small_frog/E+/Getty Images

Handling Internet of Things Data in Litigation

As the reach of the Internet of Things (IoT) expands, counsel must learn to harness the increasing explosion of data to effectively extract relevant information in litigation while balancing the operational and privacy challenges that these new sources of digital evidence raise.

SAMANTHA V. ETTARI
SENIOR COUNSEL
PERKINS COIE LLP

Samantha's extensive experience in privacy, data security, and data management issues includes legal, practical, and reputational risk counseling, often in the context of mergers, acquisitions, and technology-driven strategic and investment transactions. As senior counsel at the firm, she advises clients on both domestic and international privacy statutes and regulations, as well as cross-border transfers of data. Samantha is also a seasoned litigator and trial lawyer and has litigated diverse matters to final judgment, including contract and licensing disputes and false advertising and consumer fraud claims.

The IoT refers to the connection of everyday objects to the internet, including wearable devices (such as Fitbits and Apple Watches), home electronics (such as Nest cameras and home thermostats), devices that employ natural language digital assistants (such as Apple's Siri and Amazon's Alexa), and many others. Many devices that are both connected to the internet and collecting data, either on the device or in the cloud, are likely part of or connected to the IoT.

As sensors have become cheaper and smaller over time, the number of "smart" objects has proliferated and IoT data has grown exponentially. By some estimates, the IoT is poised to generate 600 trillion gigabytes of data per year by 2020 (see Cisco Visual Networking Index: Forecast and Methodology, 2016-2021, June 6, 2017, available at *cisco.com*; Neil M. Richards, *The Dangers of Surveillance*, 126 Harv. L. Rev. 1934, 1940 (2013)).

Unsurprisingly, the IoT data revolution has profound implications for discovery in civil litigation (see *Gordon v. T.G.R. Logistics, Inc.*, 321 F.R.D. 401, 403 (D. Wyo. 2017) (in the context of efforts to

limit the scope of discovery, noting that "[m]ore data has been created in the last two years than in the entire previous history of the human race and the amount of data is predicted to grow 10-fold by 2020")).

However, few written decisions address the use of IoT data in litigation. Those that do offer some guidance on how the data type fits into the larger body of jurisprudence concerning electronically stored information (ESI). Attorneys considering how to use or handle IoT data in litigation must think creatively and extrapolate from this body of law. This requires counsel to understand:

- The types of cases where IoT data may be relevant.
- How and to what extent parties and non-parties should preserve IoT data.
- The various methods for, and issues raised by, collecting and requesting IoT data.

Search The Internet of Things: Key Legal Issues for an overview of legal issues related to the IoT, including the benefits and risks of the IoT and IoT privacy and data security regulation under US federal law.

COMMON CASES IMPLICATING IoT DEVICES AND DATA

As emerging jurisprudence shows, the IoT and IoT data raise a host of novel legal issues in both the criminal and civil context.

CRIMINAL ACTIONS

IoT devices have increasingly provided key opportunities for prosecutors to prove their case, but this may raise significant constitutional questions surrounding a defendant's privacy (see *In re Apple, Inc.*, 149 F. Supp. 3d 341, 364 n.26 (E.D.N.Y. 2016) (noting that allowing the government to compel IoT device manufacturers to "help it surveil the products' users" could "result in a virtually limitless expansion of the government's legal authority to surreptitiously intrude on personal privacy")).

For example, in a highly publicized case, *Arkansas v. Bates*, the state prosecutor sought to obtain from Amazon information and recordings from a murder defendant's Amazon Echo smart speaker. Devices like the Amazon Echo are activated by a "wake word" (such as "Alexa" for the Echo), which triggers recording of data, including what a person says to the device, on cloud servers. Amazon fought the government's demand, but ultimately provided the audio evidence after the defendant consented to the disclosure. (See Amy B. Wang, *Can Amazon Echo Help Solve a Murder? Police Will Soon Find Out*, Wash. Post, Mar. 9, 2017.) Soon after the IoT data was disclosed, the prosecutors dismissed the charges, although it is not clear that any IoT data found (or not found) related to the defendant's Echo is what led to the dismissal (*Arkansas v. Bates*, No. CR-2016-370-2 (2017)).

