ISSN 2320 2610
Volume 2, No.4, July - August 2013
International Journal of Multidisciplinary in Cryptology and Information Security
Available Online at http://warse.org/pdfs/ijmcis01242013.pdf

Revealing the Unseen in Social Networking Sites: Is Your Metadata Protected?

April L. Tanner, Ph.D.[1], Sedrick Jefferson[2], Gordon Skelton, Ph.D.[3]
[1]Jackson State University, USA, april.l.tanner@jsums.edu
[2] Jackson State University, USA
[3]Jackson State University, USA, gordon.skelton@jsums.edu

ABSTRACT

The increased usage of mobile devices, equipped with digital cameras, has allowed users to take photographs and share them more easily and more quickly than in the past. Everyday thousands, if not hundreds of thousands, of photos are uploaded to social networking websites using computers and mobile devices. It has been said that "a picture is worth a thousand words" but now we must consider the additional information contained within these pictures taken with digital devices. This additional information, also known as metadata, can contain information such as the date and time the picture was taken, the make and model of the camera used to take the picture, and geographic location information or geographic metadata. Geographic metadata also provides valuable information such as latitude and longitude coordinates, altitude, and GPS time and date stamps using the Coordinated Universal Time (UTC) system. This information can be used to pinpoint the exact location where a picture was taken, and it can be used by criminals for their unlawful endeavors. In this paper, we will evaluate whether popular social networking sites are protecting their users' picture metadata by performing an experiment to determine whether this metadata is accessible after it has been downloaded from these social networking websites. Risks associated with privacy and possible solutions, techniques, and tools to remove metadata in photographs uploaded to social networking sites will also be presented.

Key words: metadata, mobile devices, privacy, social networking.

1. INTRODUCTION

Facebook, Instagram, LinkedIn, Flickr, and MySpace are all social networking sites that allow its users to upload their photos to connect and share with others. In 2012, Facebook users uploaded over 250 million photos each day and over 5 million photos were uploaded to Instagram daily, increasing from a total of 150 million in 2011 [1]. Although many of these sites offer privacy controls to its users, we must also consider if other measures are being taken to protect the unseen data contained within photos uploaded to these sites.

This research was funded by the US Department of Energy (DOE)/ National Nuclear Security Administration (NNSA) (Grant #: 240946).

A digital photo is not just a digital photo anymore. Photos can contain additional information that can be used to acquire additional information that users are not aware of. This data, known as metadata, can be hidden within the images and can contain geographical information as well. According to [2], "recent implementations of GPS (Global Positioning System) technology to mobile phones have enabled user to easily apply geographical information to their photographs." In more recent years, the increased use of mobile devices, which generally include digital cameras and freely available apps or applications, has allowed more individuals to instantly add their photos to various social networking sites more easily, more quickly, and more frequently. With billions of images being uploaded everyday, who is ensuring that these images do not contain metadata? Do the privacy policies of the various social networking sites include clauses for removing metadata in photos uploaded to their sites? Is your metadata protected? In this paper, we evaluate whether social networking sites remove metadata from photos uploaded to their websites. We also address the risks associated with privacy on social networking sites and present practical solutions, techniques, and tools to remove metadata from photos prior to and after uploading them to social networking websites.

2. BACKGROUND

2.1 What is Metadata?

Metadata is commonly defined as “data about data.” Many users of digital devices know very little to nothing about metadata, even though, every digital file consists of some amount of metadata. Metadata’s prime purpose is to describe files, and the data that describes the files makes finding, identifying, and cataloging files easier. Using metadata promotes interoperability, which means it can be understood by people and computers using different operating systems and different physical components [3]. It also allows people, who are collaborating on a project, to make modifications without having to worry about the project having multiple copies generated due to revisions made by different members of the project [4]. According to the National Information Standards Organization, storing metadata with the object it describes "ensures the metadata will not be lost, obviates problems of linking between data and metadata, and helps

ensure that the metadata and object will be updated together" [5]. This is very important when working in large groups on single documents, especially when the document must be shared.

