WINTER 2018 E-NEWSLETTER

At Digital Mountain we assist our clients with their computer forensics, e-discovery, and cybersecurity needs. For this E-Newsletter, we discuss social media discovery and important strategic legal insights and groundbreaking updates.

Social Media Metadata on Mobile Devices: Gathering Valuable Crumbs

If you're a fan of television crime dramas, chances are you're intrigued by how the smallest bits of evidence are often the very ones that end up closing the case on the identity of the criminal. Be it carpet fiber, a human hair, or the DNA from a single drop of blood, these infinitesimally tiny pieces of evidence can reveal vast amounts of information when handled by the right investigators. The same can be true of the small bits of information hiding underneath the content of social media postings made from mobile devices. In the hands of the right forensic examiner, the metadata behind the content can tell a lot about the briefest post. In this article, we'll look at the connection between social media apps for mobile devices and metadata collection.

What is Metadata?

In simple terms, metadata is data about data. There's a variety of metadata types, but for our purposes, we're going to restrict our discussion of metadata to machine-readable, searchable data that is generated in conjunction with content created on an electronic mobile device. The frontside data includes, but is not limited to, text and images. By way of analogy, if you look at a painting in a museum, the image in the painting your eye sees is the frontside data. The identity of the artist, the year the painting was created, the name of the painting, the type of paint used, and all other associated information are the metadata of the painting. We can't always read clearly the signature of the artist, but it's often there in the corner and if we search and squint, we might just make out a scrawled Monet. The placard of metadata placed on the wall next to the painting assures us that the painting is, in fact, a Monet. Similarly, the metadata behind a social media post can add context to content.

In the case of a social media post, frontside data is user-generated content, and often subject to ambiguity. Is that a picture of someone's actual dinner or is that a stylized meal from a menu or an advertisement? Did a hacker really post vile things on an innocent user's account, or is the

user covering his tracks? The metadata can often clarify content-origin questions as it is not generated by the user but by the device and the app used to post.

What Metadata is created by Social Media Apps?

There's a surprising amount of metadata created and archived by social media apps running on a mobile device, and the most concerning of which might just be geolocation data. Geotagging is the process of attaching location information to content. Thanks to technology advances, the accuracy of geolocating services is now in the region of fifteen feet for a smartphone with some sources claiming accuracy to within plus or minus a meter (3.28 feet). Other geolocation data includes elevation, distance, bearing, and the names of nearby places, in effect, placing the user on a map with impressive, or perhaps frightening, accuracy.

Geotagging metadata is ubiquitous in social media apps; so much so, that two Columbia University engineers were able to develop an algorithm which compares geotagged posts on Twitter with posts on either Instagram or Foursquare, to identify the owner of the accounts with a high degree of accuracy. One of the darker uses reported with respect to geolocation metadata is that it provides data that tech savvy criminals can use to create profiles of social media users to then physically stalk or commit home burglaries.

In addition to geotagging, social media app metadata can also include the type of device on which the post was created, as well as the operating system in use at the time. For an employer interested in the use of company owned mobile devices or the local law enforcement trying to trace the steps of a suspect, postings on social media which support the capture of device and operating system information is frequently valuable. In fact, in the novel case *United States vs Brown et al., (Case 0:11-cr-60285-CR-ROSENBAUM 2014)*, the US Government was ordered to respond to a request for cell phone metadata collected by the NSA that might have proven exculpatory of a defendant in a criminal case, in which the NSA was not a party.

If social media metadata can pinpoint location, device type, and operating system, is date and time information out of the question? It most certainly is not, and in fact, to ensure clarity, not only is time part of the usual metadata set, but time zones are often included, as well. Facebook, however, does allow the user to change a post's date as part of its editing menu, although any editing of posts is recorded in the post's history on-line.

Rounding out the metadata, social media apps may also include personal information input by the account holder (age, gender), unique identifiers, and subscription information including pages and causes followed by users. By compiling all the metadata, it's easy to see a fairly complete picture of the user's identity, location, the date and time, and the type of device used, making the information a valuable commodity.

