Facebook ‘Secretly’ Tracks Your iPhone Location—This Is How To Stop It

F forbes.com/sites/zakdoffman/2020/12/13/facebook-tracks-apple-iphone-locations-even-ios-14-and-iphone-12-12-pro-and-pro-max

December 13, 2020

Dec 13, 2020,06:30am EST|26,050 views

Zak DoffmanContributor ⓘ
Cybersecurity
I write about security and surveillance.

NurPhoto via Getty Images

Facebook has a data addiction—it can’t help itself. The social media giant’s entire business model is built around collecting, processing and then monetizing our personal information. Facebook seemingly can’t contemplate user information that crosses its path which it doesn’t harvest and add to its data vault. And while its privacy settings are materially better than they were, there remain *frightening* gaps.

Much of this has been exposed by the ongoing battle between Facebook and Apple over the privacy of iPhone users—cutting access to tracking IDs and the location data limitations introduced with iOS 14. But there are still those gaps. If you tell Facebook not to collect location information from your iPhone, then it doesn’t, right? *Wrong*.

I’ve warned on the risks of image metadata before. When you take a photo with your iPhone, data is embedded in the image file. Much of this EXIF (Exchangeable Image File) metadata is technical, relating to the camera and the photograph settings, but EXIF also includes the date and time the photo was taken, the phone model, “iPhone 12 Pro Max,” for example, the version of iOS and, critically, the *precise* location.

You can turn off the GPS location tagging on your iPhone’s camera, but that will prevent your phone displaying photos by location, which is useful. But when you share your photos, that EXIF data may go along as well, data that will stay with your photo everywhere it’s shared. Protecting this data is not just a Facebook issue, ironically sending photos from your iPhone by WhatsApp or Facebook Messenger strips the metadata, *but* iMessage will not, unless you share your photos in a specific way.

But there’s a huge difference between you inadvertently sharing EXIF data and having that data secretly harvested and mined, without very specific warnings that this is being done. When you upload your photos to Facebook or Instagram, most metadata is stripped out and replaced by Facebook’s own codes. The date and time remain, but the location data does not. This is a major privacy benefit, you don’t want others to download your Facebook or Instagram photos and have details of where you live or work, for example, or to map your movements by the photos you’ve taken.

MORE FROM FORBESWhy You Should Stop Sending Links On Facebook MessengerBy Zak Doffman

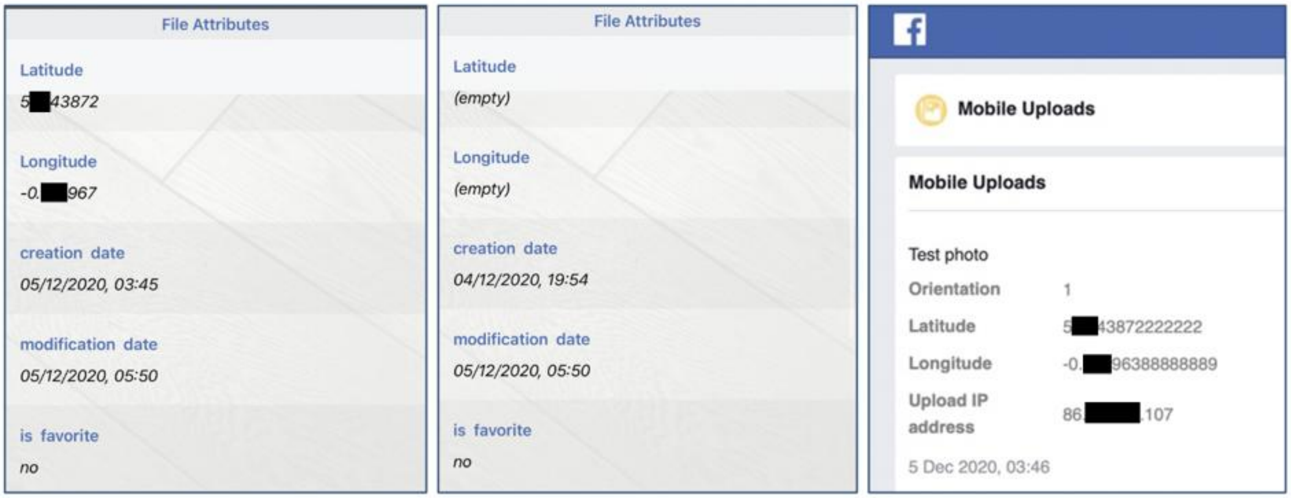
But that location metadata is not thrown away by Facebook—it is way too valuable. It is harvested, “collected and processed” to be added to the data treasure trove it holds on each of us. Let’s be very clear here, in your iPhone’s “Location Services” settings, under “Privacy,” you can select to “never” allow Facebook access to your location. This shuts down the Facebook app’s access to the location derived from the iPhone itself when using the app or in background. But Facebook still uses this hidden EXIF workaround and it’s your data that is being taken, with most of you not realising it’s being done.

You can see all this for yourself. Ensure that the Facebook location option is “Never.” Take a photo with your iPhone, go to your camera roll, open the photo and swipe up. You should see your location on a map—now you know the EXIF has been captured in the image file. Next, upload the photo to Facebook using your app. You don’t need to share it publicly—as long as it has been stored in your Facebook album, it’s fine.

Facebook location settings switched off

Facebook / MacOS, iOS

Now, if you download that photo *from* Facebook *to* your iPhone, such that you see a duplicate in your camera roll, you’ll see that when you swipe up you can’t see the location in the downloaded version. No map appears. Facebook has stripped the metadata. If you have an EXIF reader, you can open the photo and see what’s there—again, no location tag.



File Attributes

Latitude
5[redacted]43872

Longitude
-0.[redacted]967

creation date
05/12/2020, 03:45

modification date
05/12/2020, 05:50

is favorite
no

Before upload to FB

File Attributes

Latitude
(empty)

Longitude
(empty)

creation date
04/12/2020, 19:54

modification date
05/12/2020, 05:50

is favorite
no

Downloaded from FB

Mobile Uploads

Mobile Uploads

Test photo

Orientation	1
Latitude	5[redacted]43872222222
Longitude	-0.[redacted]96388888889
Upload IP address	86[redacted].107

5 Dec 2020, 03:46

FB data request

Location data stripped by Facebook has been harvested. Creation time of download in PT, not GMT
Facebook / iOS

Now to the interesting part. Facebook has harvested and stored the photo's *precise* location data. You can see this for yourself, although it's somewhat laborious and there could be lots of data. Login to your Facebook account. Then under Settings and Privacy—Settings, select "Your Facebook Information." Select "Photos and Videos" and hit "Create File." Unhelpfully, Facebook's date limiting range can skew results and may return empty folders.

Once the file is created, you can download it. For each of your albums, you will have a folder containing your photos. You can delete these. You should also have an "album" folder which contains a list of html files. This is your metadata, and it includes the stripped location tags as well as your IP address. That information has been collected by Facebook and can be mined at will. The company can infer all kinds of intelligence from the time and place, the IP address, the phone used, and even the subject matter of the photograph: Where I am, what I'm likely doing, even who I'm with. Why else would Facebook want this data?

ESET's Jake Moore warns that "users must remember that Facebook's whole business model is based on mass data collection and being a free to use network—they will collect as much as (and where) they possibly can. Facebook tracks almost everything you do both while you're on Facebook as well as when you're browsing elsewhere to help feed its impressive advertising algorithms. When you upload a photo with all its interesting and useful metadata, it seems Facebook don't want to delete this convenient information as it adds to their growing data on us."

So now we know that despite being told not to track my iPhone location, Facebook has harvested, stored and processed my location from a photo taken on my phone, adding it to the other datapoints it collects on me from countless websites and apps. As a user I have been lulled into a false sense of security by disabling location access—Facebook knows I have done this but saves my location data anyway. Given that most of my photos are taken on my phone, as soon as I upload one to Facebook or Instagram, the company can track my movements and mine location patterns to derive intelligence about my behaviors. “Metadata, data about your data,” says Cyjax CISO Ian Thornton-Trump, “is almost as powerful as the *actual* data.”

It’s this kind of shadowy collection and processing of metadata under the guise of broadly worded privacy policies that worries security advocates over Facebook’s stewardship of WhatsApp. Its much less secure Messenger and Instagram platforms are not recommended for anything private or sensitive. We know that WhatsApp is due renewed terms of service next year, and as Facebook accelerates it monetization of the messaging giant while operating with the bounds of end-to-end encryption, it’s likely to be metadata that’s in play. It’s for these kinds fo reasons that many security-focused WhatsApp users would welcome the forced divesting of WhatsApp threatened by the new legal process announced this week in the U.S.

Facebook acknowledged to me that it collects and processes EXIF data—it’s in its data policy, if you know where to look. But its explanation to me focused on technical data to better handle images—it did not want to be drawn on location data, which is the real issue. It seems clear that Facebook will harvest this tracking data regardless of any privacy settings on your iPhone, if it can. And it’s at Facebook’s discretion—subject to its data policy—how that data is used. Facebook would neither confirm nor deny to me that advertising and monetization play a major part.

“Connectedness is a reciprocal arrangement,” according to Nicola Whiting, Chief Strategy Officer at Titania. “Facebook and companies like them, provide ‘easy, quick and free’ ways to connect. In exchange they harvest your data and find ways to use it commercially. You can strip the metadata from photos before uploading, and protect your personal information, but there is a time and convenience cost. The end choice is the consumers, but connectivity providers are counting on people's inherent preference for easy, quick and free access.”

So, what can you do if you don’t want Facebook and Instagram harvesting and mining the locations of every photo you upload? No easy options, I’m afraid, assuming you want to continue to capture GPS tags with your iPhone photos—if not, disable geotagging within the iPhone’s camera settings. If you want your iPhone camera to geotag photos, then you can share your photos from within the iPhone’s photo album, stripping location settings as you do, but that will limit the features associated with posting those photos. The best option is to install a reputable EXIF app to strip metadata before you share photos. You shouldn’t need to do this—but you do.

MORE FROM FORBESIf These Apps Are Installed On Your Phone, You Can 'Easily' Be HackedBy Zak Doffman

Of course, there is another option. Facebook should not “collect and process” the location data from photos uploaded by its users—certainly not when those users have selected the option to “never” use location tracking on their Facebook app. But history suggests that unless Apple steps in, Facebook is unlikely to act.

Tommy Mysk is one of the researchers who caught multiple apps secretly reading iOS user clipboards, prompting Apple to add the clipboard access warning in iOS 14. He warns that “by allowing access to photos, users are not aware that apps can also extract the EXIF properties of each photo in their photo library and know the location and time of each photo. The app can theoretically figure out the places the user has visited. This information is particularly interesting for advertisers. There is no way we can verify what apps actually do with the data they have access to on a user's device.”

Perhaps given the focus on location tracking and privacy in iOS 14, Apple needs to add EXIF management to a future release, giving us full control of what data is shared and taking the opportunity for another swipe at Facebook’s invasive practices.

Zak Doffman

I am the Founder/CEO of Digital Barriers—developing advanced surveillance solutions for defence, national security and counter-terrorism. I write about the intersection

...