2021 Annual Conference
June 16-18, 2021
Atlanta, GA

Hey Google: How Do I Handle Digital Evidence in Claims and Litigation?

The Cloud

Microsoft explains the cloud as follows:

"The definition for the cloud can seem murky, but essentially, it's a term used to describe a global network of servers, each with a unique function. The cloud is not a physical entity, but instead is a vast network of remote servers around the globe which are hooked together and meant to operate as a single ecosystem. These servers are designed to either store and manage data, run applications, or deliver content or a service such as streaming videos, web mail, office productivity software, or social media. Instead of accessing files and data from a local or personal computer, you are accessing them online from any Internet-capable device—the information will be available anywhere you go and anytime you need it."[1]

This is helpful, but in my estimation, there is still some murk. To explain this to a layperson I would describe the Cloud as,

"a bunch of computer servers owned by big companies like Apple, Amazon, or Microsoft that remotely store your data, like your photos, allow you to use their combined processing power, or stream media like Netflix and YouTube."

The Internet of Things would not be possible without the Cloud. For the Internet of Things to exist, there must be the ability to store massive amounts of data and process information over the internet with much greater processing power than you could ever do with your personal devices alone like your cell phone or laptop computer.

---

[1] https://azure.microsoft.com/en-us/overview/what-is-the-cloud/

The Internet of Things

The Internet of Things is having its own definition issues. IOT Agenda defines it as:

"The internet of things, or IoT, is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction."[2]

I would describe it the Internet of Things as "anything that is connected to the internet".

This means that a cow with a chip in its ear is as much a part of the Internet of Things along with your cell phone, computer, and smart watch.

Hyper-connectivity is the future, and this future means that more data than ever will be collected concerning our habits, location, activities, health, and financial information. Our virtues and vices will be stored electronically, and when data is collected and stored, it can often be recovered using forensic tools and methodology.

Data Repositories

There are devices that collect and transmit data, like sensors in your activity tracker collecting and transmitting your heart rate activity and steps. However, the data is usually not stored on the device itself. It is sent to a device with the processing power and storage capacity to handle the information that has been collected by the device. This would be considered the data repository. This is a benefit to digital forensic examiners, because these repositories are usually devices that have long been examined for evidence, like computers and cell phones.

Most data related to IoT devices can be recovered and collected from the devices themselves, computers, and cell phones, and how these devices act as "repositories" of data coming from IoT devices.

Keeping that in mind, there are unique preservation collection and preservation issues related to IoT data, as collecting the information sometimes must be done through cutting-edge or nontraditional methods within the digital forensic community. In these instances, it is paramount that the data collection be done in a way that complies with best evidence and acceptable industry standards for digital forensics when dealing with novel forms of evidence.

Common Types of Consumer IoT Devices

Wearable Technology / Activity Trackers

---

[2] https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT

Wearable technology, such as fitness trackers, can contain information about a person such as their heartrate, sleep quality, activity, including both normal activity such as walking and vigorous activity like exercising, among other data types. This information can be very personal and can be used for many forms of analytics to determine content viewing times, routes of travel, markers of healthiness and disease, or if your claims of physical activity match reality.

Global Positioning Systems (GPS) Devices and Data

Location data is often of great interest in a litigation matter when attempting to establish or challenge an alibi. Today, almost every smart phone has a GPS receiver. This GPS data is used to track your location even when you are not utilizing navigation software or applications. It uses this information to provide you with restaurant recommendations near you, tag your Instagram photos with the geo-location data, allow you to see who is near you from your LinkedIn network, or give you a heads up on how long the drive home might take with current traffic.

With GPS, each satellite in the system transmits navigation data toward the Earth that contains the position of the satellite, a time stamp and the health of the satellite. When a GPS device can receive signals from at least three satellites at once, the device itself can calculate its position in two dimensions, latitude and longitude. This process is called triangulation.

In order for a GPS device to calculate its position vertically for altitude, it must be able to receive signals from at least four satellites at the same time. This process is called trilateration.

The satellite signal data is refreshed every thirty seconds, once at the top of the minute and the bottom of the minute.

For the device to calculate its position, it needs to know the position of each of the satellites, the time it took for the signal to reach the device itself and whether the satellite is healthy. Since the satellite travels at a known velocity, the data provides enough information for the device to perform the calculations.

The data contained in the signal is used by the GPS device to perform calculations not only for position, but also for direction (orientation) and speed. Bear in mind that direction and speed are derived values based on how the device is programmed to perform the calculations. Since device software is proprietary, the exact method and accuracy of the derived calculations can vary by manufacturer and model.

While the most basic GPS units only record waypoints and track points, GPS enabled cellular phones and connected GPS units can contain a great deal more data that may be of evidentiary value.

A connected GPS unit is one that has a cellular radio built into the unit. Some examples of this are the navigation systems currently available in many vehicles that use the On-Star or Microsoft Sync systems.

These units have the ability to make phone calls, receive real time traffic alerts, and search for local shopping deals, find movie times and other functions.

Since many of these units will also allow Bluetooth connections to smart phones, they can contain phone call logs and contact lists. And depending on the phone and unit, they can even receive text messages.

In Vehicle Infotainment and Telematics

Many are familiar with Event Data Recorders (EDR) in vehicles. These devices record engineering data that can be useful when investigating a traffic incident. However, there is other data that can be recovered from vehicles, and this data is becoming more as comprehensive, if not more than the data recoverable from Event Data Recorders.

This data is from the In-Vehicle Infotainment system in the vehicle. This is the actual screen in the center console that a user interfaces with, usually though a touchscreen, to select music, call or text, utilize applications, or navigate.