The *Bates* case ultimately avoided a judicial showdown on the constitutionality of obtaining data from a criminal defendant's IoT-connected home device from a manufacturer like Amazon. However, this trend of seeking information from home IoT devices is likely to continue (see, for example, *Connecticut v. Dabate*, No. TTD-CR17-0110576-T (2017) (building a case against the defendant using the victim's Fitbit data, home alarm sensors, and other digital activity)), and may draw a comparison to existing law permitting tracking technology, such as GPS, as evidence (see, for example, *State v. Jean*, 243 Ariz. 331, 350 n.3 (Ariz. 2018), cert. denied, 138 S. Ct. 2626 (2018) (in a case involving a GPS tracking device that police used to obtain evidence against the defendant, noting that "electronic tracking of people's location ... at the very least in public areas, arguably has gained widespread acceptance and cannot be deemed something society would nevertheless reasonably expect to be private")).

CIVIL ACTIONS

Substantive claims arising directly from or related to IoT devices, along with opportunities to use IoT data in support of or to defend various claims, have become more common in certain types of cases. For example, types of cases that increasingly involve IoT devices and their data include:

- **Data breach cases.** These cases typically allege a vulnerability in an IoT device through which hackers or other unauthorized users have obtained or can obtain data from the device. Plaintiffs in these cases often allege various claims, such as claims based on breach of contract or warranty, violation of state data breach statutes or consumer protection statutes, or common law negligence. (See, for example, *Flynn v. FCA US LLC,* 2018 WL 3303267 (S.D. Ill. July 5, 2018); *Cahen v. Toyota Motor Corp.*, 147 F. Supp. 3d 955 (N.D. Cal. 2015), aff'd, 717 F. App'x 720 (9th Cir. 2017); *In re VTech Data Breach Litig.*, 2017 WL 2880102 (N.D. Ill. July 5, 2017); see also *Edenborough v. ADT, LLC*, 2016 WL 6160174 (N.D. Cal. Oct. 24, 2016).) Since IoT data can be extraordinarily personal and implicates a host of privacy issues, cases seeking to hold manufacturers liable for vulnerability in these devices are on the rise. Additionally, IoT data may be relevant in these cases on questions of liability, such as whether a device collected private information in violation of privacy laws. (For more information, search Key Issues in Consumer Data Breach Litigation on Practical Law.)
- **Consumer fraud class actions.** These actions often target functionality flaws in IoT devices under various state statutory laws and common law (see, for example, *McLellan v. Fitbit, Inc.*, 2017 WL 4551484 (N.D. Cal. Oct. 11, 2017) (alleging that Fitbit misled consumers about the accuracy and reliability of heart rate monitoring on its wearable devices); *Brickman v. Fitbit, Inc.*, 2016 WL 3844327 (N.D. Cal. July 15, 2016) (alleging that Fitbit materially misrepresented the ability of its devices to track sleep-related activities)). In these cases, IoT data is critical to determining how well a device operated compared to its manufacturer's claims.
- **Patent litigation.** An increasing number of patent infringement suits have been filed in recent years concerning the technology underlying an IoT device (see, for example, *Valencell, Inc. v. Apple, Inc.*, 2016 WL 7217635 (E.D.N.C. Dec. 12, 2016) (discovery dispute in a patent infringement

case over Apple Watch's heart sensor technology); *Rensselaer Polytechnic Inst. v. Apple Inc.*, 2014 WL 1871866 (N.D.N.Y. May 8, 2014) (discovery dispute in a patent infringement case against Apple based on Siri's natural language input processing functionality)). As the types of IoT devices proliferate, patent infringement cases over them are likely to become much more common.