Metadata is automatically generated by the digital device that created it. This automatically generated data can be altered by any user with the proper metadata editing software. When a user creates a file, she can add additional metadata to the file to accompany the automatically generated data. Users also have the power to password protect metadata so that it cannot be altered by unauthorized users. Attached and embedded files in PDFs may have metadata that contains information such as author's name, author's address, author's phone number, and the network settings, that the author or an organization does not want shared [6]. Metadata is increasingly becoming more important in the field of cyber security. Computer forensics experts have used metadata to reconstruct data for use in criminal trials. In a sense, metadata can be perceived as the digital fingerprint of a digital file and can be recovered from digital devices by computer forensic professionals.

2.2 Types of Metadata

According to [3] and [7], metadata is data that describes data and serves as a convenience for users. Metadata allows resources to be found by relevant criteria, identifies resources, brings similar resources together, and helps eliminate duplicate data files [3][4]. Metadata is most popular for allowing discovery of important information on specific topics. Since metadata is interoperable, it allows people to work with digital files on computers without any restricted access or implementation [3][4]. Five types of metadata presented are technical, descriptive, structural, administrative, and geographic. According to [5], each type of metadata has a purpose to "facilitate the discovery, management, and reusability" of digital data.

Technical metadata's characteristics include file-characteristics metadata, source metadata, and process metadata. File-characteristics metadata provides technical information about the formatted digital file, source metadata provides technical information about analog or digital source items, and process metadata provides technical information about the technical processes in converting single source items into digital files provided by file-characteristics metadata [8].

Descriptive metadata describes a resource for purposes such as discovery and identification [3]. According to Oxford Digital Library it is "information describing the intellectual content of the object, such as Machine-Readable Cataloging (MARC) records, finding aids or similar schemes" [9]. Descriptive metadata can be entered into digital files manually. Data that can be entered includes basic "bibliographic information such as the creator, title, creation data, and catalog information such as accession or other identifying numbers" [10].

Structural metadata indicates how compound objects are put together, and how it may be used "to represent the physical or logical structure of a complex object" [3][11]. These objects consist of pages, chapters, tables of contents, indexes, appendices, and others. In cases were objects have limited length, structural metadata may not be needed because the descriptive metadata may be sufficient enough [11].

Administrative metadata provides information to help manage a resource [3]. According to [5], administrative metadata includes "information on creation, quality control, and rights, and preservation." Similar to descriptive metadata, data related to the creation of a file, data that tells the version or edition of a digital file, and data that shows ownership or rights are all examples of administrative metadata. Most administrative metadata is intertwined in the descriptive metadata [25].

Geographic metadata, also known as geospatial metadata, is metadata that is associated with some point on the surface of the earth. Geographic metadata has been around for over 20 years and The National Aeronautics and Space Administration (NASA) was one of the first organizations to make use of geographic metadata [12]. Due to the World Wide Web's (WWW) fast pace and rapidly changing internet technologies, geographic metadata has gone through changes. After geographic metadata became more popular, the International Organization for Standardization (ISO) released the document ISO 19115 "Geographic Information Metadata." This document was established as a guideline for geographic metadata standards. As the web became more advanced, Extensible Markup Language (XML) made use of geospatial metadata. Now, Geography Markup language (GML), a XML extension, is the most widely used format to associate geospatial metadata to maps, charts, photos, and more [26].

Metadata is simplistic, yet complex in that there are varying types and each type can be interconnected, in some way, with each of the other types of metadata. As was discussed previously, different types of metadata can be embedded in digital image files, and this data can be encoded in different formats.

2.3 Embedded Metadata Formats

Dependent on the type of file, metadata can be encoded in different formats. For instance, metadata embedded in images can be stored in EXIF (Exchangeable Image File Format), XMP (Extensible Metadata Platform), and IPTC (International Press Telecommunications Council) formats.

This research was funded by the US Department of Energy (DOE)/ National Nuclear Security Administration (NNSA) (Grant #: 240946).

IPTC was the standard developed in the 1970's for exchanging information between news organizations and has evolved over time. In 1994, Adobe Photoshop's "File Info" form enabled users to insert and edit IPTC metadata in digital image files [13]. XMP is an extensible markup language used for storing metadata in digital photos. XMP was developed by Adobe in 2001 and was later modified by incorporating the old "IPTC headers" into the new XMP framework [13][15]. Now, XMP is an open-source, public standard that makes it easier for developers to adopt the specification in third-party software [13][14]. Furthermore, the XMP model is "applied to geotagging proprietary information related to a file, as it is processed through photography, scanning, texting or editing, additionally enabling the integration of other attributes along the way" [13][14].

