wgs

The Sedona Conference

Primer on the Electronic Discovery Implications of the Internet of Things (IoT)

A Project of The Sedona Conference Working Group on Document Retention and Production (WG1)

July 2025
Public Comment Version
Submit comments by Sept. 5, 2025,
to comments@sedonaconference.org

The Sedona Conference®

The Sedona Conference Primer on the Electronic Discovery Implications of the Internet of Things (IoT)

A Project of The Sedona Conference Working Group (WG1) on Electronic Document Retention and Production

JULY 2025 PUBLIC COMMENT VERSION

Drafting Team Leaders

Greg M. Kohn Josh Zylbershlag

Senior Editor

Ross M. Gotler

Drafting Team

David K. Gaston Christopher A. Suarez

Kevin M. Clark Kyle Pozan

Mikaela Bock Sara Lockman

Warren G. Kruse II Steve W. Teppler

Dan Regard

Judicial Observer

Juan G. Villaseñor

Steering Committee Liaisons

Lea Malani Bays Ross M. Gotler

REPRINT REQUESTS:

Requests for reprints or reprint information should be directed to
The Sedona Conference at info@sedonaconference.org.

Visit www.thesedonaconference.org

Preface

Welcome to the July 2025 Public Comment Version of The Sedona Conference's Primer on the Electronic Discovery Implications of the Internet of Things (IoT), a project of The Sedona Conference Working Group 1 on Electronic Document Retention and Production (WG1). This is one of a series of Working Group papers published by The Sedona Conference, a 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of complex litigation, intellectual property rights, data security and privacy, and artificial intelligence.

The mission of The Sedona Conference is to move the law forward in a reasoned and just way. The mission of WG1, formed in 2002, is "to develop principles, guidance and best practice recommendations for information governance and electronic discovery in the context of litigation, dispute resolution and investigations." WG1 has published the authoritative Sedona Principles addressing electronic document production and several companion works, including guidelines for electronic document management, several commentaries on eDiscovery related topics, and cooperation guidance for trial lawyers, in-house counsel, and the judiciary.

This Primer has been in the making for a long time, reflecting significant advancements in the underlying technology while the Primer was being drafted. The initial "Brainstorming Group" began meeting in November 2020 and generated its project charter in May 2021. A detailed progress report was presented at the WG1 Annual Meeting in October 2021 and the first draft presented to the membership for review and comment at the April 2022 Midyear Meeting. There was a brief re-engagement with the membership at the Midyear Meeting in April 2023, after which the drafting team made significant updates to the Primer, in spite of tremendous competition for attention from developments in Artificial Intelligence and Discovery of Mobile Device Data. The paper was then presented to the membership at the WG1 Annual Meeting in October 2024 for further dialogue. A Member Comment Draft was submitted to the entire Working Group Series membership in May 2025. The editors reviewed the comments received through the entire Working Group Series review and comment process and this version is the result.

This Primer represents the collective efforts of many individual contributors. On behalf of The Sedona Conference, I thank in particular Drafting team Leads Greg M. Kohn and Josh Zylbershlag. I also thank everyone else involved for their time and attention during this extensive drafting and editing process, including David K. Gaston, Christopher A. Suarez, Kevin M. Clark, Kyle Pozan, Mikaela Bock, Sara Lockman, Warren G. Kruse II, Steven W. Teppler, Dan Regard, and WG1 Steering Committee Liaisons Lea Malani Bays and Ross M. Gotler.

The drafting process for this Primer has also been supported by the Working Group 1 Steering Committee and Judicial Advisor Hon. Juan G. Villaseñor of Colorado. The statements in this Primer are solely those of the members of the Working Group; they do not represent any judicial endorsement of any recommended practices.

Please note that this version of the Primer is open for public comment through Sept. 5, 2025, and suggestions for improvements are welcome. After the deadline for public comment has passed, the drafting team will review the public comments and determine what edits are appropriate for the final version. Please send comments to comments@sedonaconference.org.

We encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG12 and several other Working Groups in the areas of artificial intelligence, electronic document management and discovery, cross-border discovery and data protection laws, international data transfers, data security and privacy liability, patent remedies and damages, and patent litigation best practices. The Sedona Conference hopes and anticipates that the output of its Working Groups will evolve into authoritative statements of law, both as it is and as it should be.

Kenneth J. Withers
Executive Director
The Sedona Conference
July 2025

Table of Contents

I. INTRODUCTION

In the Information Age, the Internet of Things (IoT) has emerged as a transformative force. The IoT, a term commonly used to describe the network of interconnected devices that communicate with one another directly and through the internet, has created an extensive web of connectivity interlinking billions of devices. These IoT devices continuously generate, transmit, and store data, fundamentally altering the information landscape. This evolution has introduced a new frontier in the legal domain, particularly in the realm of electronic discovery – the law and process around the discovery of electronically stored information ("ESI").

