PRETRIAL PRACTICE & DISCOVERY

ABA Section of Litigation

Spring 2018, Vol. 26 No. 2

The "Internet of Things": New Challenges in Civil Discovery

By Kristen B. Weil and Ronald J. Hedges – March 20, 2018

A dizzying array of new products was unveiled at the 2018 CES (formerly, the International Consumer Electronics Show), one of the biggest conferences of its kind produced by the Consumer Technology Association. A kitchen and bath company showcased a toilet that integrates voice control technology to lift or close the seat, flush, or switch on a particular bidet spray setting. The same company also announced a cloud-based, voice-enabled bathroom mirror. A smart fabric company called Xenoma displayed a set of "smart pajamas" designed for dementia patients; sensors are imbedded into the fabric to capture the wearer's motion and vital signs. A cosmetics company introduced a tiny wearable sensor that attaches to one's fingernail and tracks UV exposure; the data is picked up by a smartphone.

What all these products have in common is the Internet of Things (IoT), which refers to connecting and networking physical devices, vehicles, and other items embedded with software, sensors, and electronics connected to the internet to create, collect, and transmit data. More than just enabling new gadgets, the rise of the IoT has implications for attorneys engaged in civil litigation: They must grapple with new forms of electronically stored information (ESI) as part of the discovery process, and they must understand how existing discovery rules apply to the IoT just as they do to more traditional forms of data.

Discovery and the IoT

Under Federal Rule of Civil Procedure 26(b)(1), parties "may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case." This broad scope of discovery applies to data generated by IoT devices.

For example, fitness trackers and other wearable devices may provide useful ESI in personal injury actions to demonstrate a party's level of physical activity before and after an injury. The ESI from these same devices may be relevant in employment discrimination actions in which accommodations for a disability are at issue. The IoT may also provide useful data about a party's whereabouts at a relevant date or time. Such data could come from GPS devices, cell phones, geolocation tagging on photos, or even smart home thermostats that reveal dates and times when a home is unoccupied. This ESI could be powerful leverage in civil litigation for settlement, or disposition of the action.

PRETRIAL PRACTICE & DISCOVERY

Section of Litigation

Spring 2018, Vol. 26 No. 2

However, not all attorneys are familiar with the IoT in general or the specific types of ESI that may be relevant to a particular action. If attorneys are unaware of the types of devices used by the parties and what kind of ESI these devices generate, store, or transmit, then they may not actively consider data generated by the IoT when crafting litigation strategy and drafting discovery requests and thus may not discover important information.

Control and the IoT

Federal Rule of Civil Procedure 34(a)(1) allows a party to request ESI in the responding party's possession, custody, or control. A responding party generally has the burden of proving that it does not have actual possession or the right to obtain the electronic information requested.

As electronic data proliferates, the issues regarding who has possession, custody, or control over data become more nuanced and complicated; and the costs and burdens associated with discovery of IoT information increase. The IoT poses challenges for litigators who must determine whether the requested data is within a party's control or is controlled by a third party. For some data, this inquiry is straightforward. But many devices transmit data rather than store it on the device itself. Is data transmitted to the cloud, or to third-party servers, subject to a party's possession, custody, or control?

Federal courts differ in how they apply Rule 34(a)(1) to determine whether a party will be deemed to have "control" over the data. Some impose an obligation to produce information when a party has the legal right to obtain that information. *See, e.g.*, *In re Bankers Trust Co.*,61 F.3d 465, 469 (6th Cir. 1995) (a party has possession, custody, or control only when the party has the legal right to obtain the documents upon demand). Other jurisdictions impose an obligation when a party has the practical ability to obtain the information. *See, e.g.*, *Tomlinson v. El Paso Corp*., 245 F.R.D. 474, 476 (D. Colo. 2007) ("'Control' comprehends not only possession, but also the right, authority, or ability to obtain the documents."); *Handi-Craft v. Action Trading, S.A.*, No. 4:02 CV 1731 LMB, 2003 WL 26098543, at *6 (E.D. Mo. Nov. 25, 2003) ("Thus, the appropriate test is not of legal entitlement, but of control or practical ability to obtain the documents."). Some jurisdictions may apply multiple standards. The answer thus depends on the jurisdiction in which an action is pending. In addition to the differing approaches adopted by the federal circuits, attorneys should be aware that state courts may have differing views on when a party "controls" data.

PRETRIAL PRACTICE & DISCOVERY
Section of Litigation
Spring 2018, Vol. 26 No. 2

In some cases, an attorney will need to serve a subpoena on a third party who controls or hosts the data, rather than seeking information directly from the opposing party. Attorneys should review the privacy policy applicable to each device because manufacturers may clearly state that they will disclose a user's information if necessary to comply with a subpoena or warrant.