Messaging apps, whether as add-ons to other social media apps or independent apps, harvest metadata not just from messages sent and received from that app, but can also gather data from mobile device contact directories and other messaging apps, including history. In practice, what users see is a messaging app asking if you'd like to import contacts from your phone, or, suggesting connections to other users of the same app based on entries in a contacts directory. If you enable the Calendar and Contacts settings under Facebook settings on an iPhone, your Facebook friends automatically populate your Contacts lists, which includes profile pictures as well as their email addresses and phone numbers (if the user made them public on Facebook). Birthdays and calendar appointments turn up in the iPhone Calendar app. This data is synced with the phone, so any changes will be pushed out to the phone. If a contact "de-friends" the user, their information will disappear the next time the phone is connected. Conversely, if the

Update All Contacts option is activated within the Facebook settings on the iPhone, Facebook information may be requested for a contact on the phone that may not be part of the user's Facebook friends. If you're someone who uses one device for both work and personal communication, this may be a concern.

Each social media app stores different metadata and the data stored may change over time. Additionally, smartphone forensics tools may not parse all the data. For example, within Chats, if you have the Facebook Messenger app downloaded, it will be rich with communication. However, other social media apps may not have communications parsed effectively by commercially available tools, so what you see may not be everything that actually exists. Reviewing applications on the smartphone is an important step in quality control of digital evidence. Additional custom parsing may need to be performed by a software engineer.

Special Considerations for Image Files

Metadata associated with image files often originates with the camera of the mobile device, tying metadata to the image from the moment of capture. This metadata again includes location, date, time, and device identifying information. Often, this data is uploaded to social media apps right along with the image file, a process many photographers have relied upon to protect their creator's rights. In addition, images can be organized and searched based on their associated metadata. Most mainstream social media sites such as Twitter, Facebook, Instagram and Flickr strip all the metadata out of pictures uploaded. When in doubt, it's good to perform testing and validate what data is being captured as the social media sites and apps are always morphing.

An Exchangeable Image File Format, known as EXIF, is a standard by which formats for images and sounds captured by electronic devices such as smartphones and digital camera are specified. EXIF metadata includes date and time information, camera settings including the camera model and make, and information that varies with each image such as ISO speed information, a thumbnail for previewing the picture, descriptions of the photo, and copyright information.

Reducing Your Metadata Footprint

If you're concerned about how much metadata is being stored on social media apps, there are a few things you can do to reduce its generation:

1. Don't publish social media posts from a mobile device. If you're inclined to do so, turn off location tracking and sharing in the device's settings.
2. Convert photos to .png files before posting, and upload to social media from a computer as it removes metadata.
3. Connect to a Virtual Private Network (VPN) which protects privacy by masking the physical location of the devices connected. Be sure to check the VPN's site for directions on how to ensure that all devices connected to the VPN are fully masked.
4. Install an EXIF viewer to inspect and edit the metadata associated with photographs you wish to publish.
5. Practice good device and network security habits by frequently deleting cookies, browsing history, and using encrypted messaging.
6. Enlist the services of a reputable computer forensics service such as Digital Mountain to examine social media accounts and demonstrate what information is being collected in metadata.

Metadata, like so much of the data and technology with which we engage, has its positive and negative attributes. The key to keeping metadata on the right side is to understand its collection and use, so that we're not inadvertently leaving tiny crumbs of electronic evidence without our knowledge. Metadata has positive attributes in validating authenticity, and hence, knowing we're dealing with an original Monet and not a copy.

Please direct questions and inquiries about cybersecurity, computer forensics and electronic discovery to info@digitalmountain.com.

UPCOMING INDUSTRY EVENTS

MASTERS CONFERENCE
Dallas, TX: February 28, 2018

THE ASU-ARKFELD 7TH ANNUAL EDISCOVERY
Phoenix, AZ: March 6-8, 2018

SECURING THE FUTURE OF THE INTERNET OF THINGS
San Francisco, CA: March 6-7, 2018

SYMPOSIUM ON SECURING THE IOT
San Francisco, CA: March 6-7, 2018

ABA TECHSHOW 2018
Chicago, IL: March 7-10, 2018

Click here to see more upcoming events and links

Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at various upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com.

DIGITAL MOUNTAIN, INC.

4633 Old Ironsides Drive, Suite 401
Santa Clara, CA 95054
866.DIG.DOCS

www.digitalmountain.com

Contact us today!

FOLLOW US AT: