Geotagging Safety

Geotags and Location-Based Social Networking:

- **Introduction**
- **What is geotagging?**
- **Location-based social networking applications**
- **Security Concerns**
- **Protecting your safety & other's.**

Introduction

- In August of 2010, Adam Savage, of "Myth Busters," took a photo of his vehicle using his smart phone. He then posted the photo to his Twitter account including the phrase "off to work."
- Since the photo was taken by his smart phone, the image contained metadata revealing the exact geographical location the photo was taken.
- So by simply taking and posting a photo, Savage revealed the exact location of his home, the vehicle he drives and the time he leaves for work.

Introduction

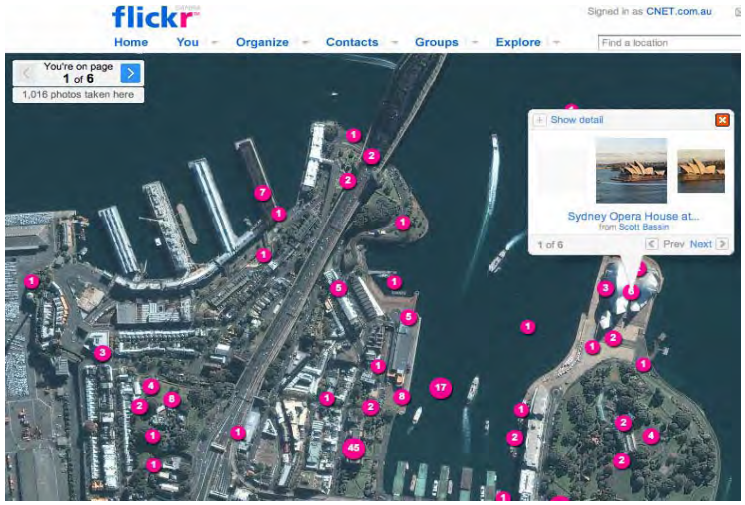
Does a stalker know where you live?

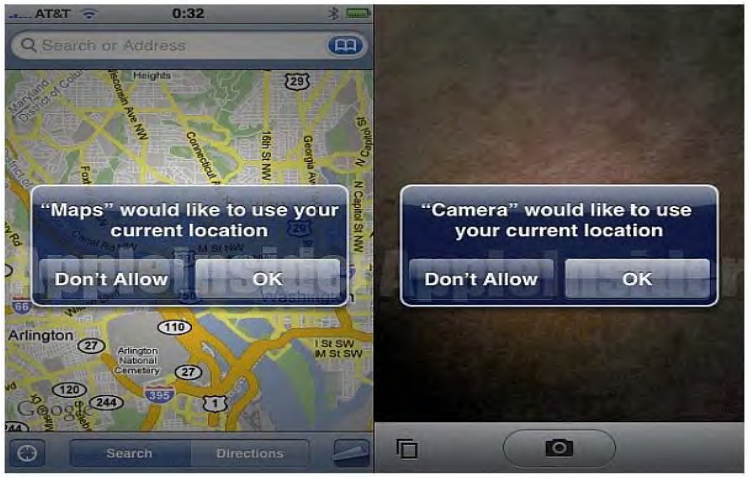
The following was published in Wired Magazine in 2009: “I ran a little experiment. On a sunny Saturday, I spotted a woman in Golden Gate Park taking a photo with a 3G iPhone. Because iPhones embed geodata into photos that users upload to Flickr or Picasa, iPhone shots can be automatically placed on a map. At home I searched the Flickr map, and score—a shot from today. I clicked through to the user’s photo stream and determined it was the woman I had seen earlier. After adjusting the settings so that only her shots appeared on the map, I saw a cluster of images in one location. Clicking on them revealed photos of an apartment interior—a bedroom, a kitchen, a filthy living room. Now I know where she lives.”

Introduction

As the stories above indicate, privacy and security aren't what they used to be. With advancements in technology, enhanced GPS capabilities and smart phones with built-in GPS, managing privacy and security is a fulltime job. The military is always working to protect itself against security breaches, but with new technologies come new risks. Today, more than ever, it is vitally important that military leaders, soldiers and civilians understand what kind of data they are broadcasting and what they can do to protect themselves and their families. CAP members should be aware of these threats to their privacy and security in this rapidly changing environment.