EXIF is the most popular metadata format in digital photography. Currently, EXIF standards are supported by JPEG and TIFF. It can easily be read by online or offline applications. The EXIF format has standard tags for location information. Included in the EXIF's standards are the specifications "for image formats like JPEG and TIFF, [which] includes the camera setting, the shooting environment as well as the geographic information" [16]. Various methods and tools for storing metadata are available for use. These tools can be used to embedded and extract metadata from files.

2.4 Metadata Tools

Metadata can be viewed, altered, and organized by free or commercial tools available on the Internet. Many of today's photo-editing and photo management software offer capabilities for embedding and editing metadata in image files. Some of the metadata editing programs allow users to password protect metadata so that no other user can delete or alter the metadata. These programs also allow users to completely strip files of almost all of the metadata associated with them [17][18].

Jeffrey's Exif Viewer, Opanda IExif, Opanda PowerExif, and PhotoMe are tools that can be used to view metadata contained in image files. Jeffery's Exif Viewer is free tool that provides users with the complete information of an image, which includes basic metadata like description, keyword, image shot date, GPS encoded location, focal length, zoom ratio, exposure time, shutter speed [19]. In addition, it shows all hidden data in an images, text, and audio files. Photos encoded with geographic location have Google Maps embedded within the summary area of the software. Opanda IExif's free version only allows users to view metadata attached to digital pictures. The paid version of Opanda IExif allows users to delete all metadata, delete some fields, alter any field, and add new fields. Opanda PowerExif and PhotoMe are commercial that allows users to add, modify, and delete photographic data contained in Exif tags of digital images from mobile devices or scanners [20]. Metadata in mobile devices can pose a threat; in addition, most users of digital devices are unaware of what metadata is and the risks associated with using GPS enabled devices to upload their photos to social networking websites.

2.5 Risks Associated with Geographic Metadata in Image Files

Many new smart devices (such as phones and tablets) are capable of attaching geographic metadata to photos and videos. Geographic metadata displays the longitude, latitude, and altitude information of where a picture or videos was taken. In mobile digital devices, metadata such as the time stamp, longitude, and latitude can be used to identify places people have been and when the places where visited [21]. Users, who take pictures using mobile devices and upload those pictures and videos to social networking sites, may be giving stalkers or burglars' information that can be helpful in determining when a user is not at home or where the user is at a given time. Simple examples, that show how metadata uploaded to a social network may cause harm, are provided below.

Figure 1 presents a photo obtained from the Flickr social networking site. As shown in the figure, a dot on the state of Missouri on the map is indicated. Above the map is a sentence that tells when the picture was taken and the city and state the picture was taken in. The user clearly stated that she was on vacation. In addition, this picture was open to the public. Such an innocent photo could be very useful to criminals interested in breaking into this user's home. The photos, located at the bottom of the Figure 2, were taken at random locations and uploaded to Flickr.com. After the pictures were uploaded to Flickr, the map tab was chosen and it displayed the location of where each picture was taken using the pictures' geographic metadata. This map could be used by anyone, especially criminals, to determine places a person's general location and places a person has visited.

Flickr, a social networking site, is dedicated to photo sharing that involves user interaction. Flickr allows its users to upload the geographical metadata of pictures or to add geographical location information, manually online. For instance, if no geographical location information is provided for a photo, users are still encouraged to share their location information by simply "dragging the photos to a particular point on the world map" [22]. Furthermore, when manually geotagging photos, Flickr often suggest the location of the last uploaded photo or simply displays the world map [22]. In addition to Flickr, several other social networking sites provide its users with the ability to upload photos to their websites. In this paper, we examine several social networking sites' abilities to remove metadata from files uploaded to their sites and present the experimental results.

