CHALLENGES IN PRESERVING AND USING IOT DATA

By H. Michael O'Brien and Daniel M. Braude - March 20, 2018

First published in Pretrial Practice & Discovery – A Section of ABA Litigation

The concept of the Internet of Things (IoT) has existed for nearly 20 years. Technology pioneer Kevin Ashton is widely credited with coining the term in 1999 to describe the connection of objects to the internet. Since that time the IoT, and the ability to control products, machines and systems over the internet, has become a reality. Last year, Gartner, Inc. estimated that there were more than 8 billion connected devices, a number that will exceed 20 billion by 2020. There is little doubt that the IoT is having a profound impact on how we live our lives - an impact that, for better or for worse, will seep into how attorneys conduct litigation.

Two primary new obligations for counsel arise out of the IoT. First, IoT devices create electronically stored information (ESI) that may require preservation. Merely determining what IoT data is available, where it is located and whether it even can be preserved creates challenges not encountered by past generations of litigators. See Model Rules of Prof'l Conduct 1.1, cmt. 1, 8. (Am. Bar Ass'n 1980). Second, litigation involving IoT devices requires retention of testifying experts capable of analyzing IoT data and, in some instances, opining on potential root cause failures.

IoT Devices in Litigation

At the forefront of IoT growth is the connected or "smart home," which embraces all types of previously "dumb" household products, systems and appliances that now can be connected to the internet and controlled from a smartphone. "Cook delicious meals at home, from the office, or on the go" is how one manufacturer promotes a device's Wi-Fi capabilities. In addition to kitchen appliances, devices that connect to the internet include security systems, garage doors, HVAC systems; washers and dryers, light switches, outlets; all forms of consumer electronics, including wearables; heavy machinery; medical devices; and too many more products to name. One thing these devices have in common is the ability to create data. Autonomous vehicles, which are essentially IoT devices on four wheels, are predicted to create four terabytes of data for every eight hours of use.

So what happens when an IoT device becomes the focus of litigation? In years past, litigation arising out of a kitchen appliance might have involved a simple allegation that a faulty switch triggered a fire. To reach that conclusion, cause-and-origin experts and forensics engineers would locate the fire's area of origin, identify potential sources of fire within that area and attempt to include or exclude each potential source. To successfully prove the source and cause of a fire, the experts would need to rule out other potential sources and causes.

The process remains fundamentally the same in today's world of IoT devices. What's different is the type of data that may need to be collected and analyzed.

Electronic Discovery Preservation Obligations

In all litigation there is a duty to preserve relevant evidence, including ESI, once litigation or an investigation can be reasonably anticipated. *Zubulake v. UBS Warburg LLC ("Zubulake V")*, 229 F.R.D. 422, 433 (S.D.N.Y. 2004). This duty falls not only on litigants directly but also on counsel to actively supervise the process. A party's failure to adequately preserve evidence in its "possession, custody or control" can result in spoliation sanctions.

Steps to defensibly preserve ESI may include:

- Distributing a legal hold to document custodians (i.e., employees that may possess relevant materials) with instructions to avoid the deletion of relevant materials
- Conducting interviews of document custodians and IT personnel to identify the location of potentially relevant materials
- Taking steps to suspend routine deletion
- Amending the legal hold as needed
- Collecting the data in a forensically sound manner, often with assistance of a data forensics expert.

Of course, the nature of the matter at issue and the volume and location of data will dictate the burden and expense of preservation efforts. But even when daunting in scope, preservation is often straightforward despite the frequent need to collect data from nontraditional locations, such as mobile devices and the cloud. The same may not apply to litigation involving IoT devices.

The initial challenge once potential IoT devices have been identified is determining whether data exists that one can preserve and collect. A host of questions may need to be answered for each IoT device:

- When was the device last accessed?
- Could the device be controlled through a smartphone app?
- Does data exist on a smartphone app such that imaging of the phone is warranted?
- What type of data may have been created?
- Does that data still exist or was it ephemeral?
- Is data stored either locally on the device or on a remote server?
- If data resides on the device, what challenges are associated with extracting the data?
- If data is on a remote server, is it maintained by the manufacturer or by a third party that manages a manufacturer-branded app?
- Is the party holding the data amenable to releasing it (even if served with a subpoena)?
- Does the nature of the incident suggest the possibility of a cybersecurity incident?
- Is the data in a proprietary format that might have limited value even if obtained?