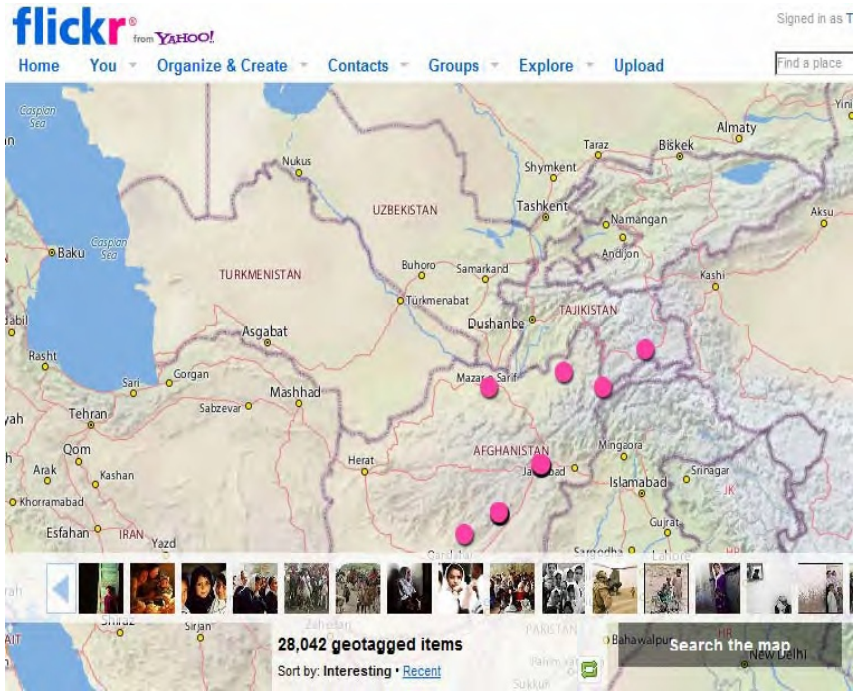
What is geotagging?





- Geotagging is the process of adding geographical identification to photographs, video, websites and SMS messages. It is the equivalent of adding a 10-digit grid coordinate to everything you post on the internet.
- Geotags are automatically embedded in pictures taken with smart phones . Many people are unaware of the fact that the photos they take with their smart phones and load to the Internet have been geotagged.
- Photos posted to photo sharing sites like Flickr and Picasa can also be tagged with location, but it is not an automatic function.

Geotagging Photos



- Digital photos have used geotagging for quite some time. Certain formats like the JPEG format allow for geographical information to be embedded within the image and then read by picture viewers. This shows the exact location where a picture was taken.
- Most modern digital cameras do not automatically add geolocation metadata to pictures, but that is not always true. Camera owners should study their camera's manual and understand how to turn off GPS functions.
- On photo sharing sites, people can tag a location on their photos, even if their camera does not have a GPS function. A simple search for "Afghanistan" on Flickr reveals thousands of location tagged photographs that have been uploaded.

Location-based Social Networking

- Location-based social networking is quickly growing in popularity. A variety of applications are capitalizing on users' desire to broadcast their geographic location.
- Most location-based social networking applications focus on "checking in" at various locations to earn points, badges, discounts and other geo-related awards.
- The increased popularity of these applications is changing the way we as a digital culture view security and privacy on an individual level. These changes in perception are also creating security concerns on an military and civilian level.

Foursquare

http://foursquare.com

- foursquare is a location-based social networking website for mobile devices. Users "check-in" at various places using a mobile website. They are then awarded points and sometimes "badges."
- Users of foursquare use the service to share their location with friends, meet new people and get coupons. Users can also connect and publish their "check ins" to Facebook and Twitter. If someone is ***not*** a friend on foursquare they can still track your whereabouts through Facebook.
- foursquare has over 4 million users.
- foursquare currently has iPhone, Android, webOS, Windows Phone 7 and BlackBerry applications.

Facebook Places

http://www.facebook.com/places

- Facebook's "**Places**" is similar to foursquare in that it gives an individual's location when the users posts information using a mobile application.
- This feature is available by using the Facebook application for iPhone, touch.facebook.com and Android.
- This function is automatically active on all Facebook accounts until disabled.