- **Personal injury cases.** Plaintiffs and defendants in personal injury and products liability lawsuits are increasingly seeking to use IoT data to support their case, such as to compare a plaintiff's activity levels before and after an injury (see, for example, *Below by Below v. Yokohama Tire Corp.*, 2017 WL 764824 (W.D. Wisc. Feb. 27, 2017) (granting the defendant's request for a spoliation instruction in a personal injury suit where the plaintiff destroyed his pickup truck, which had an electronic data recorder, after an accident)).
- **Matrimonial disputes and defamation cases.** These cases often turn on how parties communicated certain messages and to whom. For that reason, enterprising attorneys are likely to seek discovery of recordings by digital devices like Amazon Echo or Google Home.

PRESERVING IoT DATA

At the outset of a dispute, counsel should analyze whether IoT devices and data may be relevant to any party's claims or defenses (Federal Rule of Civil Procedure (FRCP) 26(b)(1)). While not every case will implicate IoT data, where IoT data may be relevant, counsel should determine early on the potential need to specifically address IoT devices and data with:

- The parties counsel represent.
- Adverse parties or non-parties.

As with other forms of ESI, a data's source or location is a consideration when determining whether and how to ensure preservation of IoT data. Counsel should keep in mind that IoT data is likely to exist in multiple locations that are controlled by various parties and non-parties, including service providers, device manufacturers, and owners of the tangible IoT devices (see below *Possession, Custody, and Control Issues*).

PRESERVATION EFFORTS BY CLIENTS

As with disputes involving other types of ESI, parties must preserve IoT data if it is relevant to pending or reasonably anticipated litigation, or else face sanctions (FRCP 37(e)). Where relevant IoT data also resides on a tangible device, federal common law requires potential litigants to preserve the device when they reasonably anticipate litigation (see *Crown Battery Mfg. Co. v. Club Car, Inc.*, 185 F. Supp. 3d 987, 998 (N.D. Ohio 2016)).

Search Reasonable Anticipation of Litigation Under FRCP 37(e): Triggers and Limits for more on when a party's duty to preserve is triggered.

Counsel preparing a litigation hold for clients should consider including instructions to place a litigation hold on IoT devices and their data. Because the IoT is a relatively new concept, some litigants or document custodians may be unfamiliar with the term or fail to recognize IoT devices as a potential source of relevant information. Therefore, counsel should avoid boilerplate language that instructs parties to simply preserve "Internet of Things data." Instead, a litigation hold that seeks to preserve IoT devices and data should:

- **Specifically describe the IoT devices and data subject to the hold.** For example, where possible, counsel should direct custodians to preserve relevant IoT devices, related applications, and data by identifying the potential devices subject to the hold by name. If counsel does not know what types of IoT devices the client may have, describing common and relevant examples of IoT devices, such as Amazon Echo, Google Home, Fitbit, or smart TVs, may help the client identify what IoT devices and data it may need to preserve.
- **Identify the type of IoT data likely to be relevant.** For example, where possible, counsel should specify the individuals likely to have generated IoT data along with applicable date ranges and times for the IoT data and devices that should be preserved. When determining this information, counsel should consider, for example:
  - why an IoT device may have captured relevant statements by key individuals in the litigation (such as why a "wake

Counsel should keep in mind that IoT data is likely to exist in multiple locations that are controlled by various parties and non-parties, including service providers, device manufacturers, and owners of the tangible IoT devices.

word" may have been used at a particular time that would trigger the device to record); and

- whether the individuals were in close proximity to the device when the statements were made and, therefore, whether the device was likely to have captured relevant statements.

