

Thanks to geotagged photos, are you sharing too much?

February 17 2014

Whipping out your smartphone to snap and post online pictures of yourself and your kids relaxing at home - or perhaps that pricey new TV you just hung on your rec-room wall - is like throwing chum to a sea of hungry sharks.

That's because smartphone images can be deciphered to reveal precisely where the [photos](#) were taken, which security experts say could lead burglars and other criminals directly to your front door. Similarly, they add, posting images from vacation sites or your workplace could invite crooks to ransack your house while you're away.

"That can be sharing a bit too much," said Con Mallon, senior director of mobility at security firm Symantec. "They can then put the location of where you are now and where your house is into a maps program and work out how much time they have to pay a visit while you're out."

Smartphone photos are embedded with "geotags" containing the latitude and longitude. This data isn't visible to the naked eye. But when deciphered with the help of photo-sharing websites, various apps or other methods, those coordinates can enable someone using Google Maps to identify the precise spots depicted in the images.

That also makes the technology useful, for example, for someone with scads of photos who can't otherwise remember where some of them were taken. And sharing geotagged photos online has become so commonplace, many people hardly give it a second thought.

"I'm OK with it," said 25-year-old Roilo Escalada of Santa Clara, who is studying kinesiology at San Jose State and who occasionally posts pictures with his iPhone. "I don't have any stalkers. I feel safe."

Janisha McCoy, 30, who lives in Oakland and works at San Jose State, also was nonchalant.

"It's not really that big of a concern when you think about all the other stuff that's on the Internet," she said. Still, several people interviewed on the campus were surprised to learn their pictures could reveal where they were snapped, and McCoy added, "It's something to think about."

Indeed, geotagged photos have posed unanticipated problems for even the most computer-savvy people.

That includes John McAfee, founder of the antivirus software company that bears his name. After eluding Belize authorities, who were seeking to talk to him as a "person of interest" in the 2012 shooting death of his neighbor, McAfee's location was revealed when a photo of his Guatemalan hideout was posted online.

Adam Savage, host of the TV science show "MythBusters" was embarrassed a few years ago when he took a picture of his car in front of his house and posted it on Twitter, inadvertently disclosing to his fans where he lived.

Still another case involved Higinio Ochoa, a Texas man with ties to the hacking group Anonymous, who was convicted in 2012 of stealing data from law-enforcement computers. After he taunted authorities by posting a photo of his girlfriend's barely clad breasts, the FBI was able to track him down in part from the location revealed in the image.

Some Web commentators claim concerns about geotagged smartphone

photos are unwarranted, noting that millions of people routinely post them without being victimized. Nonetheless, the National White Collar Crime Center, a nonprofit organization that helps police combat economic and tech-related crimes, has cautioned that placing such pictures on the Internet can be dangerous.

The military is worried, too. The Army issued a warning about geotagged photos after some soldiers posted pictures of military helicopters landing at an Iraqi base in 2007. Using the photos' [location data](#), enemy attackers precisely targeted and destroyed four of the copters with mortar rounds.

In addition, The New York Times and Guardian newspapers recently reported that documents obtained from former NSA contractor Edward Snowden show U.S. and British spy authorities have the ability to view geotag data in photos uploaded to various social media sites.

Experts advise anyone nervous about others knowing where their photos are snapped to block their phone's geotag features through the phone's settings or with geotag-disabling apps available on the Internet.

"Is location sharing a bad idea? Yes and no," said Tony Anscombe, senior security evangelist at AVG Technologies. "I take many pictures and post them on photo-sharing sites so that others can enjoy them." But he advises caution, because revealing where a person lives, works or otherwise frequents creates "a risk that most would agree is not necessary."

KEEPING YOUR PHOTO LOCATIONS SECRET

Various apps can be downloaded - including one from pixelgarde.com - that claim to remove geotag data from smartphone photos. But the easiest way to prevent others from knowing where you took the images

is to disable the geotag feature in the phone's camera.

How that's done varies by phone type, but it typically can be accomplished through the device's settings. With Apple's latest iPhone, for example, go to "settings," "privacy" and "location services," and then hit "camera off." That won't disable the camera; it merely prevents it from embedding location data in its pictures.

With Samsung's Android-based Galaxy S, click the camera icon, then click the settings wheel and the next two settings wheels that appear, then click "location tag" and disable it by hitting "off."

©2014 San Jose Mercury News (San Jose, Calif.)
Distributed by MCT Information Services

Citation: Thanks to geotagged photos, are you sharing too much? (2014, February 17) retrieved 20 March 2024 from <https://phys.org/news/2014-02-geotagged-photos.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--