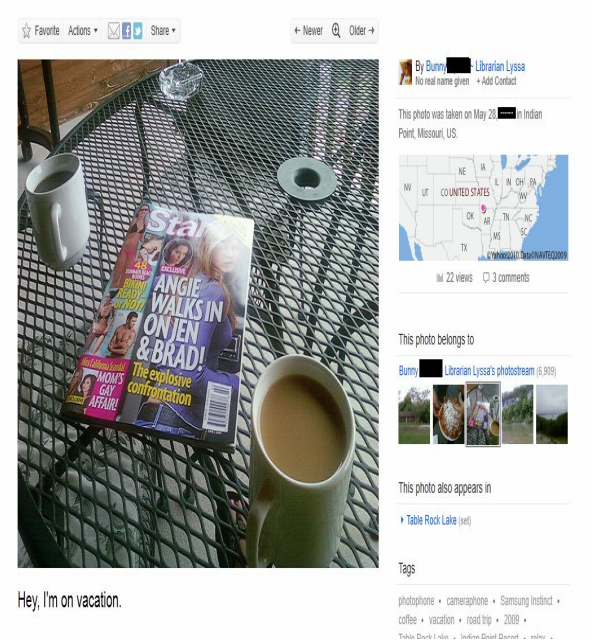

Figure 1: Example of Photo Indicating User's Status and Location [13]

3. EXPERIMENTAL DESIGN AND IMPLEMENTATION

The goal of this research was to determine whether social networking sites removed metadata from photos uploaded to their sites. Two GPS-enabled smart phone camera-equipped devices (Android and iPhone) were used to capture and upload metadata embedded photos to the twelve social networking websites listed in Table 1. In addition to their GPS capabilities, these devices were chosen because they allowed users to quickly upload photos directly from their devices to these social networking sites.

Two tools, Jeffrey's Exif Viewer and Opanda PowerExif 1.2 Professional, were used to view the metadata contained in photos before and after uploading and downloading the photos to and from social networking sites. Jeffrey's Exif Viewer extracted metadata from photos directly from the social networking sites; whereas, Opanda PowerExif was used to confirm the presence or absence of metadata, contained in photos, prior to uploading and after the photos were downloaded from the social networking sites. For example, Figure 3 provides an example of a photo taken using an HTC Evo 4G Android device. The metadata contained within the photo is provided to the right of the photo.

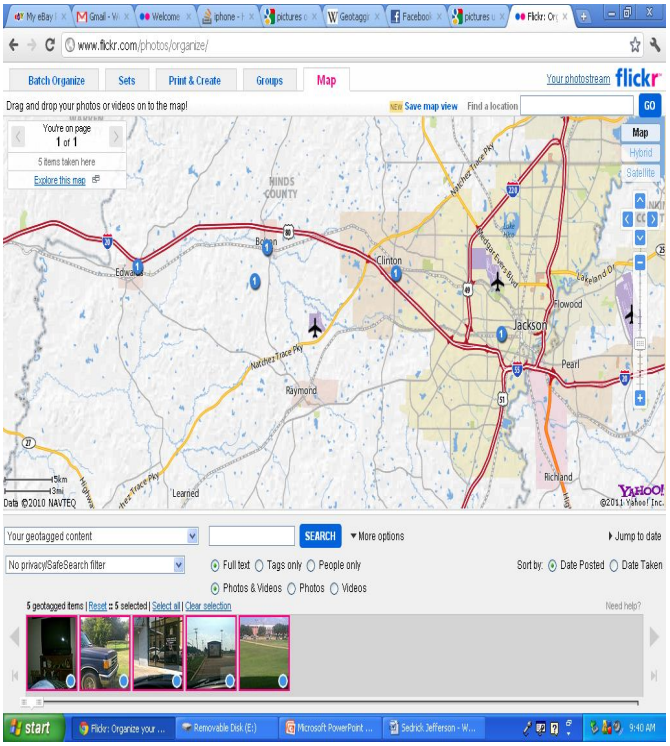

Figure 2: Example of Several Photos Uploaded to Flickr Pinpointing the Route Taken Using Map View

The metadata provides the type of device used, including the model number, the date and time information of the photo, and GPS information, which includes the latitude and longitude coordinates, altitude, the GPS date stamp, and the type of file (JPEG). This information can be very beneficial for criminals or terrorists seeking to determine the location of individuals for the purposes of burglarizing their homes, stalking them, or committing murder.