For hundreds of models of vehicles, digital forensic technology exists that allows the data from the In-Vehicle Infotainment system to be collected and analyzed. The information contained in the system includes data such as navigation history, social media feeds, emails, text messages, Bluetooth connections, whether the vehicle's lights were on and off, if the driver was turning volume or tuning knobs, opening a window, locking or unlocking doors, gear indicators, and more.

This type of information can be critical for a human factors expert to determine if a driver was distracted. For instance, were they selecting music on the touchscreen at the time of an accident, or were they reaching over to turn the tuning knob?

Also, imagine a scenario where a phone critical to a case has been lost or the data has been wiped. There are no cloud backups of the phone, and the phone was never backed up to a computer. There is still one place to look for the data; the car. When a user syncs a cell phone to a vehicle it copies over contact lists, messages, emails, chat apps, and more depending on the vehicle and model of phone.

Internet Connected Surveillance

The ability to integrate smart home surveillance systems that connect to cloud (remote storage) has revolutionized the consumer market for video surveillance systems. For a few hundred dollars, or less, a home surveillance system can be installed by a layperson or homeowner in an afternoon. This video surveillance is usually of high definition quality with multiple recording cameras that can capture activity both at the home, but also on the street, the hours next door, and more.

Further, since these are IoT devices, the video is easier to recover, either from a local computer, cell phone, or a cloud user account associated with the surveillance system. However, as with all forms of video surveillance, new or old, it is critical that the evidence is handled appropriately.

Video and image evidence must be handled with great care, and any examinations or enhancements performed must be thoroughly documented. If the evidence is not received in the most viable format

and preserved correctly, or if the examiner does not perform the forensic examination properly, it is possible to jeopardize the evidence. With surveillance footage becoming more common due to the availability of home systems that are both affordable and require a low amount of technical sophistication to install, the prevalence of such evidence has increased dramatically over the past few years. While surveillance footage is more common, the means by which is it collected, examined, and if necessary, are enhanced, are of paramount importance.

Documentation is paramount when examining video and photo evidence. The Law Enforcement/Emergency Services Video Association explains the necessity of proper and thorough documentation as follows:

> "The best way to ensure the reliability of the video evidence is to have standard operating procedures (SOPs) in place. SOPs assist the forensic video analyst in maintaining proper records of the processes used to examine the evidence and that the processes are performed in a scientifically appropriate and uniformed manner. Records should be complete enough that a similarly experienced and trained individual, working with the same technology, could reproduce similar results."[3]

Just as with computer evidence, an examiner dealing with video and photo enhancement needs to document everything they do in the process of their examination so that another expert can duplicate the results. Without this documentation, it would be extremely difficult and inefficient for another examiner to duplicate the results, if it could be done at all. Improper documentation also calls into question the viability of what the examiner produces in forensic analysis or enhancement, as the improper handling of video and image evidence can create visual information that did not exist in the original video or image, known as artifacts.

Smart Home Technology

The ability to monitor, control, and manipulate your home remotely from a cell phone or computer is transforming how people interact with everyday objects, such as thermostats, alarm systems, and baby monitors.

While this revolution in convenience and usability has been a boon to homeowners, it has also presented significant security and data privacy risks. It is important to understand that much of the security many of these devices have, especially devices that are not coming from larger more sophisticated companies like Apple, Amazon, or Google is subpar to say the best.

The reason for this is because the security is "tacked on" at the end instead of being a part of the entire design and development of the product. Therefore, there are baby monitors that can be hacked easily, thermostats that can be accessed and manipulated via the most rudimentary intrusion methods, and why webcams are still easy to access for a technically capable person.

---

[3] Law Enforcement/Emergency Services Video Association (LEVA), *Guidelines for the Best Practice in the Forensic Analysis of Video Evidence.* http://www.leva.org/pdf/BestPractices forVideoEvidence.pdf

The other issue is simple user data security hygiene. Weak or default passwords on smart devices, poor wireless internet security, and risky internet behavior by users creates a perfect environment for data to be compromised.

While cybersecurity is not the focus of this paper, the evidence that will come from these devices is. Deficient security means that forensic experts have the ability using tools and methods to recover that data from the devices and it can then be utilized as evidence in a case.

Coupled with the fact that Amazon has already provided Law Enforcement with recordings in a home from an Alexa device while it was passively listening[4], and Google recently admitted with the Nest home system that they "forgot" to inform consumers that t contained a microphone[5], the evidence that will be recovered from these devices, or retrieved directly from the providers will likely only increase over time.

Medical Ingestible and Insertable Devices

The advancements in medical technology have coincided with the ability to collect and analyze medical data, and this data is collected closer to the original source, being the patient, more than ever before.

Medical devices that are ingested or inserted into the patient's body are becoming more prevalent and are creating data that is collected via applications on cell phones, computers, and in the in the cloud.

This information can then be shared with the health practitioners, the patient's family, and the patients themselves in real, or near real time. Primary drivers for these devices include patient compliance and risk management.

For example, Proteus Digital Health has designed ingestible pills that are both medication delivery and IoT connected. The stated purpose for this is because 20 to 30% of patient prescriptions are never filled, 50% of medications for chronic diseases are not taking as prescribed, month typically only ½ of a full prescription is consumed by a patient, causing an estimated 125,000 deaths annually and 10% of all hospitalizations. The estimated cost of this non-compliance to US hospitals is in the range of $100-$289 billion annually.[6]

---

[4] https://www.wired.com/2017/02/murder-case-tests-alexas-devotion-privacy/

[5] https://www.usatoday.com/story/tech/talkingtech/2019/02/20/google-nest-secure-microphone/2925026002/

[6] https://www.godaddy.com/garage/the-iot-in-healthcare-forget-wearables-now-there-are-ingestibles/