Metadata

Another term I'm going to be using that you need to know and understand is *metadata.* Metadata is any data that doesn't directly expose any sensitive information, but can be used to expose information about us. For example, **Hold several books up** libraries use metadata to sort books by *title, author, and publishing information. Having 2 of any of these three 3 things is enough information to find that book, open it up and view the contents.* This is very similar to our digital lives; where even though your messages may be encrypted, there could be metadata collected like who's talking to who at what time for how long, all things that can be used to figure out what is being said.

We're going to explore this further after a quick message...

Promotional Spot

A post by Kurt Opsahl from the *EFF, a digital rights group*, gives a few examples as to why metadata can be so dangerous.

They know you rang a phone sex service at 2:24 am and spoke for 18 minutes. But they don't know what you talked about.

They know you called the suicide prevention hotline from the Golden Gate Bridge. But the topic of the call remains a secret.

They know you spoke with an HIV testing service, then your doctor, then your health insurance company in the same hour. But they don't know what was discussed.

So just because the contents of the call or message are confidential, doesn't mean there isn't data being collected that can give more than enough information to figure things out. Metadata isn't inherently harmful and has been in our society for thousands of years. The issue is that it's being utilized as a method to track users.

One organization who abuses metadata is *FISA, who oversees all requests for surveillance warrants against foreign individuals in the US,* which seems reasonable since it requires a court order. *The problem is that in 2012, 1,856 requests were presented, and 1,856 requests were approved,* suggesting that the process today is largely a political coy to make it appear like there's selection in these surveillance decisions. After the FISA court grants a request, law

enforcement can force private corporations to turn over all of your data and specifically metadata-- *assuming they haven't already done so.*

Now you might be saying, this doesn't impact me, I'm not one of those 1,856 people. Well if you're following the tips in this course, you could raise a lot of suspicions, so yes it still may concern you, even if you don't do anything illegal. On top of that, one person can ruin it for everybody. When the FBI was trying to get Edward Snowden's emails on Lavabit, *they forced Lavabit to hand over the SSL keys which wouldn't just let the FBI access Snowden's keys, but everyone on Lavabit, giving access to all Lavabit user's private emails. When the FBI wanted Apple to unlock the single iPhone from the San Bernardino case, it meant installing a backdoor which would give them access to any iPhone around the world.* When VPN companies are forced to keep logs to catch a user, it typically means keeping logs on all users in a server. So yes, you might not be committing the crime, but you're suffering the privacy invasion, which (without getting too off topic) is why metadata can be just as revealing as the contents in your texts, emails, and operating systems.

A person who fell victim to metadata was *John McAfee, a cyber-security expert, and although people don't typically like him as a person, he spreads a lot of good information related to privacy and security.* He developed the *McAfee antivirus which many of you might be using right now.* McAfee didn't have the cleanest life though, as he admits to *living sexual fantasies with guns and bath salts in Belize, where he was accused of killing his neighbor.* He eventually fled and went into hiding. So how did law enforcement find him? It wasn't from his blog post detailing what happened, it was actually from a picture he posted on Twitter. *The picture contained exchangeable image file data, or EXIF data, which is photo metadata. It includes things like color saturation and other color details, as well as the exact location that a picture was taken.* This is how he was eventually tracked and this is why your camera on your smartphones asks for your location the first time you start it up. *McAfee did sneak by all of this and ended up running for US presidency in 2016 for more cyber friendly policies. Lately he's become fascinated with blockchain technology* and is always saying the next "out there" thing. Really interesting dude.

To view the metadata of your files, you can use sites like these to see what kind of information there is on a file. There are programs and sites out there that claim to delete metadata on your files, so definitely take a look at them. *For Android, there's Scrambled EXIF, photexif for jailbroken iOS devices, viewExif for non-jailbroken iOS devices, and the LiveOS tails includes a tool as well, we will discuss Tails in section 4 of the course.*

Queue Outro Promos

And that is it! Thank you for watching, I know this stuff might not be the most fun to learn about, but it is necessary to know and it only gets better from here. We have to cover all the basic terms so we can learn about the advanced things later on in the course. I'll see you in the next lesson, discussing a neat thing *called The Convenience Line.*