During implementation, several tasks were performed to determine whether photos containing metadata retained their metadata after they were uploaded to sites. First, several photos were taken from each of the GPS-enabled smart phone devices. Second, the metadata contained within each photo was verified using the Opanda PowerExif 1.2 Professional software tool. Third, a user account was created for each of the social networking sites and the social networking applications were downloaded to each device. One photo was selected from each device, and that photo was uploaded to each of the social networking sites. Next, the uploaded photos were downloaded from each site either via a download link on the site or by right clicking and saving the picture to the computer. Lastly, each photo was again checked using the Opanda software tool to determine whether any metadata information was retained.

Table 1: Listing of Social Networking Sites Tested

MySpace	Flickr	Twitter (Twitpic.com)	Bebo
Facebook	Black Planet	Orkut	Badoo
Google+	LinkedIn	Tagged	Foursquare

In addition, Jeffrey's Exif Viewer was used to extract metadata directly from the photos on the social networking sites using the photos' web address link. The web address link was copied and pasted into Jeffrey's Exif Viewer and the tool displayed any existing metadata in the photos without having to download the files to the computer.

Two tools, Jeffrey's Exif Viewer and Opanda PowerExif 1.2 Professional, were used to view the metadata contained in photos before and after uploading and downloading the photos to and from social networking sites. Jeffrey's Exif Viewer extracted metadata from photos directly from the social networking sites; whereas, Opanda PowerExif was used to confirm the presence or absence of metadata, contained in photos, prior to uploading and after the photos were downloaded from the social networking sites. For example, Figure 3 provides an example of a photo taken using an HTC Evo 4G Android device. The metadata contained within the photo is provided to the right of the photo.

The metadata provides the type of device used, including the model number, the date and time information of the photo, and GPS information, which includes the latitude and longitude coordinates, altitude, the GPS date stamp, and the type of file (JPEG). This information can be very beneficial for criminals or terrorists seeking to determine the location of individuals for the purposes of burglarizing their homes, stalking them, or committing murder.

During implementation, several tasks were performed to determine whether photos containing metadata retained their metadata after they were uploaded to sites. First, several photos were taken from each of the GPS-enabled smart phone devices. Second, the metadata contained within each photo was verified using the Opanda PowerExif 1.2 Professional software tool. Third, a user account was created for each of the social networking sites and the social networking applications were downloaded to each device. One photo was selected from each device, and that photo was uploaded to each of the social networking sites. Next, the uploaded photos were downloaded from each site either via a download link on the site or by right clicking and saving the picture to the computer. Lastly, each photo was again checked using the Opanda software tool to determine whether any metadata information was retained.

In addition, Jeffrey's Exif Viewer was used to extract metadata directly from the photos on the social networking sites using the photos' web address link. The web address link was copied and pasted into Jeffrey's Exif Viewer and the tool displayed any existing metadata in the photos without having to download the files to the computer.

Figure 3: Example of Photo Taken Using Smartphone and the Metadata Embedded Within the Image

4. RESULTS

The results of the experiment showed that each of the social networking sites in Table 1 removed metadata from the photos uploaded to their sites. Table 2 provides the findings of each social networking site where the Jeffrey's Exif Viewer tool to verify if metadata still remains after the file has been downloaded from the sites via web address links. As shown in Table 3, Flickr and Foursquare, removed the metadata from the pictures, however, they also provided the location of where the picture was taken by depicting it on a map.

Although the exact longitude and latitude coordinates were not provided, indicating where the picture was taken, on a map, could still prove to be harmful to an individual. Flickr is a social networking site that is centered on photos and is widely used by professional photographers who love to use metadata and geographic metadata to archive their photos.

Table 3 lists the results of each social networking site that used the Opanda Exif Viewer tool to verify whether metadata persisted after the download of the photos. Similar to the results provided in Table 2, none of the social networking sites listed in the table failed to remove the metadata contained in the photos, but the location of where the picture was taken was still indicated on a map linked to the GPS information. Although two different devices were used to upload photos to the social networking sites listed in Tables 2

and 3, the same results were achieved using two different photos from two different devices. In addition, all of the images were of the JPEG file format. The results presented are encouraging. It is apparent that these social networking sites are taking the necessary steps to protect their users' photos. Moreover, Flickr also allows users to restrict access to metadata or to remove metadata from their photos.

