# Geotagging Where Cyberspace Comes to Your Place

**Craig Valli and Peter Hannay**
secau – Security Research Centre
School of Computer and Security Science
Edith Cowan University
Mount Lawley, WA, Australia

**Abstract** - *The combination of GPS services and information technology is increasing with the use of geotagging now occurring as a default action in many commodity based devices functionality for example mobile phones and cameras. The camera in suitably enabled phones takes the picture and embeds GPS co-ordinates of the location into the metadata of the resulting image file. Furthermore there are now online services such as foursquare that are targeted at the geotagging or geocaching community. In addition to this overtly designed service other social online services such Flickr, Twitter are providing a means of geotagging users. This enablement of technology has significant and profound effects on bpersonal security and also extending into corporate security.*

**Keywords:** geotagging, geocoding, GPS, security, smart phone, Facebook, Twitter

## 1 Introduction

GPS technology is a stable mature technology, likewise mobile devices are becoming increasingly mature and more powerful. Recently 1GHz based smart phones have been released in large quantities, these devices have up to 64GB storage, 32MB memory, network connectivity, GPS, cameras and the ability to handle a variety of business documents. In addition to this many of these now are transforming into a mobile application platform with a high degree of personalisation and customisation with the introduction of Google's Android [1] and the Apple iPhone[2]. These devices are increasingly generating richer digital narratives of their users as they telecompute, connect to an increasing array of online services and facilities such as cloud computing services. This increase in narrative also makes these devices an increasingly attractive target for compromise for malfeasant behaviour or pure criminal behaviour.

One of the recent innovations enabled in these phones is the use of GPS services to tag location of where the device is, or a digital photograph was taken referred to as geotagging. The phones also compute location as an ongoing feature that is used to report location on social networking application and services when interacting with services. Many of these services not only utilise GPS, but also wireless access points and mobile telephony towers as an example the first generation iphone used Skyhook[3] to provide locational service by this vector. Some later devices are now using combinations of positional services to get even finer resolution of location. This paper will investigate the issues with the use of geotags from an aspect of personal privacy and security as well enterprise implications of same.

## 2 How geotagging works

Geotagging most commonly refers to the tagging of images with GPS location data. However the use of geotagging has been extended to include elements of objects on social media services such as Twitter and Flickr. The implementation details of both image and social applications of geotagging will be discussed below using these two services as examples.

### 2.1 Geotagging of Images

Geotagging in images involves the insertion of location data specifically latitude and longitude format into an image file. Insertion of location data can be performed as a manual operation or automatically by a location aware image capture device (commonly a camera or mobile phone) at the time of creation.

The Exchangeable Image File format (EXIF) is a published industry specification for the image file format used by digital cameras[4]. The location data is typically stored within the EXIF records for the image using the EXIF Global Positioning System sub-IFD that uses the TIFF Private Tag 0x882. The EXIF can also contain information that uniquely identifies the device that has taken the image as well. Graphics tools such as ExifTool are able to extract this extended device and locational data, likewise digital forensics tools are able to locate this data.

Both the iPhone and Android platforms have geotagging functionality built and bundled with the base operating system. These two platforms have been selected for this research as they are emergent and dominant in this appliance space. The geotagging/geocoding functionality is disabled for both platforms by default, however the iPhone will automatically prompt the user to enable the function when first launched (shown in figure 1 below). The Android platform provides no such prompt and instead requires the user to enable geotagging support manually (shown in figure 2 below).


Figure 1 - iPhone Location Warning

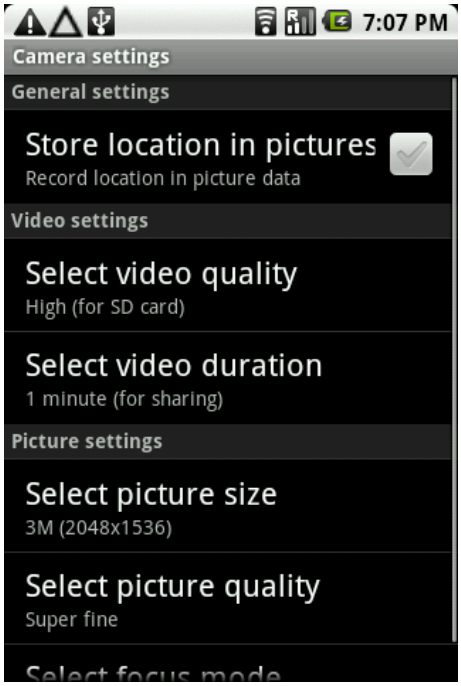


Figure 2 - Android Geotagging Setting

### 2.2 Social media as the enabler

Geotagging in social applications is achieved in much the same manner as that of images; however instead of tagging individual files, objects within a social media construct are tagged with geolocation data. The geolocation data is harvested from media at the time of upload or provided by the client application at the time of submission. There are a number of social media services that have enabled geolocation features, we will be examining two of the most widely known services in the social media arena: Twitter and Flickr.

### 2.3 Twitter

Twitter is a micro-blogging service that allows its users to post 140 character status updates. These status updates are then visible to the user's friends or the wider internet; this is dependent on the user's privacy settings. The ability to tag posts with geolocation information was added in November of 2009[5].The ability to submit geotagged status updates is not available on the Twitter website, however the ability to view geolocation data is present, this functionality is shown in the diagram below. There are a number of Twitter clients that support geotagging, the majority of these being for mobile platforms such as iPhone OS and Android.

Through the Twitter API there are a number of calls that exist to allow searching for posts. The utilisation of these calls provides the ability to search for posts based on a number of criteria, included in this is location and user details. In this manner it is possible to profile users behaviours or identify users which frequent specific locations.