The implications of such "IoT ESI" are profound and multifaceted. For instance, consider a fleet management system used to resolve classic on-the-clock/off-the-clock wage and hour claims. Such a system can provide precise data on vehicle locations, driver activities, and time logs, offering critical evidence in employment disputes. Similarly, smart home devices, such as thermostats and security cameras, can generate data that may be pivotal in civil litigation, providing insights into occupancy patterns and activity timelines relevant to property disputes or insurance claims.

The integration of IoT ESI into legal proceedings marks continued evolution in the electronic discovery process. However, this integration is not without its complexities. The sheer volume, variety, and velocity of ESI generated by IoT devices present unique challenges. Legal professionals must navigate issues related to data privacy, security, and the authenticity of IoT ESI. Additionally, the decentralized nature of IoT ESI, often spread across multiple devices and platforms, complicates the collection, preservation, and analysis processes.

This *Primer on the Electronic Discovery Implications of the Internet of Things* aims to provide judges, practitioners, and parties with an understanding of the unique aspects of IoT ESI. Specifically, this *Primer* will provide an overview of what constitutes IoT ESI, and explore how IoT impacts traditional electronic discovery processes, including practical guidance for managing IoT throughout the electronic discovery life cycle.

Other papers published by The Sedona Conference may be read along with this *Primer* to help provide a broader understanding of the impact of technology on the electronic discovery process; they are referenced in context below.

By fostering a deeper understanding of IoT ESI and its implications, legal professionals will be better equipped to navigate the complexities of IoT discovery.

II. UNDERSTANDING IOT DEVICES AND IOT ESI

The term IoT "refers to the collective network of connected devices and the technology that facilitates communication between devices and the cloud, as well as between the devices themselves."[1] A seemingly endless array of types of IoT devices are in use today, both in the home and business contexts;[2] billions of IoT devices are already active, with billions more to come.[3] As opposed to typical computing devices like computers, laptops, and tablets, IoT devices are "physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment."[4] Understanding the specific applications and implications of IoT devices in these areas can provide helpful background that can assist with effectively managing IoT ESI in legal proceedings.

A. Context of IoT Devices

The IoT encompasses a wide range of devices that are integrated into various contexts, each serving distinct purposes and offering unique benefits. These contexts include commercial, consumer, and industrial/engineering/diagnostics environments.

1. Commercial

In the commercial context, IoT devices can be utilized as part of operations, security, and customer experience. Examples include:

- **Smart Retail Shelves**: These devices can monitor inventory levels in real time, alerting staff when restocking is needed.
- **Building Management Systems**: Systems in buildings can analyze occupancy and usage patterns and control aspects of the environment such as lighting, heating, and cooling.
- **Asset Tracking**: Using GPS and RFID tags, these systems monitor the location and condition of assets in transit or storage, as part of logistics and asset management.

---

1 Amazon Web Services, *What is the Internet of Things (IoT)?*, https://aws.amazon.com/what-is/iot/ (last visited Apr. 7, 2025).

2 *See, e.g.*, Scientific Working Group on Digital Evidence, *SWGDE Technical Notes on Internet of Things (IoT) Devices, Version: 1.0* (Sept. 17, 2020), https://www.swgde.org/20-f-004/.

3 An International Data Corporation (IDC) report predicts that by 2025, 73.1 Zettabytes (ZB) of data will be generated from 55.7 billion connected IoT devices. *Worldwide Global DataSphere IoT Device and Data Forecast, 2019-2023* (IDC #US45066919, May 2019).

4 Gartner Information Technology Glossary, *Internet Of Things (iot)*, http://www.gartner.com/en/information-technology/glossary/internet-of-things (last visited Apr. 7, 2025).

2. Consumer

In the consumer context, many IoT devices focus on improving the convenience, comfort, and health of individuals. Examples include:

- **Fitness Trackers**: These devices collect data on physical activity, heart rate, and sleep patterns, helping individuals monitor and manage their health and fitness.
- **Smart Home Devices**: This category includes smart thermostats, security cameras, and voice assistants that automate and control various aspects of home life.
- **Wearable Health Monitors**: Devices such as these continuously track vital signs like blood pressure and glucose levels, providing alerts and insights for health management.
- **Smart Appliances**: Appliances like refrigerators, ovens, and washing machines can be controlled remotely and provide status updates and maintenance alerts.

