What is GeoTagging?

A new function of many computing devices-including smart phones, some digital cameras, and even portable game systems (in some cases)-is the ability to track your location to near-GPS precision. While this feature is for "location services," which can be fun or useful, they also present a risk.

In particular, many devices add location data to photos by default. Called "Geotagging," the data becomes part of the image file and goes wherever the image goes. By uploading or sending such images to the Internet, you may have provided an adversary with critical information.

Consider:

1. Public sharing sites like Flickr® or Google™ maps are public. An adversary can search by location to see who takes photos there and research the users who took the photos.
2. Even profiles that are set to "private" could compromise photos if the privacy controls are not set or used properly. The hosting service itself could sell or lose your data as well.
3. Pictures taken at sensitive locations can lead adversaries directly to supply depots, command centers, or our troops. Pictures taken from home (often found in the same user's profile) can also paint a target on our friends and family.
4. If many photos are available from the same user or a collection of related users (several people in the same military unit, for example), the adversary may be able to determine patterns of your activities.

What to do:

1. **Be Aware**. Now that you know about this capability, think twice before taking and sending photos. You can test to see if you have geotagging capability by taking a photo and checking properties in Windows® Vista, or higher. Some photo editors as several custom programs allow for the viewing and manipulation of location data as well.
2. **Evaluate the Need**. Do you have a specific point or purpose to tagging photos? If not, it's far simpler to disable the feature instead of trying to remember to "clean the photos later." Instructions for doing so can be easily found by searching for the model of your phone with the keywords "disable" or "geotag".

Bottom Line:

Even if posted briefly, photos can enable the adversary to capture vital information and record exact grid coordinates. Rather than risking "forget-then-regret," consider disabling the feature and thus avoiding the risk entirely.

Think before you upload!