Additionally, if counsel has any concern that a relevant IoT device may be destroyed or misplaced, counsel should consider pursuing the collection of the IoT device and data as soon as possible, such as by imaging a client's device. This type of preservation-by-collection approach can guard against the risks that:

- The loss or destruction of an IoT device may render relevant data inaccessible, and make it difficult or impossible to preserve related data.
- Client IoT data that resides with non-party data service providers may expire under the providers' existing retention periods. These providers may have short retention periods for that data, particularly where the device owner's subscription does not include payment for the provider to maintain the data on a long-term basis.

Search Litigation Hold Toolkit for a collection of resources to help counsel preserve a client's documents and implement a litigation hold.

When determining the scope of a litigation hold, counsel should keep in mind the proportionality principles embedded in FRCP 26(b)(1) and the difficulty and cost associated with preserving certain forms of ESI, which may extend to IoT data (FRCP 26(b)(1) ("[p]arties 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")).

Courts have not, to date, clearly endorsed invoking proportionality principles to limit the scope of preservation. However, courts must now consider proportionality when determining the reasonableness of a party's preservation decision (2015 Advisory Committee's Note to FRCP 37(e) ("Due to the ever-increasing volume of [ESI] and the multitude of devices that generate such information, perfection in preserving all relevant [ESI] is often impossible. ... This rule recognizes that 'reasonable steps' to preserve suffice; it does not call for perfection. ... Another factor in evaluating the reasonableness of preservation efforts is proportionality. ... [A]ggressive preservation efforts can be extremely costly ...")).

Where the burden of preserving large amounts of ESI from an IoT device appears disproportionate, counsel should:

- Before litigation has commenced:
  - explore the possibility of reaching an agreement with known adverse parties to limit the scope of discovery and determine how much ESI to preserve;
  - research any applicable case law that may apply to the facts of the particular case and support a decision not to preserve certain categories of IoT data; and
  - if counsel decides not to preserve certain IoT data, thoroughly document the reasons for the decision in the event of a later challenge.
- After litigation has commenced, seek a protective order from the court to limit discovery (see below *Proportionality Concerns*).

Search Sanctions for ESI Spoliation Under FRCP 37(e): Overview for more on determining the scope of a party's duty to preserve ESI under FRCP 37(e).

PRESERVATION DEMANDS TO ADVERSE PARTIES AND NON-PARTIES

A preservation letter may be required when counsel has determined that adverse parties or non-parties, such as device manufacturers and data service providers, might be in possession, custody, or control of IoT data relevant to the dispute.

As with a litigation hold, any preservation letter in this scenario should specifically request:

- The preservation of IoT devices and data and, where possible, identify the devices and data to preserve.
- The suspension of any auto-delete features or programs, such as those that non-party service providers may have in place that delete certain data after a short retention period based on the device owner's type of data subscription.

Search Non-Party Responses to Preservation Demands for information on the key issues and practical considerations for non-parties who receive a demand to preserve potentially relevant ESI before a complaint has been filed or a subpoena has been served.

Search Document Preservation Letter (Demand) and Document Preservation Letter for a Cloud Service Provider for sample preservation demands that counsel can use to ask an adverse party or a non-party to preserve relevant evidence, with explanatory notes and drafting tips.

COLLECTING AND REQUESTING IoT DATA

Where IoT data is relevant in a litigation, counsel must carefully consider:

- Defensible methods to collect IoT data.
- The appropriate parties or non-parties from whom to request the relevant IoT data.
- The potential need for protective orders, given the privacy and confidentiality issues that the disclosure of IoT data is likely to raise.

COLLECTION METHODS

Collection of IoT data may take multiple forms. As with other forms of ESI, a vendor may be retained to forensically collect the data. Alternatively, data that is readily accessible from an IoT device or a related application or website may be collected by counsel or the client. However, if counsel intend to collect the data, or have the client collect the data, counsel should

consider discussing collection methods with opposing counsel to eliminate objections later.

Search Back It Up: Custodian-Directed Preservation of iPhone Data for guidance on incorporating a custodian-directed iPhone backup technique into a preservation and collection protocol.

