

# Geotagging Risks and Solutions

634 Administrator Mon, Aug 16, 2010 [Best Practices](#) 0 3447

The ubiquitous automatic geotagging of pictures taken with smartphones and digital cameras and then posted on the Internet could prove to be a real security risk.



*Fred wants to hang out with his friends, and checks to see where they are.*

Here's an example: "MythBusters" host Adam Savage took a picture of his car parked in front of his house, and posted the picture on Twitter. The picture also contained a geotag - metadata that reveals the exact latitude and longitude of the spot on which the picture was taken - which ultimately revealed to anyone who might be interested where his house was located.

Combining this information with the Twitter status saying "Now it's off to work," he has given potential thieves the perfect opportunity to burglarize his home.

He says he's aware of the existence of geotags, but that he simply forgot to disable the geotagging function on his iPhone. He also says he doesn't worry about the consequences because of his recent move and jokingly asserts he's not famous enough to have a stalker.

But, there are a lot people out there who don't know that this kind of data is often included in digital images, or that the option of turning the GPS on these devices even exists. And even if they do, this option is almost always hidden behind several menu

levels, and turning it off often means losing other GPS benefits.

To people concerned by the possible risk tied to geotagging, The New York Times recommends visiting ICanStalkU.com, a website that provides simple, step-by-step instructions on how to disable the option on various mobile devices.

But even as the awareness of the risk is rising among the lowly users, online services such as Flickr have recently made the geotag data of pictures posted via mobile devices unavailable by default to anyone except the photographer. But, of course, if the user chooses to share it, he can.

Also, some other sites - and Facebook is one of them - sometimes format the uploaded pictures in such a way as to make it impossible to fish out geotag data, but that is purely accidental.

Security experts are particularly worried about the pictures posted on social networks, since they are usually accompanied by real-time statuses. They say that anyone with a modicum of programming knowledge can write a program that could search for the combination of geotagged pictures and "On vacation" statuses. And with plug-ins that can extract geotag data from pictures, even people keeping blogs or personal pages are not safe.

The ultimate consensus about the issue is that every user should be aware of this feature, and take responsibility of informing his or her friends about it. After all, you can choose not to post a revealing picture, but your friend might.

Online URL:

<https://www.articlediary.com/article/geotagging-risks-and-solutions-634.html>