that you make informed Privacy Settings choices.

iPhone Settings for Privacy

All of the major iPhone Settings which affect Privacy are located within the Settings app. You have to scroll down the first screen of Settings to the section which begin with General. Privacy is the last item in that section.

When you click on this Privacy section, a long list of items appears on the next screen which let you control which parts of your operating system can be read by each of the apps on your phone, and by those apps' developers and distributors.

Prepared February 2020

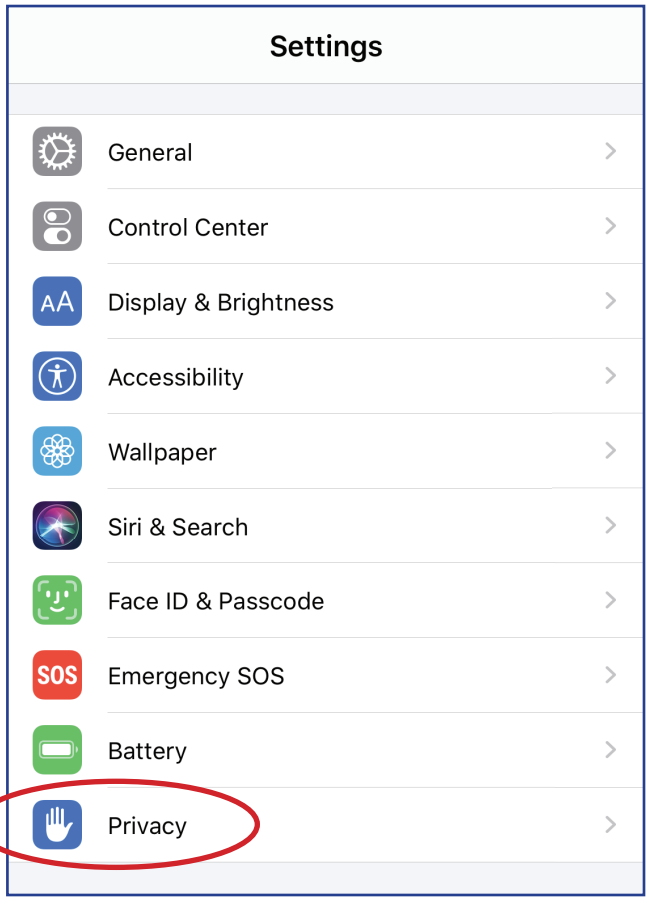
by Stephen Huston

AlamedaMUG@gmail.com

All screenshots captured

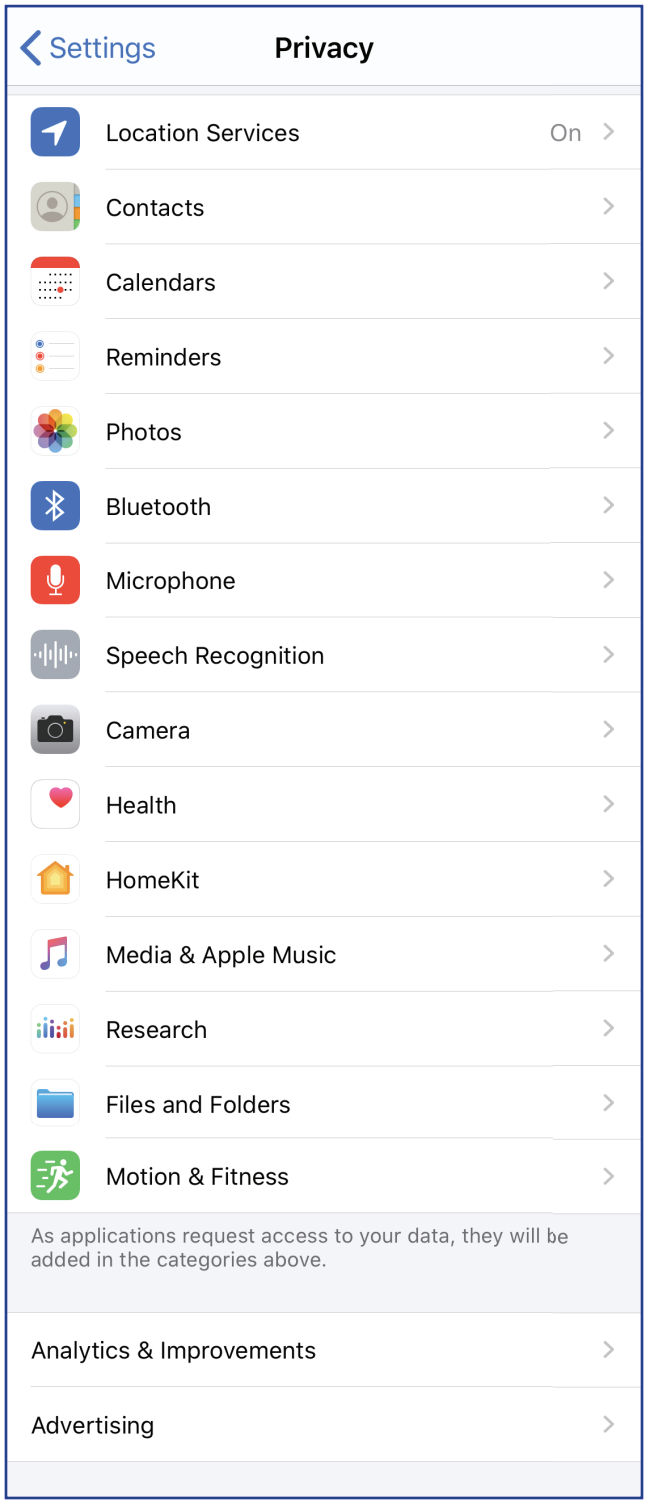
on an iPhone XS

running iOS 13.3.1



Privacy Settings

The Privacy area in Settings lists all of the major apps and system components from which information (data) about you, your files, and your hardware get revealed to the apps installed on your iPhone. Each of these sections represents a portion of your iPhone's operating system, stored information, and hardware capabilities, including the camera and microphones, that each app on your iPhone may need or want to use.