Production and the IoT

But even if ESI is under a party's control, must the party produce it? Under Rule 26(b)(1), the scope of discovery must be proportional to the needs of the case. In considering whether discovery is proportional, courts may consider "the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit."

Moreover, a party may be able to credibly argue that under Federal Rule of Civil Procedure 26(b)(2)(B), it need not provide discovery of certain electronic data because the data is not reasonably accessible. When considering whether information is reasonably accessible, courts should consider the technological feasibility and realistic costs of preserving, retrieving, reviewing, and producing the information in question.

The IoT poses special challenges with respect to collecting data. Data stored in the cloud may reside in multiple physical locations, whether because it is split across multiple locations or stored in duplicate locations for backup and redundancy storage. Collection of data stored directly on a device may be difficult because forensic data collection tools may lag behind technological innovation of the devices themselves. Security and encryption measures built into devices may make it challenging to gain access, particularly if the owner of the device is either unwilling or unable to voluntarily provide access. The forensic computing industry is struggling to catch up to new technologies, which in turn means that attorneys are struggling to find ways to adequately preserve, collect, and utilize these new forms of electronic information.

Given these challenges, a party may try to resist discovery of devices involving the IoT by arguing that discovery is not proportional or is not reasonably accessible because of undue burden or cost. If the information is only minimally relevant and collecting such information poses an undue challenge, a party may be able to persuade a court not to require its disclosure.

Preservation and the IoT

The IoT has dramatically expanded the volume of ESI being generated. Parties cannot—and

PRETRIAL PRACTICE & DISCOVERY

ABA Section of Litigation

Spring 2018, Vol. 26 No. 2

should not—reasonably be expected to preserve every scrap of electronic data generated across all platforms and devices. Of course, if attorneys are aware that certain IoT data is relevant to claims and defenses in dispute, they should take steps to preserve it.

But preservation obligations may not always be so clear. For example, voice-controlled, home-based digital assistants feature microphones that are always on to hear a user's voice command. Such devices are always listening; when a "wake word" is heard, the device activates and sends a recording of the command to its cloud servers. The command is translated into action—for example, a song will be played or a weather update will be given. If a party is unlikely to have "woken up" the device in connection with a matter relevant to a litigation, is that party still obligated to preserve all of the data created or transmitted by the device? Or may a party justifiably argue that it was reasonable not to preserve such data?

Federal Rule of Civil Procedure 26(f) encourage parties to discuss the scope of discovery, including data preservation and collection issues, at the outset of a case. Several courts, including the Northern District of California and the District of Kansas, have adopted e-discovery guidelines that direct parties to apply the proportionality standard set forth in Rule 26(b)(1) to the discovery plan, including preservation. Attorneys should clearly communicate their expectations as to what data will be preserved by the opposing party because opposing parties and their counsel may not be considering the wide range of electronic data that could be relevant to a case.

Unfortunately, by the time parties reach the discovery stage of litigation, crucial decisions about data preservation may have already been made. Under Federal Rule of Civil Procedure 37(e), the court may issue sanctions for failure to preserve ESI "[i]f electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery." If those threshold criteria are met, the court may fashion sanctions depending on the intent of the spoliating party. Rule 37(e)(1) is designed to address situations where a party loses ESI through negligence. Intent to spoliate evidence is not required under subsection (e)(1); if the court finds prejudice to another party from loss of information, sanctions are still appropriate. On the other hand, if the court finds that a party intentionally spoliated evidence, it may presume that the lost information was unfavorable to that party and instruct the jury to that effect pursuant to subsection (e)(2). The court is also empowered to enter a default judgment or dismiss the case entirely.

PRETRIAL PRACTICE & DISCOVERY

ABA Section of Litigation

Spring 2018, Vol. 26 No. 2

The Sedona Conference has recommended, in its "Commentary on Proportionality in Electronic Discovery," that proportionality principles may be considered when evaluating prelitigation preservation efforts. However, it may be difficult to properly apply principles of proportionality to preservation because a party cannot be certain about the scope of the claims and defenses that may later be asserted. Parties should therefore be cautious in their preservation efforts to help ensure that these efforts are later considered "reasonable" under Rule 37(e) because once ESI is deleted or destroyed, it may be impossible to recover. While this may result in overpreservation, parties may prefer to exercise such caution rather than face potential sanctions.

Kristen B. Weil is a senior managing associate and Ronald J. Hedges is senior counsel with Dentons, based in the New York City office.