



Geotagging is an OPSEC



Concern – Be Safe!

Look out! That photo or info you post can tell bad guys more than you'd like

One of the foundations of force protection is to always keep the bad guys guessing. Letting them know where you are and what you're doing is never a good idea.

These days, with smart technology finding its way into almost everyone's pockets, and social media keeping the global information highways buzzing, guarding your actions can be tricky.

Geotagging and "location-based social networking" are two technological challenges technology that worry Army antiterrorism and force protection experts.

Geotagging is a function of many of today's digital cameras and smartphones with GPS capabilities. Geotagging embeds geographical information into a photo's metadata that can be used to determine exactly where the photo was snapped.

For example, CPT Jones uses his smartphone to shoot a picture of his Dodge Ram truck parked in front of his house and then posted it on Twitter with the note, "Now it's off to Wild Wings for dinner! Glad work is done." Little did he know that the photo was geotagged, and that he had just told the world exactly where he lives, what he drives, and when he leaves work -- practically an open invitation to potential thieves.

Army officials say the information that geotagging can add to photos -- and videos, websites and SMS messages -- "is the equivalent of adding a 10-digit grid coordinate to everything you post on the Internet."

And, they add, many people don't even know the geotagging function exists. They suggest that owners check their instruction manuals for information on a device's GPS capabilities and how to turn them off.

A related concern is that photos uploaded to public sharing sites such as Flickr and Picasa can also be tagged with an exact location, regardless of

whether the cameras that took them have GPS functions. A simple search for "Afghanistan" on one site can reveal thousands of tagged images.

Of equal concern to the security experts is location-based social networking, which has spawned a growing number of applications to satisfy users' desires to let people know where they are. Several of these sites offer "rewards" to users who "check in" at various locations. Of course these applications can also tell bad guys where you are or will be.

The dangers are that these location-revealing functions allow potential bad guys to watch your movements and uncover patterns in your behavior; reveal the exact locations of places, such as your home or office, where you will be (or not be); and help enemies to determine potential Army targets and classified locations.

An Army briefing on geotagging warns: "Something as simple as loading a photo of your bunk in Afghanistan ... can bring a mortar right into your area of operation."

Soldiers deploy to areas all over the world. Some locations are public, others are classified. Soldiers should not tag their uploaded photos with a location. Publishing photos of classified locations can be detrimental to mission success and are in violation of the Uniform Code of Military Justice."

Reminder: Users should never discuss military or government information while using social media sites. Check with the manufacturer or online to see how to disable GPS capabilities on your device.



Office of the Staff Judge Advocate
Legal Assistance Office
6450 Way Avenue
Fort Benning, GA 31905
706-545-3281/3282