You probably use some apps which need to access some data or hardware to accomplish what you want, and that is perfectly fine.

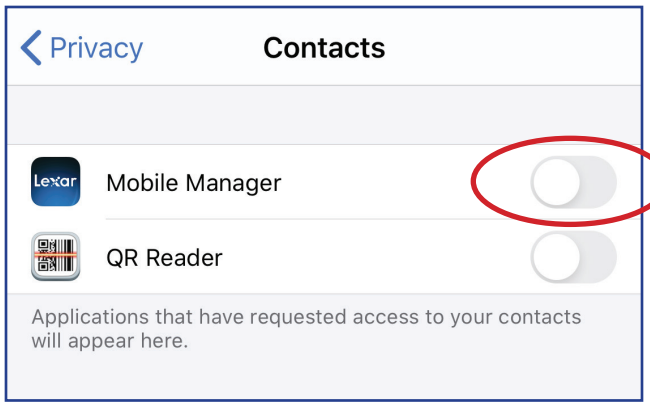
However, some apps have ulterior motives for accessing the various areas of your iPhone — to take your data, send it to the developer or their business partners, and let them use or even sell your information.

Unfortunately, that's a fairly common business model in the modern digital world, and iPhones are among the most-targetted of devices for this type of sleazy dealing — iPhone owners are thought to have more disposable income than users of other devices. If you own an iPhone, you really are a target.

(**NOTE**: if you were to switch to a non-Apple phone, the Android operating system was built with Google's input and backing. Much of the Android software funnels users' data to Google for them to monetize, so that's even less private.)

So let's dig in and see who is trying to see what you've got on your iPhone, and whether or not you should let them have their way with your stuff.

I'll focus on a few of these sections, but your should eventually check them all.