In the world of IoT devices, the traditional approach of using data mapping to identify locations of potentially relevant ESI – specifically, conducting interviews with document custodians and IT personnel – will likely only be the first step. The services of a data forensics expert, retained initially as a consultant, may be needed as well. In fact, until the majority of the questions listed above have been answered, adequately preserving relevant IoT data may be impossible.

In addition, answering many of these questions may be necessary to determine the type of expert or experts that ultimately will be required to analyze the IoT data and offer opinion testimony. In other words, it may be necessary to retain an expert, at least a consulting expert, merely to determine what other experts are needed.

Traditional Experts May Not Qualify to Opine on IoT Devices

Experts with background, education or experience sufficient to address potential root cause failures with a "dumb" version of a product may not have the requisite expertise to address the root cause failure with a "smart" version of the product. In *American Strategic Insurance Corp. v. Scope Services, Inc.*, the plaintiff's expert witness was precluded from offering testimony on the standard of care for the installation of a "smart meter" that was the focus of the plaintiff's subrogation action for property damage. The complaint alleged that the defendant's employee was professionally negligent with the installation, which caused a fire due to high-resistance contact between the new smart meter and the meter base. *Am. Strategic Ins. Corp. v. Scope Servs.*, Civil Action No. PX-15-2045, 2017 U.S. Dist. LEXIS 149789, at *3 (D. Md. Sep. 15, 2017).

The plaintiff's expert conceded at his deposition that he could not identify the factual basis for his proposed six-step smart meter installation procedure being an accepted industry standard. This opened the door for the defendant to challenge the qualifications of the plaintiff's expert under Federal Rule of Evidence 702. Because the expert did not have specific experience installing electric "smart" meters and lacked knowledge of the industry standard of care, the court held that he failed to qualify as an expert regarding his proposed six-step standard of care. The court ultimately held that the expert's testimony "at best [amounted] to his personal views on what the industry standard of care *should be*." *Id.* (emphasis in original).

Identifying the Correct IoT Expert

The obvious solution to the dilemma of the plaintiff's counsel in *American Strategic Insurance Corp.* would have been to retain one or more additional experts who had sufficient experience with "smart" products. For starters, the correct IoT expert may need to rely on standards and guidelines that are currently being developed and evolving at varying speeds across the spectrum of various government and industry sectors:

- Some – such as UL 2900 Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements, UL 2900-1– are focused on developing a conceptual framework to be used with existing UL standards for specific products.
- Other standards are emerging through government agencies, such as the National Institute of Standards and Technology: Framework for Improving Critical Infrastructure Cybersecurity and the Department of Homeland Security: Strategic Principles for Securing the Internet of Things.
- Still others are coming from collaboration among diverse industry technology stakeholders, such as the Online Trust Alliance IoT Trust Framework.

As these standards become more widely accepted, experts will need to become familiar with them and be able to address questions of their relevancy and applicability to their expert opinions and determine whether compliance or noncompliance with any given standard is foundational to their opinions. In addition, for any matter involving an IoT device, the type of device at issue and the nature of the data available for analysis will dictate the type of expert needed. This may include expertise as to particular types of IoT devices *and* specific IoT platforms, including Samsung SmartThings, Google Thread, Apple HomeKit and Amazon Echo. This may even require an assortment of data forensics investigators and data security experts.

Final Thoughts

The traditional approach of retaining a single expert to opine on the failure of a "dumb" product is, naturally, going the way of "dumb" products. Today, lawyers must address litigation involving IoT devices in a manner that takes into account the complexities of the device and its data. This starts with evidence preservation. The inability to prove or defend a case could result from a failure to appropriately preserve relevant IoT data. Even where the data is available, it will be difficult to "rule out" an IoT device as a potential cause of an incident without experts who possess the requisite skill to address the complexity of "smart" products.

— **H. Michael O'Brien** and **Daniel M. Braude** are partners with Wilson Elser in New York, New York.

H. Michael O'Brien
White Plains | New York
914.872.7234
michael.obrien@wilsonelser.com

Daniel M. Braude
White Plains | New York
914.872.7210
daniel.braude@wilsonelser.com