The Secret Life of Metadata

Author : Cat

Date : October 5, 2015

The word 'meta' is used to describe something that is contained within itself. The term 'metadata' is then the information about other information. This is not specific to digital data, technically a table of contents in a book is data about data, but online we use metadata to encompass a lot more than an index. Though mostly helpful, sometimes the digital metadata we create can breach our privacy. The best defence we have is to understand what it is, when it is generated and how we can limit its distribution.

Each time you create a digital file, that files gets tagged with numerous data, which is its metadata. Depending on the application, some of the data is visible and accessible and some is hidden. A basic example would be a Word file on your computer. When you create the file, you can access things like file size, time of creation, author, and last edit. Additional metadata will include every access date, older revisions of edits and potentially the location from which it was accessed. This second set of data is retrievable via software forensic tools. Many of these tools are available free online, others are run by law enforcement agencies to catch criminals using digital data.

What complicates things is the transfer of information online. Each time we interact with the internet, metadata is being created to track those emails, images and app use, and we can't even see it happening. Additionally, because we are able to have handheld devices with us, we are also generating use data that describes patterns in our day.

In a day, my device would have logs of the following information:

- When my alarm goes off
- All instances when I check my email, browser, social channels and apps
- My location at all times of the day (if geolocation is turned on)
- All phone calls, texts and email messages

The collective data would easily give you patterns on my schedule (home - kids' school - work - kids' school - after school lessons - home), my most frequent contacts, as well as details on my interactions. This kind of information is invaluable to companies selling you product in addition, sadly, to those wanting to use it for malicious purposes. So how do I keep that kind of data *on* my device and make sure I am not giving it away? There is no simple answer but here are the three biggest areas of concern.

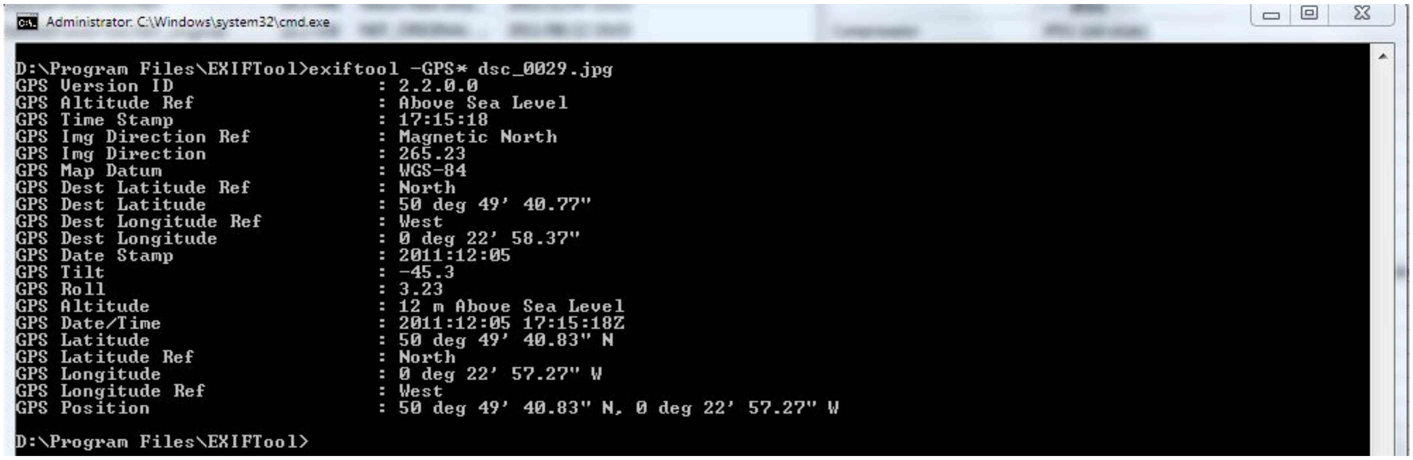
Location Services

One of the big advantages to handheld apps is the ability to tailor your information to where you are. Think maps, weather, news and restaurant locators. The problem here is the exchange of your location with the service you are using. Depending on the app, this exchange may only happen when you need to use it. In other cases, the app may be continually sending your location to the service so it always knows where you are. Since this data is sent as metadata, you do not see its transfer or frequency.

On my device I have turned my Location Services off. When I need a map application, I turn it back on. You may not feel the need to go that far. If you do, try a Google search on *your* device since settings differ between both device type and software versions. For some devices the location services can be turned off for each app, in other cases you need to turn it off at the main settings for your whole device.

Images

The digital image metadata is called EXIF (Exchangeable image file format). It holds a myriad of information ranging from the camera used to take the photo to the aperture length. Typically the most concerning of the data is again the location. Below is a capture of some location data scraped off of a photo using a readily available forensics tool called *EXIFTool*. Here you can see the details including the exact time the picture was taken along with its position.. right down to the tilt and roll. Unless you have turned off *geotagging* in your location services (above), this kind of information is being attached to every photo you take. The worry is that most people like to share and post their device photos. That means anyone can capture your location from your bedroom to your school or workplace. Bigger services, like Facebook, Twitter and Instagram, started stripping this data off a few years ago. From a safety/security perspective, this is a big relief. That said, professional photographers have argued this may have been done so that the copyright is also effectively stripped thus allowing sharing of the photo without breach of terms and conditions.



```
D:\Program Files\EXIFTool>exiftool -GPS* dsc_0029.jpg
GPS Version ID                  : 2.2.0.0
GPS Altitude Ref                : Above Sea Level
GPS Time Stamp                  : 17:15:18
GPS Img Direction Ref           : Magnetic North
GPS Img Direction               : 265.23
GPS Map Datum                   : WGS-84
GPS Dest Latitude Ref           : North
GPS Dest Latitude               : 50 deg 49' 40.77"
GPS Dest Longitude Ref          : West
GPS Dest Longitude              : 0 deg 22' 58.37"
GPS Date Stamp                  : 2011:12:05
GPS Tilt                        : -45.3
GPS Roll                        : 3.23
GPS Altitude                    : 12 m Above Sea Level
GPS Date/Time                   : 2011:12:05 17:15:18Z
GPS Latitude                    : 50 deg 49' 40.83" N
GPS Latitude Ref                : North
GPS Longitude                   : 0 deg 22' 57.27" W
GPS Longitude Ref               : West
GPS Position                    : 50 deg 49' 40.83" N, 0 deg 22' 57.27" W

D:\Program Files\EXIFTool>
```

App Requested Data

The operating system of your device should present you with a set of access requests to accept when you start a new application. Some of them may include access to your contacts, email or location. Sometimes this access is needed to run the application, and sometimes it is additional data the app makers want to have. Downloading to a computer or laptop is more difficult to control because the operating system does not control the application integration like it does on a handheld. In all cases, unseen metadata may be sent to the app makers. To protect yourself, I tell both kids and adults to consider the following:

- Do I trust the source of this application? Be sure to download only from the App Store of a device, not a website unless trusted.
- Does this app need **that** information? If not, deny access or find a different version of the app. A flashlight should not need location and a sudoku game does not need contacts.
- If it's free, it may be too good to be true. Free games or apps may be a lure to access other info from you and your device. Be wary.

Since devices and technology are here to stay, so is metadata. Be aware of the apps you are using and how you are connecting with them. Turn off the data you do not want shared. As always, *free* online services are an exchange for information. How much you give and take are always up to you.