Contacts

This screen shows which currently-installed apps have requested to read your Contacts data. Toggle buttons (as noted above) indicate whether or not you have currently given each app permission to read your Contacts.

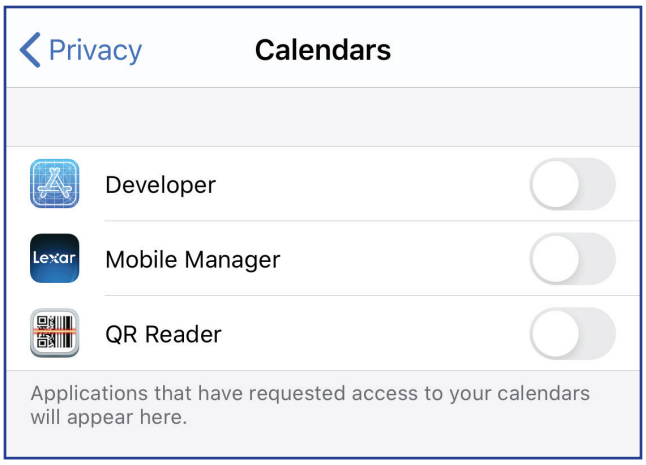
At the moment you launch a new app, if it asks for permission to access your Contacts, and you do give it permission, it may simply download your entire Contacts file to the developer's server for them to use any old way they want. Once they have it, you don't necessarily know they took it, but you won't get it back.

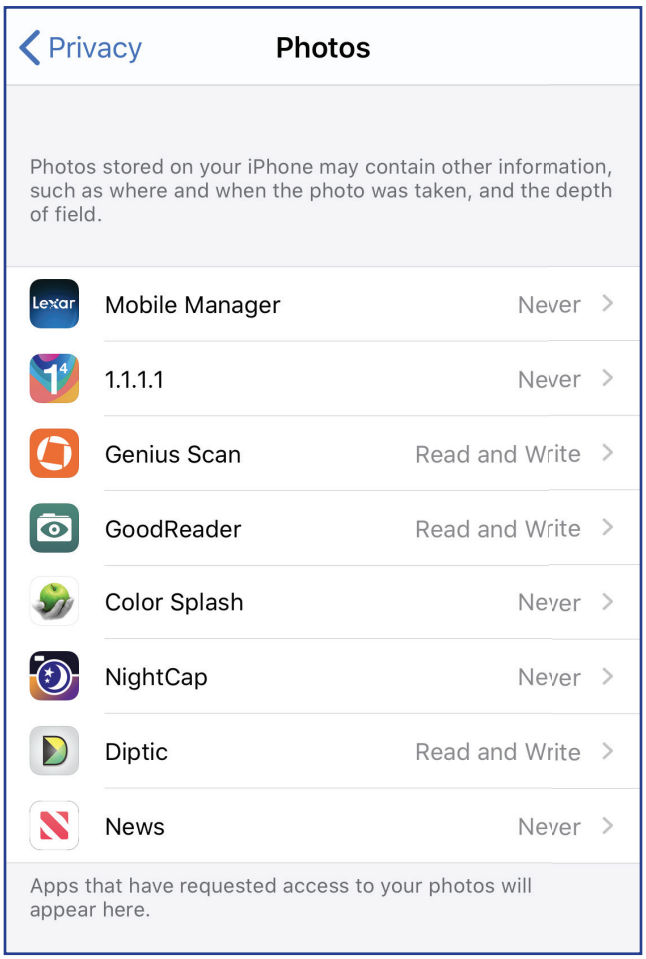
But you can turn OFF permission for it to keep checking your Contacts. Now you see why automatically okaying permissions might be a huge mistake.

Calendars

How many of your apps really need to know your private schedule of events and plans for the future?

