DO MORE › **WEB & SEARCH**

Why Stalkers Love Your Geotags

Learn why 'checking-in' while you're on vacation might be a bad idea

f Share   **Ⓟ Pin**   **✉ Email**

Peter Muller/Cultura/Getty Images

by **Andy O'Donnell** ⓘ
Updated February 02, 2018

Stalkers no longer have to creep around corners to follow you. Geo-stalkers can now find out your whereabouts by following the trail of digital breadcrumbs you leave them via your geotags posted on Facebook, Twitter, and other social media apps and services, and by the geotag data embedded in the photos taken on your smartphone.

We have been slowly conditioned by Facebook, [Foursquare](), Apple, and others to give out our current location through the use of [location-tagging]() apps and services. Sure, we can track our friends down and get location specific coupons sent to our phone by just walking into a store but at what cost to our personal safety?

Geotagging your position reveals a lot of information about you which could potentially be used by stalkers, private investigators, and thieves. Let's take a look at some of the things that you are revealing about yourself when you geotag your location:

Tagging Your Current Location is a Bad Idea

This is an obvious piece of data that we know is being provided when we geotag ourselves. Your geotags tell someone both where you are and where you aren't. If you just checked in at your favorite restaurant while on vacation, then guess what? You are not at home. If your friend left his [Facebook account logged in on his phone that was just stolen](#), then the thieves who took his phone now know that you are a pretty easy target since you're 'checked-in' at a pizza parlor a thousand miles away.

Your Location History Can Make You Vulnerable

Your location history is recorded as you move about from place to place. Location history can be extremely useful for stalkers or investigators because it tells them where they can

likely find you and what time you are likely to be at locations that you routinely frequent. If you 'check-in' at the same coffee shop every Tuesday, then they probably know where you'll be next Tuesday.

Your location history reveals your buying habits, your interests, where you hang out, where you work, and who you hang out with (when you check others in who are with you or they check you in to a location).

Where You Took a Photo Shows More Than Your Smile

Some people are likely unaware that their cellphone or digital camera captures Geotag location information every time they take a picture. Geotagging a photo seems harmless enough right? Wrong!

The geotag, which doesn't appear in the actual image, but is none the less part of the

picture's 'meta data', can be viewed and extracted. If criminals extract the location information from the picture you posted on an online sale or auction site, then they now

know the exact GPS location of the item in the picture you snapped. If the item is of high value, then they might just come and steal it.

The geolocation data for most images is stored within the image file in a format know as EXchangeable Image file Format (EXIF). The EXIF format has placeholders for GPS information that often gets recorded as you take a photo with your smartphone. The location data can be extracted by EXIF viewer apps such as the [EXIF Viewer Firefox Add-on](#) or via an app such as [EXIF Wizard](#) for the iPhone, or Jpeg EXIF Viewer for Android

You might consider downloading one of the above applications to see if your pictures have geotags embedded in them.

What Can You Do to Protect Yourself?

- **Consider turning off location services on some location sharing apps:** Find the location sharing settings on your smartphone and turn off the ones that you think might pose a personal safety risk. You can always turn them back on later if you want to.

    - Most smartphones will let you turn off location sharing for individual apps as an alternative to turning them off globally.

    - There are some apps such as 'Find My iPhone' that you won't want to disable location sharing on. If you do disable location sharing on apps like 'Find My iPhone', then your phone won't be able to relay its position and you won't be able to find it using the 'Find My iPhone' service should it get lost or stolen.

- **Remove geotags from your digital photos:** If you want to remove geotag information from your image files then you can use an app such as [deGeo](#) (iPhone) or Photo Privacy Editor (Android) to remove the geotag info from your photos.

    - Consider turning off the location sharing setting of your phone's camera app as well so that the GPS info does not get recorded as part of the picture's meta data, this will save you the hassle of having to strip out the location data later on

How to Re G Fr iP Pi

7
Th
Yo
Sh
No
Pu
In
Yo
O
Da
Pr

10
Th
Yo
Sh
No
Po
on
So
No

Ti
fo
Ba
Ge
Ca
O

W
Yo
Sh
Kr
Al
Fa
Ne
Fr
Fe

5
Ti
fo
St
Sa
on
Tw

Lifewire

Get the Most From Your Tech With Our Daily Tips

Enter Your Email

SIGN UP

Follow Us

f Facebook

HOW TO

FIX

BUY

DO MORE

About Us

Advertise

Privacy Policy

Cookie Policy

.dash

Lifewire is part of the Dotdash publishing family.

The Balance | **ThoughtCo** | **The Spruce** | **TripSavvy** and more