METROPOLITAN
CORPORATE
COUNSEL®

DECEMBER 2016

WWW.METROCORPCOUNSEL.COM

IoT Data: Objective, Consistent & Pervasive

Using metadata to build compelling narratives for litigation

By Charlie Platt / iDiscovery Solutions

Your phone records who you call and text, what websites you visit, and when you are active or asleep. Your fitness tracker records your heart rate and pace. Your GPS records your location, direction and speed. All of this is IoT data and has three critical characteristics: It's objective, it's consistent, and it's pervasive.

Objective refers to the nature of the data. Data isn't reliant upon a person's ability to recall, understand or accurately relate information. Let's say I send a message to a colleague telling him I'm in London, when I'm actually sitting at home. The content of this message can be true or false and is subject to recollection, understanding and veracity. However, the metadata, or the context, from my phone's geolocation services relates the undeniable fact that I was home at the time, no matter what was recalled or said to the contrary.

Consistent refers to the nature of how the devices record and communicate. They are designed to take a sensor reading on a schedule and record and report the result. This process is automated, meaning that the schedule is consistent and results in large amounts of data being captured. Inconsistent data leads to anecdotal reporting, while consistent data over time develops a pattern and is much more compelling.

Pervasive refers to how these devices, and their sensors, are proliferating at an alarming rate. In 2015, there were an estimated 50 billion IoT sensors in the world, but that number is expected to jump to over 1 trillion by 2020. This pervasiveness means that IoT data is likely going to be used in the future in cases you are working on if it isn't already. How many people do you know who don't have some sort of smartphone, fitness tracker, smart thermostat or other IoT device – or multiple IoT devices?

How does IoT data specifically apply itself within the litigation landscape? The three aspects – objective, consistent and pervasive – all apply and the following cases studies illustrate how they and their data can make a difference.

> *There will be an estimated 1 trillion IoT sensors in the world by 2020*

Case Study: Data Rich vs. Data Poor

Our first example is a wage and labor class action and has to do with the pervasive and consistent nature of IoT devices. A group of employees brought a class action suit alleging off-the-clock uncompensated work. In this case, employees claimed that they had to work through lunch and were not being properly compensated for their time.

As in most class action lawsuits, one party was data rich and the other party was data poor. This leads to asymmetrical discovery, where the data rich party shoulders additional risk, burden and cost related to discovery aspects of the case, while the other party shoulders little due to their apparent lack of relevant data. In this scenario, the data rich party carries the risk of spoliation, as well as the additional cost and burden involved in preservation, review and production of data.

In this case, with our assistance, counsel successfully argued that the employees' cell phones contained metadata that was relevant to the litigation. The cellphones contained metadata for emails, calls and text messages that showed the employees were engaged in non-work related activities while on the clock. Not only did this bring relevant and important data to light, but in successfully arguing this point, the responsibility for discovery became a shared burden between both parties. All parties now had a vested interest in conducting discovery smoothly and working towards a mutually beneficial solution.

Case Study: SEC Insider Trading Investigation

Our second example is an SEC investigation into insider trading, and primarily revolves around the pervasive and objective nature of IoT data. We assisted the SEC with attributing a specific individual with accessing information via a computer terminal. One of the trickiest problems with forensic analysis is attribution, or more simply put, can we identify whose hands were at the keyboard? We can show that a specific terminal was used to access the information (that's a traditional focus of digital forensics), but can we say who was actually using that terminal?

To make this argument, we brought together multiple disparate data sources, including IoT devices, social media, forensics and online trading data. Digital forensics evidence was used to first associate a terminal in the suspect's cubicle with unauthorized access to prerelease corporate earnings information. Since the terminal was in an unsecured cubicle, the suspect could easily argue that anyone who had access to the office building had access to the terminal and plausibly deny his involvement. We needed to put the suspect in the seat with his fingers on the keyboard.