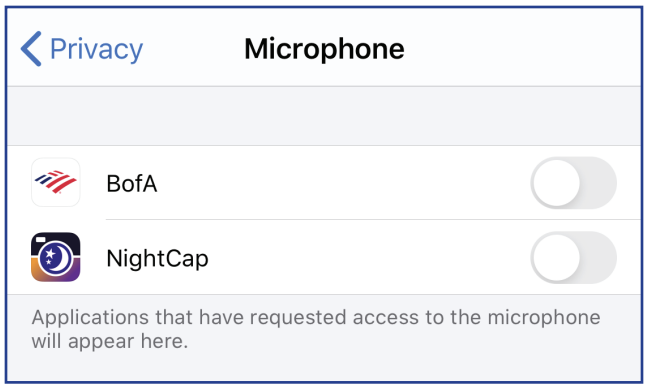
With each of these items, you can stop the ongoing flow of private information (hence ***Privacy***) from your iPhone.





Photos

Some apps have legitimate reasons to read from or write to your Photos. You can decide what permission each app gets, and you can come back to this panel to change that at any time. You decide!



Microphone — *Who's Listening?*

Unless your iPhone is completely Powered-Off (not just sleeping with the screen blacked out) you microphone is ALWAYS ON! It is picking up the sounds around you, including your conversations with friends and family.

How much of that sound might be ***captured and saved*** depends on which apps you have given permission to access your Microphone.

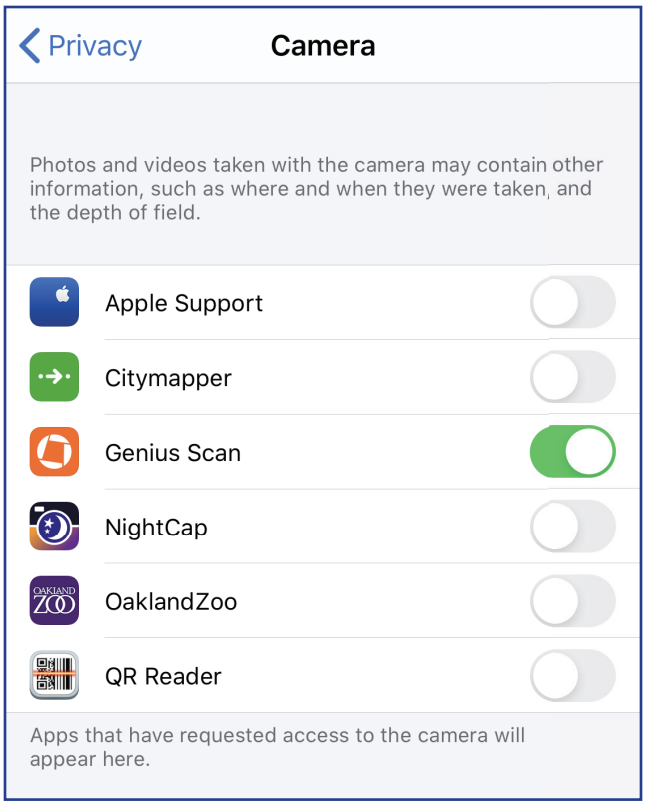
While there is little reason to suspect that most apps which have any obvious reason to interact with your voice are actually recording everything all the time, we know that hackers have used the microphone to do that in some cases.

Decide who you trust to listen to you via your mic, and stop the rest.

Camera — *Who's Watching?*

Just like with the Microphone, your Camera's light sensor is ALWAYS ON unless the phone is Powered-OFF!