Other considerations for counsel when collecting IoT data include:

- **The form of the IoT data.** For example, some IoT data can be readily downloaded into a spreadsheet or other similar word processing format.
- **The accessibility of the IoT data.** Some IoT data may require software to read and translate the data. If the software is costly or proprietary, counsel may need to analyze cost, burden, and proportionality under FRCP 26 (see above *Preservation Efforts by Clients* and see below *Proportionality Concerns*).

As with all forms of evidence, counsel should consider how to authenticate and use the IoT data in dispositive motions or at trial. Where IoT data is retrieved from a non-party service provider or manufacturer, counsel may need to authenticate the data by establishing account credentials and ownership through:

- Interrogatories, requests for admission, or depositions.
- Other common or uniform credentials, such as email or physical addresses, telephone numbers, photographic identifiers, or biometric data that links the IoT data with the device owner.

Search E-Discovery: Authenticating Electronically Stored Information for information on the standard and process for authenticating ESI in federal court under the Federal Rules of Evidence.

POSSESSION, CUSTODY, AND CONTROL ISSUES

If adverse parties may possess potentially relevant IoT data, counsel should separately request production of IoT data through document requests under FRCP 34, which allows a party to request ESI that is within the other party's "possession, custody, or control" (FRCP 34(a)(1)(A)). However, counsel should be cognizant of varying jurisdictions' views on what constitutes "control" of IoT data in analogous ESI cases.

Obtaining IoT data from non-party custodians is not as simple as issuing subpoenas under FRCP 45. Among other complications, counsel must determine whether:

- The adverse party is also in possession, custody, or control of the IoT data sought from a non-party provider.
- Certain statutes or regulations prevent or limit a non-party's ability to disclose certain IoT data, such as health data or some electronic communications (see below *Protective Orders*).

Before issuing a subpoena to a non-party provider, counsel should determine whether the adverse party might have copies of the IoT data. As with many sources of discovery, requesting IoT data from an adverse party may ultimately be the most direct route to the data. Indeed, courts often resolve disputes over subpoenas to non-party providers by requiring the parties to directly provide the information sought from non-parties (see, for example, *McBeath v. Tucson Tamale Co.*, 2017 WL 3118779, at *10 (D. Ariz. July 21, 2017) (denying a motion to compel non-party Google to disclose the defendants' emails and directing the defendants to produce the requested emails instead)).

Search Possession, Custody, and Control of ESI for information on the traditional tests that courts use to determine control over ESI in a non-party's possession and emerging jurisdictional issues related to cloud-based ESI.

Search Document Requests and Subpoenas in Federal Court Toolkit for a collection of resources to help counsel serve and respond to document requests and subpoenas in federal court.

PROTECTIVE ORDERS

Protective orders concerning IoT data may be particularly appropriate in discovery for various reasons, including because:

- Potentially massive volumes of IoT data raise a significant risk of disproportionately expensive and burdensome discovery.
- Access to IoT data may be unreasonably burdensome or expensive.
- IoT data often includes extremely personal and confidential information or implicates electronic communications that a non-party may not disclose without the consent of the party who made the communication.

Any of these circumstances may encourage counsel to seek protective orders to set parameters around the production, use, and destruction of IoT data.

Proportionality Concerns

Courts recognize that producing massive amounts of IoT data is potentially burdensome and may be disproportionate to the needs of the case (FRCP 26(b)(1)).

Where discovery requests for IoT data are burdensome, counsel should meet and confer before moving for a protective order (see, for example, *Mancia v. Mayflower Textile Servs. Co.*, 253 F.R.D. 354, 364-65 (D. Md. 2008) (issuing an order *sua sponte* requiring counsel to meet and confer in good faith to address potentially burdensome discovery)). For example, counsel can seek agreement on alternative methods for producing relevant IoT data and ESI collection protocols, and on the scope of requested data given proportionality considerations.

