Even the most tech-savvy attorney has questions about how data collection works and what information is stored on mobile devices. What type of information can be found and produced from the device? Can deleted information be restored? Do you have to have the device’s password to collect the data?

The answers to these questions may surprise you. Today’s smartphones track our every move, and if users don’t properly protect their information – including messages, browser history, location information, data from third party apps and more – all of that data is available for collection.

Let’s look at the data stored on mobile devices in more detail and how you can protect it from collection.

LOCATION

Cell towers record the geo-location of every phone call. Photos are automatically geo-tagged when they are taken. When a Wi-Fi network is joined, that location information is stored. Myriad apps ask to use your location information. Basically, a mobile device holds tons of information about where the user has physically been.

That location information is recorded to increase the phone’s functionality: Facebook’s app can
tell a user where a message was sent from, for example, and your iPhone can remember where your house is if you set it. The Google Now service on a Google phone is a particularly effective stealth repository of geographical information, as it continually identifies and records a phone's physical location. Investigators can access this repository and get a complete history of where the phone has been and when it was at each location. And investigators don't even need the phone to access this information. They can get it all by logging into the user’s Google account. Obviously, having access to a detailed log of where someone was at any particular time of day could be quite valuable in some types of litigation.

A forensics expert can gather a geographic history from all of the data stored on a phone, not just location-specific apps like Google Now. Texts, photos, social media, exercise monitoring apps, GPS apps – anything that records data can be a source of location information. Software is available that scoops up all of this information and spits it out into a file. When this file is loaded into a program like Google Earth, investigators are able to plot out a history of where the phone has been, even, depending on the phone, linking photos to locations and when they were taken.

Keeping some of this location data is unavoidable because smartphones must communicate with cell towers to operate. However, there are ways to protect your information. For example, photo geo-tagging can be disabled, so the metadata won’t include latitude and longitude information. Location information can also be turned off for other services, like Google Now, which will prevent the data from being recorded and potentially collected for litigation.

MESSAGES AND OTHER DATA

Most people are aware that messages on the device can be collected, along with their time stamps. What surprises people is that even deleted messages can be acquired. When a text message or email is deleted, a flag is placed next to the item in the database, and it disappears from the user-facing part of the device, but the actual content stays stored on the phone and is kept there until it is eventually overwritten. So, while there is not an unlimited amount of messages stored on the device and able to be collected, deleted messages are easily recovered, especially if they were sent or received recently.

Full browsing history, including deleted information, can also be collected for litigation. When a site is deleted from the history, a flag is added to that record in the database so it doesn’t show up on the device. Just like with a computer’s browsing history, a record of visiting that site still exists in the database, so it can be collected. Information used by third party apps is also stored on the device – even for apps that are supposed to be secure or delete information. For example, even though messages sent via Snapchat “disappear” from the phone after they are viewed, the files are saved onto the device and can be collected.

The best way to protect messages, browsing history and application information from...
collection is to strengthen the device’s general security. Many phones ask users to create a four-digit passcode to lock the device, but these passcodes are actually fairly easy to hack since there are a limited number of combinations. Using a longer password with uppercase and lowercase letters, numbers and symbols makes it exponentially harder for anyone – including digital forensics experts – to break into your phone. Even computer programs designed to break passwords could take months or years to hack a relatively complex password.

The thumbprint is a newer way to lock and unlock a mobile device, but this can also create a privacy issue. Law enforcement cannot force someone to unlock a password-protected device (for now) because the password is protected intellectual property. If you use the thumbprint option, though, police in some jurisdictions can compel you to open your phone because the thumb is a body part and not intellectual property. To protect yourself, only use the thumbprint for activities on your phone after it is unlocked – like confirming app purchases – and stick to a complex password to get into the device.

New operating systems for iPhones and Google Android phones have made it much more difficult to break into a phone without a password, especially if the phone was powered off before it was handed over to a forensics investigator – in which case the investigator is largely out of luck without knowing the password. The reason is that these new operating systems require a passcode to be entered when the phone is powered back on. If this is not done, everything is locked down. The investigator can try running password-cracking software, but it may not always work. If these newer phones are already turned on, it is easier for a skilled forensics investigator to access the data without a passcode.

In civil litigation, the court typically orders the custodian to share the necessary passwords to access any devices that house relevant data. This opens the floodgate of data that could be relevant to litigation. Heavy phone users can have thousands of files stored on their devices without even realizing it. Attorneys need to be aware of the information that could be collected and produced from mobile devices at the beginning of a case because it could include data that the user thought was deleted.

Andy Spore is digital forensics analyst at Nashville-based DSi, which provides advanced eDiscovery and digital forensics services. aspore@dsicovery.com