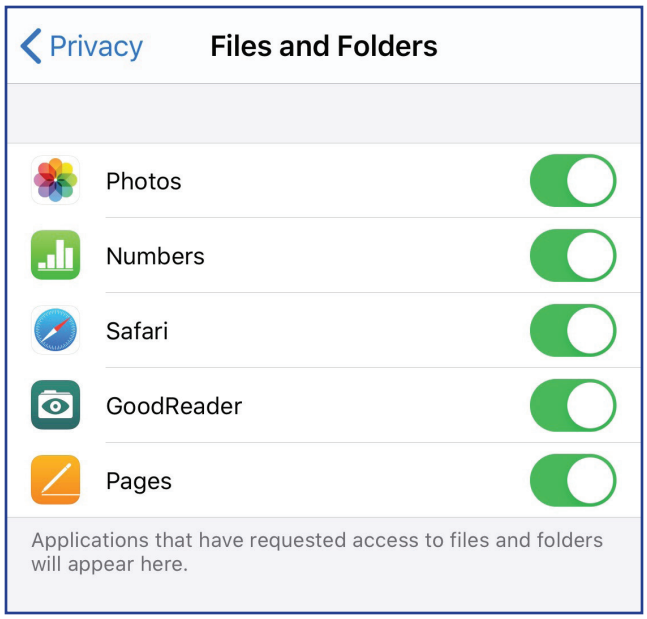
Hackers have used this fact to hack into both phones and computers with built-in cameras in the past. If you carry your iPhone in your shirt pocket, a



hacker could theoretically watch your personal viewpoint as you walk around all day! Even some embarrassingly private activities have been captured and posted on the web by hacking phone or computer cameras.

Limit access to your Camera to just the apps you trust. If you're like me, you might even turn off Camera access to most of them except when you're ready to use them, them disable it again when you're done.

NOTE: Of the 6 apps I currently have installed which have requested access to my Camera, I know of valid reasons for 5 of them to use it at times. I think the other one just tried to grab all the permissions it could get, but I declined. Even so, I turn Camera access on/off as needed with apps I don't use daily.



Files and Folders

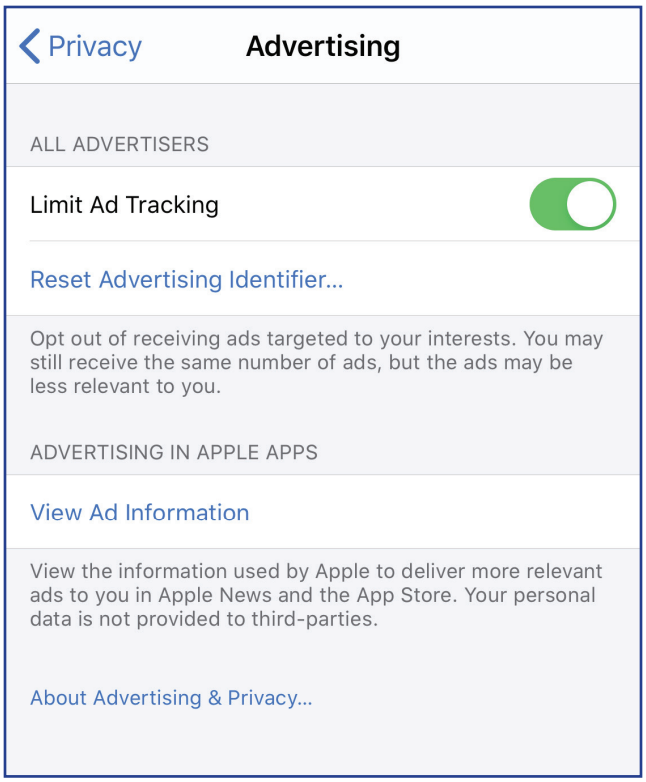
This controls access to read from and write to your iCloud documents storage via the Files app or via the sharing icon when manipulating files within apps. Permission to access your iCloud area can be particularly sensitive if you place anything of importance in iCloud storage, but this setting must be enabled to allow the programs you use with iCloud storage to save files.

NOTE: I have enabled only one app which isn't from Apple itself. I use iCloud to expand beyond my iPhone storage of PDFs in a third-party app, *GoodReader*.

In my experience, Files and Folders is not one of the areas where hackers have yet focused for breaking into iCloud, but it's worth thinking about which apps have access into your iCloud storage.

Advertising

At the bottom of the Privacy Settings list is ***Advertising***. Nobody likes advertising.

