LTT LAW TECHNOLOGY TODAY

PANDORA'S FORENSIC BOX: THE DATA YOU DIDN'T KNOW EXISTED

Wes Johnson | April 3, 2020

You've likely heard the reference to Greek mythology's "Pandora's Box". Something that at first seems valuable but then presents unexpected troubles. While many things in our culture could fall into that category, one such "Pandora's Box" that I deal with daily is technology. It is an undeniable asset in many scenarios, but it can also become a "curse" against its owner in legal matters.

The "curse" results from users being unaware of the data accessible on their devices and how this data can be forensically collected and used as evidence in litigation. Whether it's to prove innocence or guilt, this data is extremely valuable to attorneys, as it could be what makes or breaks a case. Here are three common types of data that many people don't realize exist:

continued next page

Location settings on iPhones

Most iPhone users have been cautioned to turn off location settings for certain apps, or at least change the settings to only track their location while they're using the app. However, few people realize there's yet another level of tracking taking place – and that feature is set to "on" by default. You can see the data for yourself in Settings --> Privacy --> Location Services --> System Services.

This location data is necessary for many of the system processes we love, such as apps like "Find My iPhone" (or "Find My" on newer devices), location-based ads or Google searches, or updating your time zone while traveling. However, it can also be incriminating if it puts you in a suspicious place at a specific time.

Forensics professionals can make a forensic image of the device and search through its location history to find data that supports their case. Known as "significant locations," iPhones track the places you visit most often and the dates and times you visit them. That is why your phone might suggest the quickest route to get to and from work – it has learned the days and times you frequently travel that path. Curious what places your phone recognizes as significant? Within System Services, tap Significant Locations, and you'll find a list of all the places you have visited often since you purchased your phone.

Android devices and Gmail accounts

Not surprisingly, Androids collect much of the same location data as iPhones do. That data is automatically linked to the Gmail account associated with the device (all Androids require a Gmail account in order to use many of the features). User activity is collected through Google Chrome and Google Maps and tied to Gmail accounts – so with more than 1.5 billion active Gmail accounts, Google gets a lot of data from its users.

In fact, Google currently collects more than 50 different categories of user data, including:

- Location history
- Web searches and website viewing history
- Shopping information
- What you've watched on YouTube
- Health activity data collected from connected fitness devices
- Audio of commands recorded on Android-based smart home devices, such as Google Home

continued next page

If you have an Android device, you can see the activity it stores by going to Settings --> Google --> Google Account --> Data & Personalization --> Activity & Timeline --> My Activity.

Social media

When signing up for a new website, many of us blindly accept its privacy policy without giving it a second thought. Unfortunately, that negligence can lead to consumers' data being used as evidence in court – even if they thought it was deleted.

Some social media platforms, such as Facebook and Twitter, have temporary deactivation periods prior to accounts being fully deleted. Both of these websites implement 30-day deletion policies in which a person's account and all its data is stored for 30 days after the owner has "deleted" it. If the user attempted to hide incriminating evidence by removing his or her account, forensics professionals can discover that evidence, as long as they are acting quickly to preserve the data within the time constraint.

Once the 30-day holding period has passed, it becomes much more difficult to recover data from these social media sites, though it is sometimes still possible with a court request or subpoena. However, if the deleted information is significant enough, the simple act of deletion alone during a suspicious time frame could serve as sufficient evidence. In the end, it's essential to know what social media platforms could hold critical evidence, understand their privacy policies and act quickly to retrieve the data so that it can be presented during legal matters.

Tips for attorneys dealing with digital evidence

There are several different types of data that can be used as evidence, each with its own set of rules on how and when to collect it. Here are three tips for attorneys handling data:

Check to see if the data can be collected forensically
You may be surprised by the type of data that is tracked, not just by phones and computers but even digital assistants, video doorbells and gaming consoles like Xbox or PlayStation. These devices (and many others) can hold incriminating evidence. Alexa can hear suspicious activity or conversations, video doorbells can identify a person's location and gaming systems' chat features can hide questionable exchanges. The bottom line is that most devices connected to the internet are usually tracking some type of information, so you should talk with a forensic professional about any data that may be relevant to your case to determine whether or not it can be collected and used in litigation.

continued next page

Collect the data as soon as possible

Many types of data have time constraints, so it's important to issue a legal hold as soon as you're aware of relevant data. Some platforms have system policies (such as Facebook and Twitter's 30-day deletion policy), but other devices have user settings that allow the individual to elect how long the data will be saved before being overwritten. For example, users can choose to save text messages for 30 days before self-deleting, after which the information is irretrievable and therefore unusable in legal matters (that is, unless the texts are still saved on the recipient's device). Some messaging platforms allow the user to specify much shorter retention periods. The good news is that forensic tools are constantly improving to stay up-to-date with the latest technology, so just because it may not be possible to retrieve deleted data now doesn't mean it won't be in the future.

Work with a licensed forensic professional

We've already discussed the difficulty of knowing what data can be collected, how to legally collect it and when you should start. It's always a good idea to consult a forensic expert to discuss these variables. General technology experts have ample knowledge of the technology industry, but they probably aren't familiar with the tools and techniques required to defensibly collect the various types and formats of data. Trained forensics professionals, on the other hand, are aware of the many places data is stored, and they know how to collect it in a way that maintains the data's integrity while also capturing the metadata.

With more and more evidence being found online, it's wise to carefully consider a suspect's entire digital footprint and the evidence it may contain before litigation occurs. Forensics experts may be able to mine multiple sources and uncover data you didn't even realize existed – data that might even expose the smoking gun.

ABOUT WES JOHNSON

Wes Johnson is the senior digital forensic examiner at eDiscovery and digital forensics company BIA. He has more than 20 years of experience in forensically retrieving and analyzing computer evidence and providing litigation support. He has analyzed and presented evidence in cases involving theft of intellectual property, theft of trade secrets, fraud, breach of contract, Securities and Exchange Commission investigations, spoliation and destruction of evidence.