3. Industrial/Engineering/Diagnostics

IoT devices in engineering and diagnostics are used for monitoring, maintenance, and troubleshooting of industrial systems and machinery. Examples include:

- **Predictive Maintenance Sensors**: These sensors monitor the condition of equipment, predicting failures before they occur and scheduling maintenance accordingly.
- **Environmental Sensors**: These devices measure variables like temperature, humidity, and pressure in industrial environments to manage operating conditions and equipment function.
- **Industrial Robots**: Robots may be equipped with sensors to monitor their own performance and detect anomalies as part of their operation in manufacturing and other industrial settings.

B. Methods of Communication and Control

IoT devices employ various methods of communication and control to manage data and interactions. These methods are influenced by the nature of the data, which is often system-generated, shared in small quantities, and triggered by specific thresholds and algorithms.

User-activated IoT devices are designed to be accessed, controlled, or operated through direct user interaction. These are among the most common types of consumer context IoT devices. Examples include a wide range of home automation devices such as TVs, lighting systems, HVAC controls, home appliances, vacuums, door locks, garage door openers, and lawn sprinklers. These devices typically require no infrastructure and minimal training to deploy. They can be used individually or in collections, providing flexibility and ease of use for consumers.

Application-managed IoT devices are controlled via applications that can be installed on pre-existing devices, such as smartphones, tablets, or computers. These devices may lack physical buttons or screens. An example is the Apple AirTag, which provides haptic and sound feedback through vibrations and beeps. This category also includes commercial and industrial sensors such as RFID tags, edge devices, and flow meters.

Web-based management platform IoT devices allow authorized users to log into a web-accessible interface to control specific devices. For instance, a factory supervisor can use a web interface to monitor sensors placed on multiple robots on the production floor. This method provides centralized control and monitoring, which is particularly useful in industrial and commercial settings.

Many consumer IoT devices now feature hybrid controls, allowing them to function independently while offering enhanced data and functionality when paired with a smartphone or tablet. For example, modern thermostats can connect to smartphones, enabling users to view energy consumption and usage data that is not directly accessible from the thermostat itself.

Different IoT ESI may be communicated to different stakeholders. A single device may be accessible via user activation with local controls, supported by a smartphone app to display trending data over time, while providing additional data to the manufacturer for troubleshooting, product improvement, or monetization purposes. For instance, a robotic vacuum could have local on-and-off controls, could send usage and maintenance details to the user's smartphone, could send room layout and diagnostics data to the manufacturer, and the manufacturer could re-sell information on usage peaks to the local utility company.

C. Storage Locations of IoT ESI

The data associated with IoT devices—IoT ESI—can be found in multiple locations. Understanding these potential data locations can help with later analysis and planning for discovery.

- **Internal Storage**: Many IoT devices have built-in storage where data is directly recorded and stored. This can include logs of device activity, sensor readings, and user interactions. For example, a fitness tracker may store data on steps taken, heart rate, and sleep patterns within its internal memory.

- **Local Servers and Gateways**: IoT devices often communicate with local servers or gateways that aggregate and process data from multiple devices. These local systems can store substantial amounts of IoT data before it is transmitted to cloud servers or other external locations. For instance, a smart home hub may collect and store data from various connected devices such as thermostats, security cameras, and lighting systems.

- **User Devices**: Data from IoT devices can also be stored on user devices such as smartphones, tablets, and computers. Applications that manage IoT devices often store data locally on these devices, providing users with access to historical data and device settings.

For example, a smartphone app controlling a smart thermostat may store temperature settings and usage history locally on the mobile device or in the cloud and accessed via the device.

- **Cloud Service Providers**: Many IoT devices transmit data to cloud storage services managed by third-party providers. Cloud storage offers scalable and secure data storage solutions, allowing for the aggregation and analysis of large volumes of IoT ESI. For example, data from industrial IoT sensors may be sent to a cloud platform for real-time monitoring and predictive maintenance analysis.

- **Device Manufacturers**: IoT device manufacturers often collect and store data from their devices for various purposes, including troubleshooting, product improvement, and customer support. This data can include diagnostic information, usage patterns, and firmware updates. For example, a manufacturer of smart appliances may collect data on appliance performance and user interactions to enhance product features and address issues.

- **Service Providers**: Service providers that offer IoT solutions, such as home security services or fleet management systems, may store data on their servers. This ESI can include service logs, user activity, and system alerts. For instance, a home security service provider may store video footage and alarm logs from connected security cameras.

- **Internet Service Providers (ISPs)**: Data transmitted by IoT devices over the internet may be logged by ISPs. These logs can include information on data transmission times, IP addresses, and data volumes. While ISPs typically do not store the content of the data, their logs can provide valuable metadata for understanding data flow and connectivity.