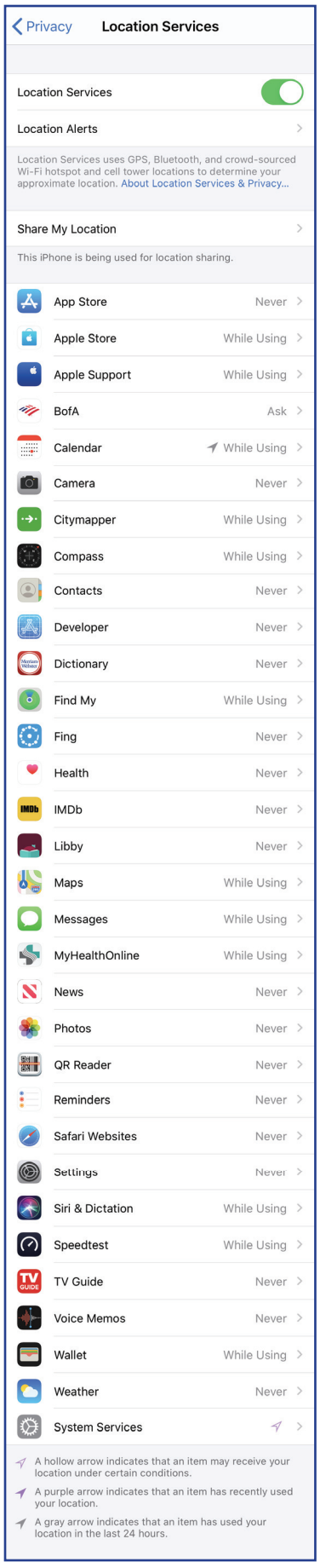


We have both *good news* and *bad news*.

The *good news* — there's a couple of things you can set here to reduce the amount of *targetted advertising* you see. Targetted ads are those which appear because websites and ad-bots are watching where you go and what you view on the web, then intentionally showing you related ads. To limit tracking, turn ON "Limit Ad Tracking."

You can also Reset Advertising Identifier, which changes the device ID of your iPhone, disconnecting old tracking data from new. (I reset my *identifier* whenever I'm in Privacy settings.)

The *bad news* — you won't see fewer ads, but they won't be *targetted* based on your viewing history. This also means advertisers won't get as much private info about you as they previously collected.



Location Services and Location Tracking

We're now going up to the very top of the Privacy settings to dig into Location Services. This is where you decide which apps get to see your location and track it, including sending it to advertisers and surveillance businesses.

A ***New York Times*** article published December 19, 2019, illustrated how a typical database of location data allowed researchers to identify individuals from supposedly *anonymized data* by using GPS coordinates to locate a phone at an individual's work or home location and then track that phone over time. So much for both anonymity and privacy.

Some people's first instinct is to completely turn OFF the big green Location Services toggle at the top of this screen. Unfortunately, doing that cripples the iPhone's operating system. Your iPhone will quit working as it should.

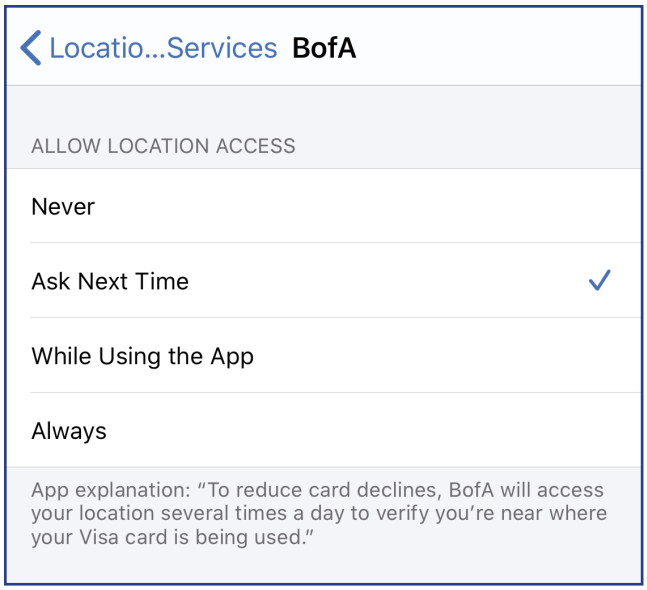
Instead, you should go through this list of the apps which want permission to use your location, and restrict them as you feel it is appropriate.