Table 2: Metadata Recovered Using Jeffrey's Exif Viewer

Social Networking Sites	Metadata Present Before Uploading to Site	Metadata Present After Downloading from Site
MySpace	Yes	No
Facebook	Yes	No
Google+	Yes	No
Flickr	Yes	No*
Twitter (Twitpic.com)	Yes	No
LinkedIn	Yes	No
Orkut	Yes	No
Tagged	Yes	No
Bebo	Yes	No
Foursquare	Yes	No*
Badoo	Yes	No
Black Planet	Yes	No
*** indicates that the location of where the picture was taken was indicated to some extent on a map.**		

Table 3: Metadata Recovered Using Opanda Exif Viewer

Social Networking Sites	Metadata Present Before Uploading to Site	Metadata Present After Downloading from Site
MySpace	Yes	No
Facebook	Yes	No
Google+	Yes	No
Flickr	Yes	No*
Twitter (Twitpic.com)	Yes	No
LinkedIn	Yes	No
Orkut	Yes	No
Tagged	Yes	No
Bebo	Yes	No
Foursquare	Yes	No*
Badoo	Yes	No
Black Planet	Yes	No
*** indicates that the location of where the picture was taken was indicated to some extent on a map.**		

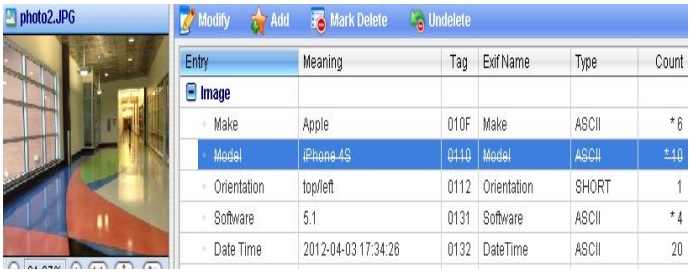

Figure 4: Displays Metadata Removal Using Opanda Power Exif

5. WAYS TO MINIMIZE RISKS ASSOCIATED WITH GEOGRAPHIC METADATA IN IMAGES

Geographic metadata can be removed from digital photos and videos using metadata removal software, but it is recommended that users become educated on how to prevent their mobile devices from attaching geographic metadata to their digital files. Various websites, such as "*I Can Stalk U*" and "*Please Rob Me*", seek to raise awareness about the dangers of geotagging [21][23][24]. Additionally, ICanStalkU.com, lists the steps needed to hinder specific mobile devices from attaching geographic metadata to photos and videos [3]. When using an iPhone or an Android device, users should first check their devices' Global Positioning Satellite (GPS) settings to make sure they are disabled before snapping pictures or capturing video. In most mobile devices, it is easy to disable location services within those devices.

In addition to disabling GPS capabilities on mobile devices, geotags can be deleted from existing photos by using a metadata removal tool. These types of tools allow the manipulation of geotags directly. Not only can extraction tools, such as Opanda Power Exif and PhotoMe, be used to recover metadata, they can also be used to delete metadata also. For instance, once an image, including its embedded metadata, are uploaded into this type of tool, options are available for adding metadata, editing existing metadata, or deleting metadata. Figure 4 displays an image and its metadata using the Opanda Power Exif tool. As shown, the metadata includes the make and model of the device used to take the picture, and it also provides the date and time information. To delete specific metadata, an individual can highlight that information and select the "Mark Delete" option to delete the desired information. Once the information is deleted, the metadata is highlighted and marked through to indicate that it has been deleted from the photo's metadata information.

6. CONCLUSIONS

The goal of this research was to determine whether social networking websites were taking the initiative to protect its users' photos by removing the metadata contained within them. It was shown that, of the twelve sites tested, all removed the metadata contained within the photos. However,

some websites still provided the map location of where the picture was taken, but it did not provide the actual GPS coordinates. Although metadata allows users to complete certain tasks more effective and efficiently, it can also be used inappropriately by others as well.