### 2.4 Flickr

Flicker is a social photo sharing service, users are able to upload images to Flickr. These can then be viewed publicly or by a restricted group of people. This limit of distribution is determined by the security and privacy settings of both the user and the individual image itself. Geolocation support is present within Flickr and is achieved through the harvesting of geolocation data from the meta data of images as they are uploaded. Separate security settings exist for this functionality, however the recommend settings are that full public access be given to location data.

API calls available to developers allow for searches to be performed based on location, user and many other parameters (examples of this are present within the flickr directory). One possible application of this functionality would be the identification of images taken at a specific location at a specific time, for example it would be possible to search for all flickr images taken during an assassination within a certain radius of the event, the resulting images may provide additional intelligence aiding an investigation.

# 3 Issues with geolocational tagging

### 3.1 Internet/Social media enabled issues

Geotagging technology is a technology that brings about the intersection of cyberspace and real space, real object and real people. Already GPS style technologies can be used for a variety of good uses and reasons including the safe tracking and monitoring of the vulnerable i.e young children or senile seniors. These technologies however are normally a closed interactive loop and do not allow access to these systems by potentially any user of the Internet like some of the online systems do. The increasingly open nature of these systems brings with this openness a wide range of security issues, some of which will be outlined below.

An obvious and sinister use for this technology is the ability for the predator to track its prey. The combination of social networking sites and geotagging is one that could prove deadly. This combination of technologies delivers true cyber stalking capability to predators from the anonymity of cyberspace. An example of this enablement of this for criminality is the site called pleaserobme.com [6] that aggregated Facebook users holiday entries and indicated whether an individual was home or not. The use of geolocation tags allows for even more definitive answers to where a home owner maybe i.e you upload photos of your holiday to your favourite online photo repository indicating you are currently in another country.

Another example is the case of the apprehended violence order (AVO) where a person who is a stalker or previously been violent to another party can be required to remain a certain distance from the victim. In the cases of domestic abuse often the victim will relocate to another city or even state to feel safe. But how does the AVO translate to cyberspace if the victim is uploading pictures of themselves to a website and the assailant in this case then uses these to track or even worse locate the victim. This same scenario also has major impacts on current witness protection programs.

There are numerate cases where employers and employees use social networking sites to research one another. The use of geotagging adds an extra layer of information into this intelligence. This extra information then allows either side to examine wider the social interactions and relationships that a person holds with other parties.

### 3.2 Other potential issues and uses

Asset tracking software is available that reports the geolocation of an asset or even a vehicle. These are legitimate services that again are in typically closed systems and used is some cases as a layer of security to protect the asset or assets in transit. What happens when a guard for instance unwittingly leaves updates enabled on a phone to their social networking account and allows tracking of a goods transit or delivery?

What about a staff member who is being geolocated during a sick day off where they have taken a photo with a friend at a location like a movie theatre. What right does an employer have to use this information to track an employee's location and then deduct pay? Given that some phones and services are now bundled as part of the employment package and not as a result of the need for 24/7 response where does the work tracking end and start?

The use of geotags embedded in picture metadata provides an avenue for law enforcement to provide at least locational data for specific offences or incidents. The ability to search for images for instance that have a particular geolocation and time window may greatly aid law enforcement and agencies in the investigative process. These tags in of themselves may not be accurate to a room but may indicate a street or neighbourhood in which the offences occurred. This use will greatly enable police to follow up on crime and reduce workloads in gathering intelligence and locating crime scenes.

The use of geotags in forensic investigations has significant potential for making it possible to achieve rapid triage of crime scene or site mapping for disaster victim identification. Accurate geotagging will provide an enhancement to conventional scene documentation standards.

Much physical security is enabled by the fact that a location is unknown except to a few individuals however one geotagged image could undo this. This issue has significant implications for corporate security where staff may take workplace photos and for instance publish them on social media sites. This issue then enables the organisation or location to be located without the risk of discovery for instance associated with conventional physical reconnaissance.

# 4 Conclusion

Geotagging and geocoding present a use of technology that can be used in a variety of ways to provide information about location. The problem is that the information in of itself is not harmful but rather the exploitation of it by end users some with criminal intent is the issue. The issues with this amalgam of technology are manifest and profound, this type of combined technology definitely allows for the crossover linkage from cyberspace into the real world.

With many of the newer smartphones, cameras and other technologies now having this technology available it is imperative that companies and individuals who are serious about security including information, corporate, physical and personal re-evaluate their use of this type of technology. There also needs to be consideration of

sanitisation of image data by stripping or cleansing for these types of files before upload. It could be argued that sites that have a true interest in the users privacy could enable this as a feature for uploading the material in the first place.

Finally, the use of this technology also has large impacts on society at large but in particular the law and how it relates to this particular technology set. As mentioned in this paper how does the law now deal with technology that transcends cyberspace to real space and vice versa.

# 5 References


[1] Google, "Nexus One - Web meets Phone," 2010.

[2] Apple, "Apple - iPhone 4 - Video calls, multitasking, HD video, and more." vol. 2010, 2010.

[3] Anonymous, "Skyhook Wireless: How it works?," Skyhook Wireless Incorporated, 2010.

[4] CIPA and JEITA, "Exchangeable image file format for digital still cameras: Exif Version 2.3," Japan Electronics and Information Technology Industries Association 2010.

[5] Anonymous, "Think Globally, Tweet Locally," twitter.com, 2009.

[6] B. Borsboom, B. VanAmstel, F. Groeneveld, and Forthehack, "pleaserobme.com," 2010.