Don't give permission for location tracking unless you have a clear idea of why that app needs that information to function for you. Most apps can safely be set to "Never" allow location info. Others, such as Maps, you probably want to set to allow "While Using" the app.

You can also set some apps to "Ask" for permission, forcing them to tell you the next time they want location information, which you can approve or not at that time.

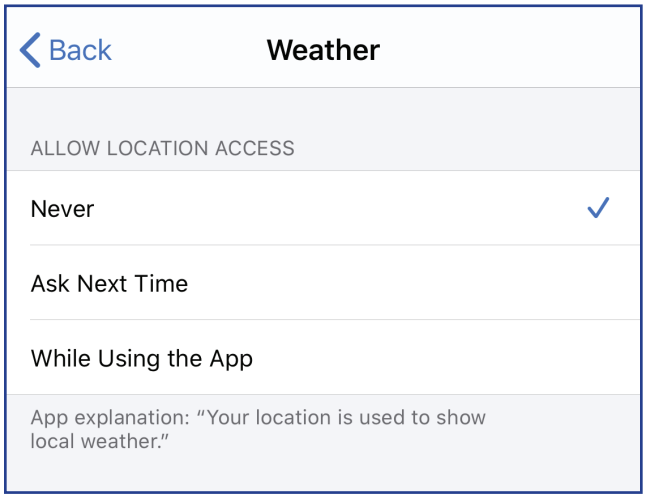
Most apps no longer ask to "Always" read location info because they have no valid reason to do so, although "Always" was once the default for any app using location. (None of my apps are set to "Always" see location data, and they all work just fine.)

Let's take a look at just a few examples, including one default app that comes with new iPhones which is now known to be a major offender when it comes to privacy.



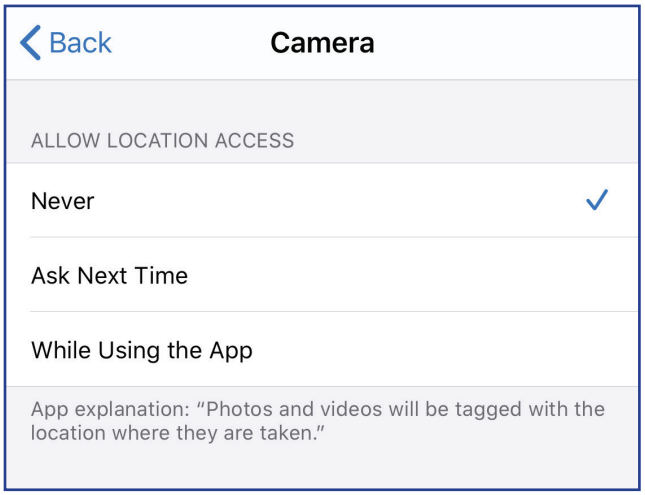
Banking Apps

I use a banking app to monitor my credit card activity. I currently have it set to "Ask" so the next time it wants to check my location it must Ask again for my permission. During some trips, I've reset it to "Always" so that my bank can see that I am right there with my card when it is being used far from my home.



