Collecting Your Company's Digital Breadcrumbs

Analytics can uncover correlations, anomalies and more

On October 3, Metropolitan Corporate Counsel hosted Understanding the Value & Risk of Digital Breadcrumbs, an online event featuring ***Hunter McMahon*** *of* ***iDiscovery Solutions****, Bobby Malhotta of Munger Tolles & Olson and Jennifer L. Eglander of Ogletree Deakins. This presentation offered insights as to how companies can leverage event-based analytics and interactive visualizations to see relationships and pinpoint possible inconsistencies in a way that content-based analysis cannot. Our editors sat down with Mr. McMahon to explore some of the important topics discussed during this presentation. His remarks have been edited for length and style.*

Coming off of that event, can we start with a quick definition of the Internet of Things?

Hunter McMahon: Think of IoT like a giant spider web, connecting different branches, trees, bushes, etc. IoT is essentially the interconnected world (web) of devices (branches) that has enabled the collection and transfer of information without the need for user interaction. A quick example would be the sharing of all your data from your smart phone, fitness tracker, fitness equipment, music platform, etc. between one another to let you know how active (or inactive) you've been, what music motivates you and if you are on track to reach your fitness goals. This web of connectivity has led to data now being able to know us better than we know ourselves.

The benefit of additional data sources is not simple addition, but rather exponential value.

I'd like to focus on this issue as it relates to employer/employee relationships. With so many more devices and more access to Wi-Fi, all of this interconnectivity, comes easier access to data. How do employers need to approach dealing with all of these additional points of access and new data repositories that their employees now have?

McMahon: Companies need to think of this from a few different vantage points. First, there is a benefit of employee connectivity and convenience of access, but there is also the tradeoff of "always being on." It's easy to see the risks, but remember there may be an overriding business benefit. While "easy access from anywhere" can increase productivity, there is the issue of securing the company's sensitive information with proper safeguards to prevent the misappropriation of that information. Lastly, companies need to understand what data they now have because of all the new devices and the access (e.g., location history, activity history, etc.), and the liability associated with the retention of this data. For example, do you have access to or are you keeping personal information when you don't need to?

Along those lines, we also spoke about privacy and protecting company information. What should companies be concerned about and how should they instruct their employees on these situations?

McMahon: For better or worse, users rarely read the terms and conditions when signing up for the "cool new app or service." That makes security a perpetual challenge. As it relates to privacy, it starts with understanding the data and managing expectations. Security and privacy are tightly intertwined – both benefit tremendously from the education of the employer and the employee. As cliché as it sounds, if the company helps the employees understand the "dos and don'ts" for their own personal protection and benefit, they will also reap the benefits by having better trained employees. Educate!

During our event, we discussed a couple of litigation scenarios where event data was key to establishing the facts. Can you give an example of how event data has helped in the past?

McMahon: We've had much success with analyzing event type data to help counsel uncover the real story. As we discussed in the webinar, event data is more readily available now with the advent of IoT. A great example is how we've been able to assess billions of location and time records to understand when and where employees were during their claims of overtime. A single piece of information was not conclusive, but as additional information was layered together the narrative became very clear – that employees were not working nearly as much as they said they were (who wants to go to the park for a jog while on shift?).

One of the important things to understand here is that the benefit of additional data sources is not simple addition, but rather exponential value. Just like your fitness apps, the more data input you give it, the better insight it can give you about achieving your goals. A similar concept exists for fitness goals – the more data you analyze, the better insight a client may get on how to achieve its goal of winning the case.

We also specifically discussed leveraging event data for an investigation of a possible bad actor. What are some key considerations for employers?

McMahon: These type of investigations have truly transformed in recent years and results can be very insightful. The amount of data (digital breadcrumbs) every employee leaves behind continues to grow with the adoption of new devices and technology (e.g., IoT). These breadcrumbs help us uncover the story of what really happened. When approaching these investigations, ask yourself these three questions:

- What potential data sources are available and how are they connected?
- What events could prove (or disprove) a claim?
- How can you layer those events together to tell a story?

For example, as we discussed on the webinar, an employee claims he wasn't somewhere (at a conference) but rather home in a different city. If he drove, maybe his car's GPS is a source of potentially relevant data. Maybe the maps app on his mobile device or perhaps GPS location from his fitness tracker are sources. There's also the information from his Nest home thermostat (indicating he wasn't home) and payment transactions (credit cards, Apple Pay, etc.).

Last, can we talk about the preservation of data in a world with IoT? How are you advising clients on this important issue?

McMahon: This is an ever evolving landscape and requires timely and decisive action due to how fast this data changes and how quickly it may become unavailable. Assume nothing, and call somebody who has deep knowledge and expertise in this arena to avoid any unnecessary fumbles.

"[From a data analysis standpoint, you can't visually look at five million GPS records or 30,000 badge swipes], so the key is understanding that it doesn't have to be a manual process. It depends on your underlying data sources, but there are software tools that can help translate and interpret data from various file formats. There are sophisticated consultants that can help aggregate data from those different file formats and develop the relationships, so you can understand and uncover patterns that support your legal arguments. It really depends on the issue at hand, what kind of data you have and what your budget is, to some extent. But there are mechanisms to do it. It's not a one-size-fits-all approach."

– Bobby Malhotra, Munger, Tolles & Olson

"If you have access to and are collecting information on your employees, first you want to ensure that you're complying with the relevant state privacy laws, which vary from state to state. You want to think hard about tracking and monitoring off-duty work. I think employees generally have an understanding that if they're on company devices (computers, phones, cars, etc.) they have a limited privacy interest in what they're doing. But off-duty work, even if it's on an employer device, could be a different story. Next, notify your employees about what is happening. Inform them of the monitoring activity. Let them know – in a device policy or a company car agreement, for example – that they're subject to monitoring by their employer. If you let them know, then you reduce any issues later on down the road."

– Jennifer L. Englander, Ogletree Deakins

Hunter McMahon *is the Director of Data Analytics for iDS, bringing over a decade of experience in technology and the legal field. He focuses on providing innovative solutions to overcome the unique challenges, and maximize potential advantages, from a variety of data systems. He is a member of The Sedona Conference WG1, WG6 and WG11. He has served as a testifying and consulting expert to corporations both large and small, while working with Am Law 100 and boutique law firms. He can be reached at hmcmahon@idiscoverysolutions.com.*