Absent a good faith conference, courts have demonstrated a willingness to fashion their own solution for discovery of relevant data from a voluminous ESI universe, which may differ from counsel's preferred approach (see, for example, *Solo v. United Parcel Serv. Co.*, 2017 WL 85832, at *3 (E.D. Mich. Jan. 10, 2017)).

Requesting IoT data from an adverse party may ultimately be the most direct route to the data. Indeed, courts often resolve disputes over subpoenas to non-party providers by requiring the parties to directly provide the information sought from non-parties.

Access to IoT Data

A protective order may be required where access to IoT data is not reasonable because of undue burden or cost (FRCP 26(b)(2)(B)). Factors that courts may consider when determining whether particular IoT data is accessible include:

- Whether the cost to access or produce the data appears excessive.
- Whether the data is encrypted and can readily be decrypted.
- The form or usability of the data.
- The location of the data.

In addition to logistical issues associated with the location of data, where data resides also impacts whether the data may be legally extracted and produced. For example, data located outside the US may be subject to foreign privacy laws that hinder or bar the data's production in the US (see, for example, *In re: EpiPen*, 2018 WL 1440923, at *4 & n.20 (D. Kan. Mar. 15, 2018) (noting that additional issues stemming from the location of a potential ESI custodian and related data in France made it "unduly burdensome and expensive to search, review, and produce ESI" within the custodian's possession)).

If any or all of these factors apply in a case, a court is likely to issue a protective order (see, for example, *BAT LLC v. TD Bank*, N.A., 2018 WL 3626428, at *8 (E.D.N.Y. July 30, 2018) (granting a motion for a protective order and declining to compel a party to produce data archived offline as inactive, which required special technology to access)). However, if IoT data, whether active or archived offline, is readily accessible, counsel can reasonably request or expect to produce the data.

Search Cross-Border Discovery Under the GDPR for more on issues and restrictions raised by cross-border discovery.

Search Protective Order for Documents Protected by Non-US Data Protection Laws for a sample protective order that counsel can use when non-US data protection laws apply to documents sought in federal litigation, with explanatory notes and drafting tips.

Privacy and Confidentiality Concerns

Disclosure of IoT data raises important privacy and confidentiality issues. Individual litigants may be wary of producing personal health, biometric, or private home-related data from IoT devices. Corporate litigants may have concerns about producing sensitive IoT data, including underlying source code or camera or audio files.

Moreover, requests for disclosure of IoT data may implicate laws or regulations that restrict the transfer or processing of personal information. For example, the Stored Communications Act (SCA) generally prevents providers of electronic communication services from divulging private communications (18 U.S.C. §§ 2701-2712; see, for example, *Sines v. Kessler*, 2018 WL 3730434, at *2, *10 (N.D. Cal. Aug. 6, 2018) (quashing the portion of a subpoena seeking communications from a private, invite-only social networking and instant messaging platform because disclosure from the provider would violate the SCA)). Courts may view certain records from IoT devices, such as records of questions asked of "Alexa" or "Siri," as protected communications under the SCA.

However, the SCA does not preclude a court from compelling disclosure directly from a party who also has possession, custody, or control of the communications (see *Flagg v. City of Detroit*, 252 F.R.D. 346, 366 (E.D. Mich. 2008) (in a dispute over a subpoena to a non-party provider, holding that the SCA did not preclude discovery of text messages that remained within the defendant's control and ordering the plaintiff to serve a document request under FRCP 34 directly to the defendant for the messages, noting that the court could then resort to the "usual mechanisms for ensuring the parties' compliance" under FRCP 37)).

Search Social Media: What Every Litigator Needs to Know for information on subpoenas to non-party social media providers and how the SCA applies in that context.

Search Motion for a Protective Order (Federal): Proposed Order for a sample protective order that counsel can use to protect IoT data and other sensitive information in federal litigation, with explanatory notes and drafting tips.