APRIL 21, 2016

Legaltech© news

ONLINE

An ALM Publication

The 'Discovery of Things': How the IoT Affects FRCP, Data Access

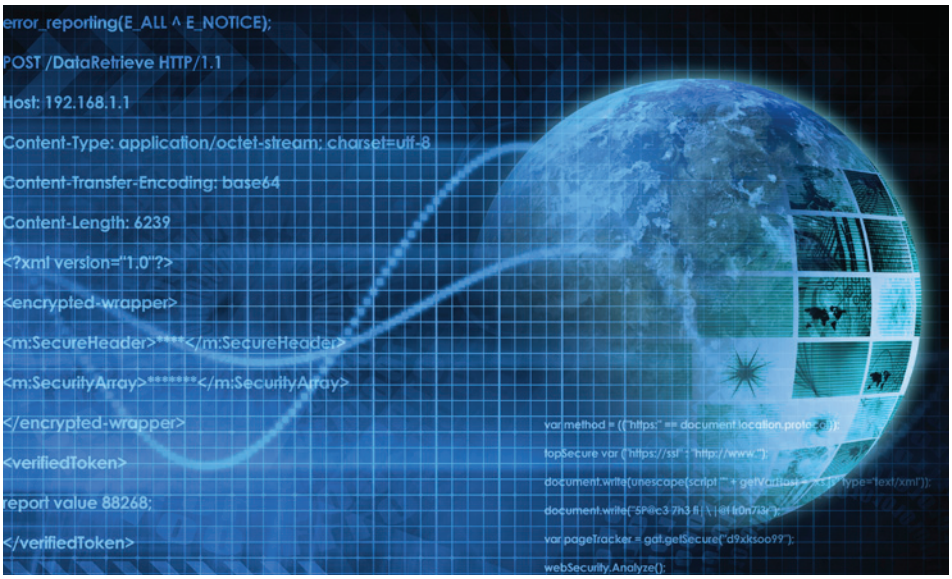
While the discovery is tasked with becoming more proportional, the ever growing mounds of novel and legally questionable data are creating pressing challenges.

BY RICCI DIPSHAN

The slide into a data-centric world did not happen overnight — nor did it happen gradually. Indeed, the legal industry is just one of many struggling to catch up with the complexities and responsibilities of a world built in bytes. And while legal tech has aided in this transition, it is far from the only force aiming to smooth's the legal industry's landing in the 21st century.

In December 2015, for example, new amendments to the Federal Rules of Civil Procedure sought to standardize and clearly define requirements concerning proportionality in the discovery processes, rule 26, and the preservation of electronically store information (ESI), rule 37(e).

In the discovery processes, rule 26 set the guidelines for requesting evidence, noting that discovery demands must be relative to the needs of the case, and be evaluated by six factors, including "the parties' relative access to relevant information, the parties' resources," and "and whether the burden or expense of the proposed discovery outweighs its likely benefit."



The rule sounds simple enough when one considers data on a company's servers and networks, or stored on employee computers. The problem is, however, that such reality no long exists — the rules themselves may not caught up with the mobility of data in today's ever-pervasive Internet of Things (IoT).

Linda Sharp, associate general counsel of ZL Technologies, noted the situation has continued to evolve.

"A few years ago, we saw BYOD enter the corporate environment and are now looking at the IoT, and the data volumes continue to grow at an exponential rate," Sharp said. "From a legal perspective, the laws really haven't caught up with the way organizations truly manage data today. There is a tremendous disconnect between how businesses need to utilize data to be more efficient and productive and the logistics surrounding potential production of this compilation."

Beyond mobile phones, the world now encompasses smart

devices such as FitBits and connected refrigerators and cars that are not only expanding the reach of the internet, but creating mounds more data — often inconspicuously. Which begs the questions: how much IoT data is out there? How much of it may be relevant? And how easy is it to access?

"Most organizations are *trying* to be proportional today. The fact that more and more data is available to us and potentially relevant to a case makes us confront the very definition of 'proportional' in a way that we previously didn't have to," said Adi Elliott, vice president of market planning at Epiq Systems. "And even outside of the law, human nature often pits 'being right' against 'proportionality' in ways that can even complicate the relationship between two people—let alone the relationship between multibillion-dollar corporations."

Sharp added, "As we look at these new unique data points, I see the need for this data to be produced. New technologies are yielding more data points, and as we collect and manage this data, we need to ensure that we are taking into consideration that it may be subject to legal hold and production. I don't see a court accepting an argument for burden when the process for production should have been contemplated as the means for collecting these data points were created."

While the complexities that arise when applying the FRCP rules to the IoT, some downplay the amendments' impact on discovery as whole, noting that as long data is relevant, no matter what its source, it's ground for discovery.

"I think that as we become more and more mobile and our devices, appliances and vehicles, among other things, create data that may be directly relevant to matters in dispute, the production and disclosure of that information won't necessarily be impacted by the amendments; as long as the data sought is directly related to the claims and not part of an overly broad discovery strategy," said Mark Yacano global practice leader, managed legal services at Major, Lindsey & Africa.

Indeed, shortly after the amendments took effect, the court in *Gilead Sciences v. Merck* addressed the proportionally rule:

> "What will change—hopefully—is mindset. No longer is it good enough to hope that the information sought might lead to the discovery of admissible evidence. In fact, the old language to that effect is gone. Instead, a party seeking discovery of relevant, non-privileged information must show, before anything else, that the discovery sought is proportional to the needs of the case."

But that may be difficult, given the novel and sometimes inaccessible nature of IoT data.

"The challenge is, how difficult it is to maintain standard processes across all these data sources as they grow and evolve? Sources that are completely under the control of a corporation remain relatively easy to access," explained Elliott.

"Cloud sources that the corporation pays for directly and has indirect control over are usually on the easier side, too. But even these two groupings can be difficult to keep up with, as there are a lot of them, and the standards change quickly. So it's always a reactive game of whack-a-mole as the software & hardware companies make changes to their technology that the e-discovery industry has to react to," Elliott said.

"As soon as you get into third party data sources that a corporation has no control over, things get more complicated. On top of the technological complexity, you also have jurisdictional complexity, as the global nature of e-discovery often results in different levels of access depending on the international jurisdiction. And it's only growing in complexity. We're still early on in all of this," he said.

"The reality is, we have to come up with better ways to manage and control our data," Sharp added.

But she also noted that beyond management of data there is still another thorny legal issue concerning IoT: "The next legal question is, 'What information can a business collect without the permission of its employees or customers?'

"As a consumers, we either need to identify better ways to protect our information or alternatively recognize that as the IoT evolves, we are going to be giving up certain privacy rights," Sharp said. "Whether it's your cell phone that beeps when you enter into a particular store and tells you about a new ad or a new product they've launched, or provides with you a coupon to get a discount, it's tracking who you are, where you are, and your shopping patterns."