- **Communication Gateways**: IoT devices often use communication gateways, such as routers and modems, to connect to the internet. These gateways can log data transmission events, providing insights into device connectivity and network performance.

- **Integrated Services and Platforms**: IoT devices that integrate with third-party services and platforms may generate data that is stored by these external entities. For example, a smart home device that integrates with a voice assistant platform may have data stored by the voice assistant service provider, including voice commands and interaction logs.

III. THE IOT RAISES UNIQUE DISCOVERY PRACTICE ISSUES

In this section of the *Primer*, we address the implications of IoT devices and ESI with respect to various legal practice issues relating to discovery. Here we will focus on unique impacts of IoT, leaving a broader discussion about discovery law to other commentaries and sources.[5]

---

[5] Such publications include The Sedona Conference, *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, 19 SEDONA CONF. J. 1 (2018); others are listed below. A full

A. Scope of Discovery, Proportionality, and Limitations

Aspects of IoT ESI may introduce novel considerations relating to a determination of the appropriate scope of discovery under Federal Rule of Civil Procedure 26(b). As an example, in a typical proceeding, a responding party may successfully resist discovery for detailed network or device log information, arguing that such log information is clearly beyond the scope of reasonable and proportional discovery as set forth in Rule 26(b)(1)[6] or is not reasonably accessible under Rule 26(b)(2)(B).[7] However, in a case involving an industrial workplace accident, logs from sensors embedded in machinery could be vital. These logs might record operational parameters, maintenance activities, and any anomalies or malfunctions leading up to the incident. Such data can help determine whether equipment failure or human error contributed to the accident, demonstrating clear importance to the case. Additionally, in a case involving industrial accidents, historical data from sensors embedded in machinery might be relevant; however, retrieving this data could require accessing legacy systems or physically extracting data from devices that are no longer in use. In an injury case, data from wearable health monitors, sensors, or cameras could all be relevant to prove aspects of the case. Finally, in a dispute involving a smart home system, logs from devices like smart thermostats or security cameras might be crucial, even though the logs are stored in proprietary formats on the devices or in fragmented cloud storage, making retrieval complex and costly.

In these examples, while the IoT ESI may appear not reasonably accessible due to technical, logistical, or financial burdens, a proportionality analysis may still justify its inclusion in the scope of discovery if the importance of the information outweighs the challenges of accessing it.

---

list of publications from The Sedona Conference relating to electronic discovery may be found at http://thesedonaconference.org/publications.

6 Under the proportionality principle set forth in Federal Rule of Civil Procedure 26(b)(1):

> Unless otherwise limited by court order, the scope of discovery is as follows: 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, considering 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. Information within this scope of discovery need not be admissible in evidence to be discoverable.

FED. R. CIV. P. 26(b)(1). For a detailed discussion of proportionality, please *see* The Sedona Conference, *Commentary on Proportionality in Electronic Discovery*, 18 SEDONA CONF. J. 141 (2017).

7 As set forth in the Rule:

> A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.

FED. R. CIV. P. 26(b)(2)(B).

Parties should collaboratively discuss, and courts should take note of, the most accessible, least burdensome sources for such discovery of relevant IoT ESI.[8] Requesting parties should consider what IoT ESI may reasonably be expected in a given matter and producing parties should give thought to what IoT ESI may be implicated in the case and determine how it could be collected and produced. For example, instead of accessing an IoT device itself—such as a wearable for location tracking—it may be less burdensome, and more helpful, to obtain discovery from the mobile phone-based application that gathers and presents information from the wearable.

In *Spoljaric v. Savarese*, the court denied a motion to compel the plaintiff's Fitbit data, finding the defendant's argument for needing it was speculative and that there was insufficient evidence to support that the data would be relevant—the plaintiff testified that he rarely checked his Fitbit and used it mostly as a watch.[9] The court saw the request as an "overly broad 'fishing expedition'" without a substantial basis.[10] The finding was similar in *In re 3M Combat Arms Earplug Prods. Liab. Litig.*[11] There, the court held that the "reliability and usefulness" of hearing data from Apple Health app was "diluted" and declined to compel its production.[12]

B. Initial Disclosures and Discovery Planning

When discovery involves IoT ESI, parties should address unique issues related to IoT ESI early and as part of their conferences and discovery planning, consistent with requirements such as those in Federal Rules of Civil Procedure 26(a) and 26(f).