Gowalla

http://gowalla.com

- Gowalla is another location-based social networking application that functions much like Foursquare and Facebook Places.
- Users can build a Passport which includes a collection of stamps from the places users have been.
- Gowalla users can also post photos and submit tips at various locations.

SCVNGR

http://www.scvngr.com/

- SCVNGR is a location-based social networking application that takes "checking in" a step further by allowing companies, educational institutions and organizations to build challenges inside the platform.

- Users are encouraged to complete the challenges in order to earn points, badges or real-life discounts and coupons.

Why are these applications potentially dangerous?

- **Establishes patterns:** Services like MotionX (on right) and other location-based social networking applications allow strangers to track your movements every day. If they watch someone long enough they will know exactly when and where to find that person on any given day.
- **Exposes places of duty and home:** By tracking movements and aggregating information, strangers can determine where someone lives and works.
- **Identifies location of personnel:** If certain applications are used daily around civilian or military populations, a criminal can determine potential targets.

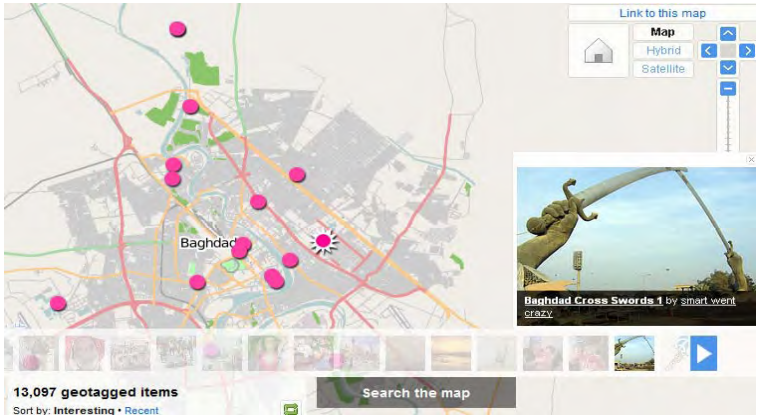
CAP Security Concerns

- CAP partners with many outside agencies in day-to-day operations. Those agencies trust our members to be as security conscious as they are.
- If we aren't careful, we put our personnel at risk as well as theirs.
- The future of our operations with outside agencies depends on our professionalism and our adherence to their operational security (OPSEC) guidelines.
- Protect yourselves and your partners!

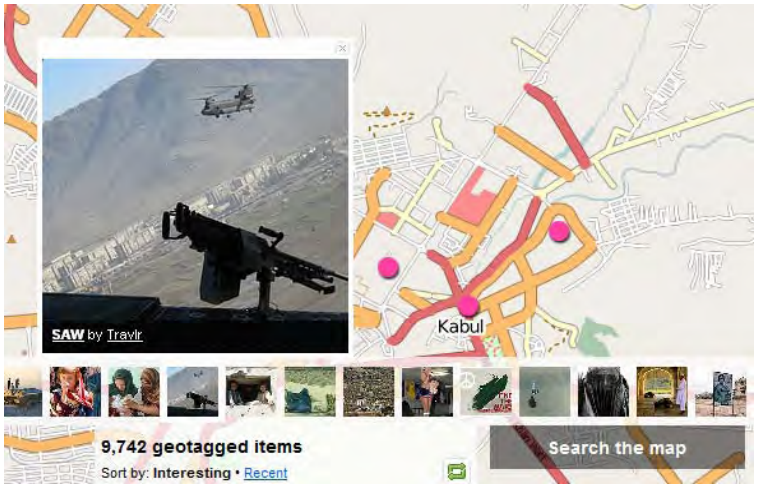
Our partners include:

- USAF
- Other DoD agencies
- DEA
- FEMA
- Other Federal agencies
- State & local EMAs
- State & local law enforcement

More Security Concerns:



- Tagging photos with an exact location on the Internet allows random people (think bad guys) to track your location and correlate it with other information.



- CAP members, military members and civilians serve in areas all over the world. Some locations are public, others are classified. They should not tag their uploaded photos with a location. Publishing photos of classified locations can be detrimental to mission success and can jeopardize lives.

Military Security Concerns

- The main function of location-based social networking applications is to broadcast a user's specific location. Exposing member and unit locations gives the bad guy the upper hand.
- One member exposing his/her location can affect the entire mission.
- Deployed Soldiers, or Soldiers conducting operations in classified areas should not use location-based social networking services. These services will bring the enemy right to the your doorstep.