Weather — or not

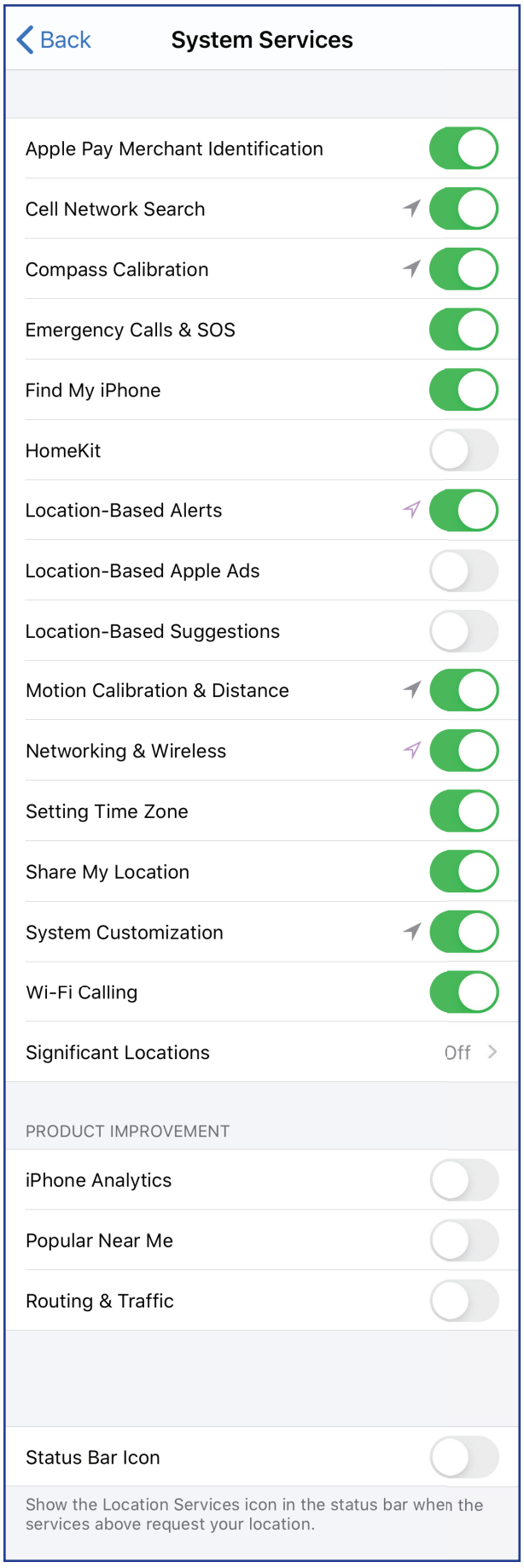
The Weather app comes preinstalled on iPhones, even though it is not an Apple-made app. It's developer collects and sells iPhone location data. They claim your location data is needed to show you local weather, though that's not all it does with it. I set mine to "Never" allow location access, and it still shows me the local weather that I've chosen by adding favorites — where I live and the many places I visit regularly. Now Weather can't grab my location all the time.



Camera & GPS Data

With Location access enabled, GPS data is embedded in each photo as it's captured. ("While Using the App" is the Camera's default permission on new iPhones. Note there is no "Always" option because Apple knows that's not necessary or appropriate.)

You can turn Off GPS tagging of photos by choosing "Never," or pick "Ask" so you can decide the next time you open the Camera app. If you do embed GPS, be aware that location is readable by anyone who gets ahold of your photo. Dig around in the Photos app for "Places" and you'll see what I mean.



System Services

This last Privacy section covers the iPhone System Software's use of Location Services. My advice on this is ***don't touch what you don't understand*** — leave it alone.

(That's why turning off the main toggle at the top of all Location Services is a big mistake. Your iPhone needs really needs most of this stuff just to work as intended.)

I've turned HomeKit off because I have no HomeKit (IOT - internet of things) devices that are HomeKit compatible. I disabled a few other items that I felt were safe and might enhance my privacy and reduce ads.

It's also perfectly okay to leave all of these turned On.

If your "Significant Locations" is turned ON, click on it and take a look at what's been collected about you by the iOS itself. I turned my Signifant Locations off after seeing what it tracked about me.

Should You Copy My Settings?

NO!

You should decide on each item in the Privacy settings area for yourself based on what you use, how you use it, how much privacy matters to you, and if you trust the app not to misuse your private data.

iPhones give us each the option to adjust these settings for ourselves. Apple's default choice for each setting is generally based on "ease-of-use" rather than what's most private.

You get to decide.