FEBRUARY 26, 2018

Legaltech® news ONLINE

An ALM Publication

# Thanks to the IoT, This Isn't 2006's E-Discovery

FTI's Jake Frazier and Relativity's David Horrigan break down why internet of things discovery is different, preservation issues and more ahead of a Legalweek panel.

*BY ZACH WARREN*

It's been about a decade and a half since the original Sedona Principles and Judge Shira Scheindlin's decision in *Zubulake v. UBS Warburg*. It's been a little less than that since the 2006 amendments to the Federal Rules of Civil Procedure. Attorneys have this e-discovery thing down by this point, right?

Not so fast. As the world changes and technology along with it, so too does the practice of e-discovery. These days, the issue isn't limited to how to collect emails. Now, e-discovery practitioners must grapple with social media, internet chat, text messages, and other data that those in 2003 couldn't have even dreamed of.

And the next wave of this data is already here: the internet of things (IoT). Sure, you know how to collect Facebook posts, but what about, say, driving data from internet-connected cars? Or what somebody says to Apple's Siri assistant? In the connected universe, there exists a whole host of issues concerning the collection, preservation and production of this massive amount of data.

A session on Jan. 31 at the Legaltech conference during Legalweek New York 2018, titled "From the Iron Rooster to Amazon Alexa: Mobile Discovery and the Internet of Things," will explore the legal, technical and practical considerations of mobile,

social and IoT data. The panel includes a former Department of Justice cybercrime coordinator (Ed McAndrew), a prominent discovery attorney (Kelly Twigger), a corporate information governance expert (Jake Frazier), and a leading legal industry analyst (Ari Kaplan), with Relativity's David Horrigan moderating.

Ahead of the panel, LTN spoke with Frazier and Horrigan to get their takes about what makes IoT discovery so different, what the new paradigm means for planning and preservation, and more.

**LTN: What exactly makes IoT device discovery different from everyday e-discovery?**

**Frazier:** IoT device discovery can contain information that Americans would consider to be extremely private and/or sensitive. This can include an individual's TV viewing habits, their internet searching habits, where they've physically been via geotracking, as well as data that may be picked up by Siri, Alexa or other "always listening" home devices. The more we integrate technology into our everyday lives and personalize it to make our lives easier, the more this technology can reveal about us.

**Horrigan:** Both the types of data and the location of the data make IoT data different. Although e-discovery is still bewildering to many lawyers and legal teams, in 2018, most practitioners specializing in e-discovery have sophisticated workflows to handle discovery of email. IoT presents new challenges. As it often does, technology has changed the rules of the ball game—figuratively, and sometimes literally. For instance, Fed. R. Evid. 902 was amended last month with new provisions for authentication of electronic data. In addition, although electronic discovery has traditionally been considered the domain of complex commercial litigation, as we'll see from the cases we're discussing at Legaltech, IoT is helping make e-discovery an important part of criminal practice as well.

**LTN: There are some cases involving some devices that most attorneys would understand have data (Fitbit, Alexa), but some others (like trucks) some wouldn't even think to check. How does the IoT change the way attorneys prepare for the discovery process by identifying data sources?**

**Frazier:** Lawyers may have a false sense of security when they use old forms that only ask about "desktops, phones, file shares and email." Legal teams should consider evaluating their e-discovery questionnaires to make sure they are incorporating potential IoT data early in the process. Relying on questionnaires from the "good old days" may leave them blindsided.

**Horrigan:** That's a great point, because IoT comes in all shapes and sizes. With the extensive publicity surrounding Amazon Echo's Alexa in *State v. Bates* and to a lesser extent, the Fitbit data in *State v. Dabate*, many lawyers and clients are on notice that IoT data are potentially discoverable in court. But a 2005 GMC pick-up truck? It's why *Below v. Yokohama Tire* is such an interesting case. In litigation over a tire blow-out, just about any practitioner would know you need to preserve the tire and mechanical equipment, but ESI from a vintage truck might not be on counsel's radar. Legal teams may want to cast a wider net, but you've also got the proportionality provisions in FRCP Rule 26(b)(1) from the 2015 amendments. You can't simply request everything and the kitchen sink; you've got to be strategic about it.

**The preservation question is an interesting one to me. With so many sources**

**of data with the IoT, does counsel need to adjust their preservation requirements at all to hold it all, or can it be included neatly in pre-existing policies?**

**Frazier:** It may depend on how advanced the corporate client is in their information governance. As part of an information governance program, corporations can evaluate IoT data and develop policies to ensure that they are not logging a bunch of extraneous data they don't have a need for, and work with IT to ensure that those logs aren't turned on.

**Horrigan:** No matter how neatly they're included in pre-existing policies, boilerplate discovery requests—and responses—aren't going to cut it. As Craig Ball noted recently, when private counsel for President Donald Trump sent a cease and desist letter to the publishers of the recent book, "Fire and Fury: Inside the Trump White House," for their preservation provisions, they apparently borrowed heavily from an exemplar Craig had created years ago. In an ironic twist, because the preservation exemplar was created over a decade ago, the demand from a famously tweeting president didn't include preservation provisions for Twitter. Second, as U.S. Magistrate Judge Andrew Peck [of the Southern District of New York] noted last year in *Fischer v. Forrest*, boilerplate responses to discovery responses won't get you very far either. In fact, they're prohibited specifically by the 2015 amendments to FRCP Rule 34.

**What's one key takeaway that you want attendees to take from the panel?**

**Frazier:** Start discussing your IoT policy now. These devices aren't perfect. There are some well-documented cases where first-generation IoT devices all had the same username and password, or that the manufacturer published the password online for all to see and access. And, some of these IoT devices allow for remote access for technical support, which could potentially lead to discovery issues. Having your IoT policy in place can act as a forcing function for the company to examine how these devices work, to educate employees on the risks, and to develop an information governance strategy that incorporates IoT data.

**Horrigan:** Perhaps the biggest takeaway is that IoT, mobile and social data can affect your case even when you least expect it. In formulating our panel for Legaltech at Legalweek, we've tried to cover all the bases. Jake Frazer of FTI Consulting Inc. brings corporate expertise, while Ed McAndrew of Ballard Spahr LLP will give both a complex commercial litigation perspective and cover criminal law considerations from his years with the U.S. Department of Justice. Ari Kaplan of Ari Kaplan Advisors will give us some insight gained from his surveys and studies, and Kelly Twigger of ESI Attorneys will provide perspectives from practitioners of all sizes. I like to think we've covered all the bases—or as many as we can in the 2018 world of the internet of things and mobile and social data.