Protecting Your Safety

How to avoid giving away TMI

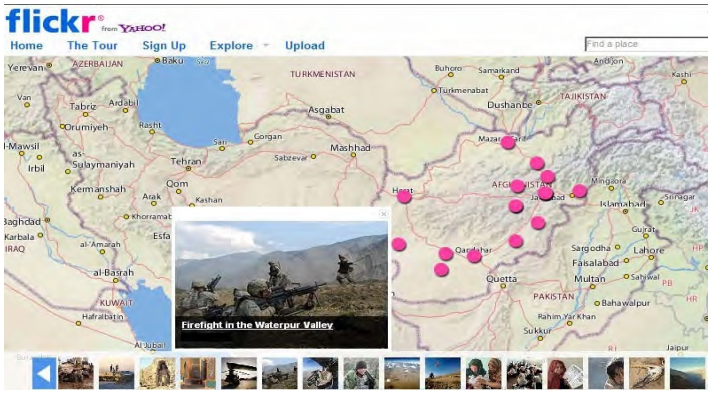
(Too Much Information)

Avoid geotags on your photo sharing apps. It can save your life!

- Many photo sharing applications give the user the opportunity to geotag a photo. In some cases, these geotags can add context to a photo, but when it comes to your safety, think twice before geotagging your photos.
- Users can delete geotagged photos, but once the information is out there, it's out of the user's hands. Even if posted briefly, a criminal can capture vital information and record your exact location.
- http://icanstalku.com for more info.

Avoid geotags on your photo sharing apps.

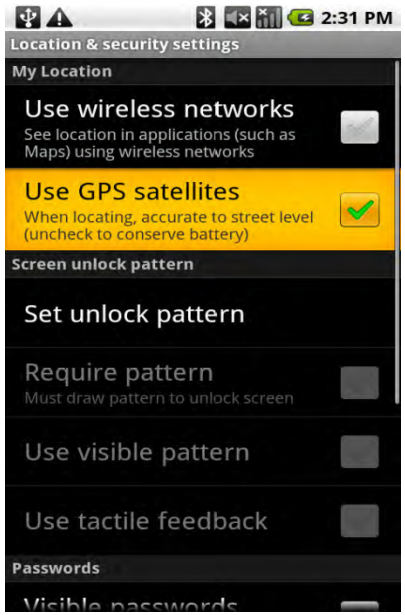
It can save your partners' lives!



Social Media Fact:
Something as simple as loading a photo of your bunk in Afghanistan to Flickr, then geotagging it, can bring a mortar round right into your area of operation.

- Many photo sharing applications give the user the opportunity to geotag a photo. In some cases, these geotags can add context to a photo, but when it comes to inter-agency operations, geotagging operational photos is not allowed.
- Users can delete geotagged photos, but once the information is out there, it's out of the user's hands. Even if posted briefly, the criminal can capture vital information and record exact grid coordinates of civilian or military populations.

Turn off GPS function on phones!



- One of the simplest ways to avoid displaying too much information is to disable the geotagging function on smart phones.
- Since most smart phones automatically display geographical information, it takes a little more effort on the user's part to protect their privacy.
- It's important that all users understand their specific systems and make efforts to turn off their phone's geotagging function.

Summary

- Geotagging photos and using location-based social networking applications is growing in popularity, but in certain situations, exposing specific geographical location can be devastating to CAP missions.
- CAP members should never tag photos with geographical location when loading to photo sharing sites like Flickr and Picasa.
- CAP members should not use location-based social networking applications when at training or while on duty at missions where presenting exact grid coordinates could endanger CAP members and our partner agencies' personnel.
- It is advised that while members are engaged in CAP missions, they should turn off the GPS function of their smart phones. Failure to do so could result in compromising the mission and even put members' families and properties at risk.
- CAP members deciding to utilize location-based social networking sites should be aware of the default settings for the services and devises they use. It is strongly recommended that the users customize settings to be mindful of security, privacy, personal and group safety, and the success of CAP missions for America.
- For more information: http://www.capmembers.com/emergency_services/operations_support/operational_security_opsec.cfm

Close the presentation. Verify that you have read the required material then click the “Start Quiz” button.

Thanks for your support of safety and for your service to CAP.