This analysis began by pulling in data from several nontraditional sources. The first step was to analyze the building's access swipe-card records, which indicated that, for the most part, the suspect entered the building shortly prior to the times that the sensitive information was accessed, but due to the nature of

Charlie Platt *is a Sr. Managing Consultant with iDiscovery Solutions. Mr. Platt has over 25 years of experience consulting with corporations and clients on analytics, digital forensics, cyber-security and incident response, and e-discovery. He can be reached at cplatt@idiscoverysolutions.com.*

building access, and some of the inherent faults such as piggybacking, this analysis was less than conclusive. In short, there were instances where no building access existed prior to a given data access event. While this was informative, it was not in itself irrefutable.[1]

To add more weight to the argument that the suspect was at the keyboard, we pulled online trading data for the suspect's accounts. Aligning trade data with the known access events revealed a high correlation between trades and unauthorized access to the earnings data. While this increased the likelihood that the suspect was indeed the individual behind the keyboard, it still wasn't conclusive.

Finally, digital forensics evidence collected from the terminal determined that, at the same time prerelease earnings data was being accessed, the terminal was also accessing the suspect's private Facebook account. All of these separate pieces aligned to make a compelling argument. This is a critical aspect to consider when using IoT data – one singular data point is less likely to be compelling in and of itself, but when multiple different data sources and points are brought together, a rich, factual story can be told that can be extremely difficult to refute.

Case Study: Flexibility Analysis

Our third and final example is another wage and labor case relating to alleged uncompensated prework, covering all three aspects of IoT data we mentioned – objective, consistent and pervasive. Plaintiffs made several claims, but primarily the case was about activities the employees were, or perhaps were not, undertaking for their employer prior to clocking in for the day.

Metadata pulled from devices and corporate data systems provided a detailed profile of how each individual interacted with the systems, and what his or her specific morning looked like. This included when they first logged in, how long the process took to complete, when they interacted with each system, and when they left their home in the morning. Using data to determine when individuals were interacting with systems, and when there were large unexplained gaps in interaction, created detailed profiles for each class member based on actual data.

The difference between actual data and estimating is important. This analysis was based on specifically assessing class members on an individual and daily level to determine their specific behaviors. Having the ability to delve this deep into personal routines showed just how dissimilar the individuals actually were. Some individuals logged in very early, while others did this closer to their clock-in times. Once logged in, some then did nothing for hours, while others interacted with the systems immediately. Each additional IT System or IoT device that class members interacted with served to increase the variability and individuality of the individuals' morning routine. These permutations proved class members were unique and dissimilar and provided the basis for the primary point: Since each individual goes about their morning routine differently, they could not be assessed *en masse*, leading to the argument that they didn't constitute a class.

Secondly, the data clearly showed that the class members were exercising flexibility in their schedules. With the varied routines, not only were individual members shown to be different from each other, but that they also exhibited varied patterns within their own individual profiles, e.g. Mondays were different from Wednesdays, Wednesdays were different from Fridays, Fridays in the summer were different from Fridays in the winter, etc. This provided critical support to counsel's argument that the class members had, and exercised, extensive flexibility in their prework activities, and that these duties could be completed with a minimal amount of time and effort, and in many cases without direct supervision.

Conclusion: Just the Facts, Ma'am.

Knowing the facts of the story is critical. The IoT is all about consistent, objective and pervasive metadata, which, when properly analyzed, tells a rich, fact-based story. IoT devices are multiplying quickly, and if we understand the data available and how we can put it to work for us, we can uncover factual data related to our cases that previously either didn't exist or was prohibitively expensive to access. Think of the IoT as the opposite of virtual reality. Virtual reality creates an imaginary world which we can put ourselves into; conversely, the IoT records real world events in a virtual environment, allowing us, with the right skills and tools, to rewind and replay reality. This data, when expertly interpreted, replays human activity with devastating effectiveness. Using these facts, an informed litigator can build a compelling narrative. Get the data; tell the story; win the case.

To review the footnotes to this article, visit http://www.metrocorpcounsel.com