Web Photos That Reveal Secrets, Like Where You Live
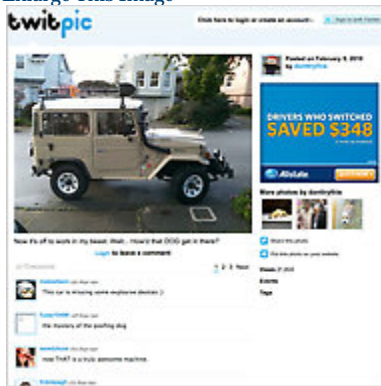
By KATE MURPHY

Published: August 11, 2010

When Adam Savage, host of the popular science program "MythBusters," posted a picture on Twitter of his automobile parked in front of his house, he let his fans know much more than that he drove a Toyota Land Cruiser.

Enlarge This Image

Adam Savage, host of the popular science program "Mythbusters," posted a picture on Twitter of his automobile parked in front of his house that was geotagged.

Multimedia

Audio Slide Show

How Geotags Unlocked a 'MythBuster's' Location

The ICanStalkU.com Web site provides step-by-step instructions for disabling geotagging on the iPhone.

Instructions on how to disable the geotagging feature of an Android phone.

Embedded in the image was a geotag, a bit of data providing the longitude and latitude of where the photo was taken. Hence, he revealed exactly where he lived. And since the accompanying text was "Now it's off to work," potential thieves knew he would not be at home.

Security experts and privacy advocates have recently begun warning about the potential dangers of geotags, which are embedded in photos and videos taken with GPS-equipped smartphones and digital cameras. Because the location data is not visible to the casual

viewer, the concern is that many people may not realize it is there; and they could be compromising their privacy, if not their safety, when they post geotagged media online.

Mr. Savage said he knew about geotags. (He should, as host of a show popular with technology followers.) But he said he had neglected to disable the function on his iPhone before taking the picture and uploading it to Twitter.

"I guess it was a lack of concern because I'm not nearly famous enough to be stalked," he said, "and if I am, I want a raise."

Still, Mr. Savage has since turned off the geotag feature on his iPhone, and he isn't worried about the archived photo on Twitter because he has moved to a new residence.

But others may not be so technologically informed or so blasé about their privacy.

"I'd say very few people know about geotag capabilities," said Peter Eckersley, a staff technologist with the Electronic Frontier Foundation in San Francisco, "and consent is sort of a slippery slope when the only way you can turn off the function on your smartphone is through an invisible menu that no one really knows about."

Indeed, disabling the geotag function generally involves going through several layers of menus until you find the "location" setting, then selecting "off" or "don't allow." But doing this can sometimes turn off all GPS capabilities, including mapping, so it can get complicated.

The Web site ICanStalkU.com provides step-by-step instructions for disabling the photo geotagging function on iPhone, BlackBerry, Android and Palm devices.

A person's location is also revealed while using services like Foursquare and Gowalla as well as when posting to Twitter from a GPS-enabled mobile device, but the geographical data is not hidden as it is when posting photos.

A handful of academic researchers and independent Web security analysts, who call themselves "white hat hackers," have been trying to raise awareness about geotags by releasing studies and giving presentations at technology get-togethers like the Hackers On Planet Earth, or Next HOPE, conference held last month in New York.

Their lectures and papers demonstrate the ubiquity of geotagged photos and videos on Web sites like Twitter, YouTube, Flickr and Craigslist, and how these photos can be used to identify a person's home and haunts.

Many of the pictures show people's children playing in or around their homes. Others reveal expensive cars, computers and flat-screen televisions. There are also pictures of people at their friends' houses or at the Starbucks they visit each morning.

By downloading free browser plug-ins like the Exif Viewer for Firefox (addons.mozilla.org/en-US/firefox/addon/3905/) or Opanda IExif for Internet Explorer (opanda.com/en/iexif/), anyone can pinpoint the location where the photo was taken and create a Google map.

Moreover, since multimedia sites like Twitter and YouTube have user-friendly application programming interfaces, or A.P.I.'s, someone with a little knowledge about writing computer code can create a program to search for geotagged photos in a systematic way. For example, they can search for those accompanied with text like "on vacation" or those taken in a specified neighborhood.

"Any 16 year-old with basic programming skills can do this," said Gerald Friedland, a researcher at the International Computer Science Institute at the University of California, Berkeley. He and a colleague, Robin Sommer, wrote a paper, "Cybercasing the Joint: On the Privacy Implications of Geotagging," which they presented on Tuesday at a workshop in Washington during the Advanced Computing Systems Association's annual conference on security.

The paper provides three examples of so-called cybercasing that use photos posted on Twitter and Craigslist and a homemade video on YouTube.

By looking at geotags and the text of posts, Mr. Sommer said, "you can easily find out where people live, what kind of things they have in their house and also when they are going to be away."

"Our intent is not to show how it's done," he said, "but raise awareness so people can understand their devices and turn off those options if they want to."

ICanStalkU.com, developed by the security consultants Larry Pesce of the NWN Corporation in Waltham, Mass., and Ben Jackson of Mayhemic Labs in Boston, uses a more direct approach to warning about the potential dangers of geotags. The site displays a real-

time stream of geotagged photos posted on Twitter; the person who posted the photo also gets a notification via Twitter.

"The reaction from people is either anger, like 'I'm going to punch you out,' or 'No duh, like I didn't already know that' or 'Oh my God, I had no idea,' " Mr. Pesce said.

In the latter category was Cristina Parker of El Paso, who sells appliances part-time at Kmart and also manages social media for small companies. ICanStalkU.com notified her last week that a photo she had posted on Twitter of her Chihuahua, Zipp, also revealed where she lived.

"I immediately tweeted back to find out what I can do about it," said Ms. Parker. The site sent her a Web link to instructions on how to turn off the geotag function on her LG Ally smartphone. "It's definitely good to know for me personally and because of my social media work, too," she said

Because of the way photographs are formatted by some sites like Facebook and Match.com, geotag information is not always retained when an image is uploaded, which provides some protection, albeit incidental. Other sites like Flickr have recently taken steps to block access to geotag data on images taken with smartphones unless a user explicitly allows it.

But experts say the problem goes far beyond social networking and photo sharing Web sites, regardless of whether they offer user privacy settings.

"There are so many places where people upload photos, like personal blogs and bulletin boards," said Johannes B. Ullrich, chief technology officer of the SANS Technology Institute, which provides network security training and monitors the Internet for emerging security threats.

Protecting your privacy is not just a matter of being aware and personally responsible, said Mr. Sommer, the researcher. A friend may take a geotagged photo at your house and post it.

"You need to educate yourself and your friends but in the end, you really have no control," he said, adding that he was considering writing a program to troll the Internet for photos with geotags corresponding to users' home addresses.

"I'm beginning to think there may be a market for it."