Given recent events and the ever-increasing importance of data, it is vital to know what information is being shared on publicly accessible websites. Many of the social networking sites are aware of this danger and some are trying to put a stop to this by utilizing numerous privacy policies and by removing metadata from photos. Users should take the necessary steps to insure that only the data they want to share is shared. Fortunately, there are several paid and free programs that can assist users in removing information that they do not want to share from their photos. Because so many users today use many different social network sites, the amount of information that can potentially be obtained is frightening. In some cases, bits of information on different sites can be pieced together to tell a whole story. As the digital world continues to progress, users should be constantly educating themselves and others about the potential dangers they may face with sharing too much information knowingly and unknowingly online. However, as long as individuals willingly continue posting information about their locations on these sites, there will always be security and privacy issues that will need to be addressed.

REFERENCES

1. B. Honigman. **100 fascinating social media statistics and figures from 2012**, http://www.huffingtonpost.com/brian-honigman/100-fascinating-social-me_b_2185281.html.
2. K. Hoashi, T. Uemukai, K. Matsumoto, and Y. Takishima. **Constructing a landmark identification system for geo-tagged photographs based on web data analysis**, *IEEE International Conference on Multimedia and Expo*, pp. 606-609, June 2009.
3. R. Guenther and J. Radebaugh. ***Understanding metadata***, http://www.niso.org/publications/press/UnderstandingMetadata.pdf, 2001.
4. K. Murphy. **Web photos that reveal secrets, like where you live,** 2011.
5. National Information Standards Organization. **Understanding metadata**, 2004.
6. National Security Agency. **Hidden data and metadata in adobe pdf files: publication risks and countermeasures**, 2008, http://www.nsa.gov/ia/_files/app/pdf_risks.pdf .
7. L. Rosenthol, **Metadata in p*df/a***, *2011*.
8. Federal Agencies Digitization Guidelines Initiative. **Technical Metadata**, 2012.
9. M. Popham. **Metadata in the oxford digital library**, 2005.
10. L. Newton. **How to geot-tag your photographs with Google maps**, 2012.
11. Yale University Library. **Best practices for structural metadata**, 2008.
12. L. Olsen. **What is dif**, *2010*, http://gcmd.nasa.gov/User/difguide/whatisadif.html.
13. P. Serdyukov, V. Murdock, and R. van Zwol. **Placing Flickr photos on a map,** *Proceedings of the 32nd International ACM SIGIR Conference on Research and Development in Information Retrieval*, pp. 484-491, July 2009.
14. PhotoMetadata.org. **Meta101: types of metadata**, 2012, http://www.photometadata.org .
15. Adobe Systems. **Metadata for digital asset management**, 2012.
16. A. Castiglione, G. Cattaneo, and A. De Santis. **A Forensic Analysis of Images on Online Social Networks**, *2011 Third International Conference on Intelligent Networking and Collaborative Systems*, IEEE, pp. 679-684, Nov. 2011.
17. Microsystems. **Filling the metadata gap: the next generation of metadata risks & solutions**, http://www.microsystems.com/pdfs/filling-the-metadata gap.pdf, 2011.
18. **Metadata, photography and workflow for the web**, http://www.oceanlight.com/log/metadata-photography-and-workflow-for-the-web.html, 2009.
19. Controlled Vocabulary. **Use Jeffrey's Exif Viewer to see Exif, IPTC, and XMP photo metadata**, http://www.controlledvocabulary.com/imagedatabases/exiftoolonline.html, 2012.
20. PhotoMe. **PhotoMe: digital photo metadata editor**, http://www.photome.de/.
21. J. Goldstein. **Privacy watch: cell phones, metadata and geotagging**, 2011.
22. A. Vila Tena and Y. Raivio. **Privacy challenges of open APIs: case location based services,** 2011 *Ninth Annual Conference on Privacy, Security and Trust*, pp. 213-220, July 2011.
23. D. Fletcher. **Please rob me: the risks of online oversharing**, *Time Magazine online*, Feb. 2010.
24. C.R. Vicente, D. Freni, C. Bettini and C. Jensen. **Location-related privacy in geo-social networks**, *IEEE Internet Computing, vol. 15, no. 3, pp.* 20-27, May 2011.
25. **Examples: administrative metadata**, http://www.uky.edu/Libraries/NDNP/administrative.pdf, 2011.
26. Federal Geographic Data Committee. **Geospatial Metadata**, http://www.fgdc.gov/metadata, 2012.