As required by Rule 26(a)(1)(A)(ii), parties must be prepared to identify and disclose sources of ESI, including IoT ESI, that they may use to support their own claims or defenses. Since Rule 26(a) does not impose any obligations to disclose information or documents to support an adverse party's claims or defenses, where IoT ESI may be at issue, practitioners should consider proactive steps to educate themselves on the adverse party's IoT sources and the parties should discuss these sources during the development of their discovery plan. For example, in a case involving a dispute over the performance of smart home devices, the parties may need to educate each other on the various IoT data sources, such as sensor logs, device usage records, and firmware updates. They may also need to discuss available collection methods and any perceived challenges, such as the time required to extract data, the costs involved, the volume of data generated, and control over the data stored on third-party servers.

---

8 Technical experts may be helpful here and at many stages throughout the IoT discovery process.

9 Spoljaric v. Savarese, 66 Misc. 3d 1220(A), 121 N.Y.S.3d 531, 2020 WL 611911 (N.Y. Sup. Ct. 2020). *But see, e.g.*, Bartis v. Biomet, Inc., No. 4:13-CV-00657-JAR, 2021 WL 2092785, at *2 (E.D. Mo. May 24, 2021) (compelling the production of Fitbit data in a personal injury case).

10 Spoljaric, 2020 WL 611911, at *2.

11 *In re* 3M Combat Arms Earplug Prods. Liab. Litig., No. 3:19-md-2885, 2022 WL 4448917 (N.D. Fla. Sept. 23, 2022).

12 *Id.* at *5.

As part of developing a discovery plan, parties commonly agree on the form of production, specifying detailed requirements for technical formatting and metadata fields. However, with IoT ESI, the information necessary to determine such production specifications may not be available during the early stages of proceedings, which is typically when ESI protocol agreements are made. Furthermore, the complexity and variety of IoT ESI can make it challenging to reduce to a specific production format. For example, determining whether the production format for environmental sensors in a warehouse should be the proprietary back-end database, a conversion to .csv format, a collection of reports from the management interface, or a combination of these options, might not be feasible until later stages. As such, parties and courts, when agreeing to and interpreting ESI protocols, should remain flexible and open to revisiting production specifications as more information about IoT ESI becomes available. This could be dealt with, for example, by including a specific provision related to IoT ESI in the ESI protocol, with the IoT ESI production format to be agreed upon later. Such a collaborative approach can help ensure practical and efficient production formats, accommodate the diversity of IoT ESI, and align with the principles of proportional discovery.

When addressing complex IoT ESI sources, it may be beneficial for parties to engage technical and business experts early. This helps address key questions during Rule 26(f) conferences and can aid in developing practical, proportional discovery plans.[13] Coordinated efforts of the parties, with the guidance of these experts, can facilitate negotiations over the scope of discovery and streamline the process of reaching an agreement or informing the court.[14] As part of discussions between parties, understanding how the requesting party intends to use IoT ESI can aid in evaluating the burden versus benefit aspects of proportionality considerations.[15]

---

13 A discovery plan between parties "must state the parties' views and proposals on . . . any issues about disclosure, discovery, or preservation of electronically stored information, including the form or forms in which it should be produced." FED. R. CIV. P. 26(f)(3).

14 This approach aligns with *The Sedona Conference Database Principles*, which similarly advocate for practical, proportionate strategies to handle complex data sources during discovery. The Sedona Conference, *Database Principles: Addressing the Preservation and Production of Databases and Database Information on Civil Litigation*, 15 SEDONA CONF. J. 171 (2014).

15 *Id.*, cmt. 6.A.:

> While a requesting party is not required to divulge its counsel's work product or its litigation strategy, it may be impossible for a responding party to take appropriate steps to provide database information in a reasonably useful format if it does not know how the requesting party intends to use it. A requesting party's failure or refusal to identify the intended use of database information, especially upon request, may limit the responding party's ability to accommodate the format request, particularly where the responding party's preferred format is less expensive and appears *ex ante* reasonable. To maximize the value of the database information it will receive, a requesting party should provide detail sufficient to describe the tools or broad evidentiary use that it intends to make of this material.

C. Possession, Custody, or Control

Federal Rule of Civil Procedure 34 allows parties to serve on other parties a request for documents within their "possession, custody, or control."[16]

Determining possession, custody, or control of IoT ESI for the purposes of Rule 34 can be challenging and often depends on the specifics of the requested IoT ESI and the circumstances of its creation and storage. These challenges, while present with other forms of ESI, are often amplified by the interconnected nature of IoT devices.

Evaluating possession, custody, or control involves understanding how and where data is created, generated, derived, stored, or transmitted. Data might originate from a device, be processed and modified locally, then stored in repositories or transmitted to downstream locations—or a combination of these stages. For example, IoT ESI from a Peloton bike could be generated by the bike, created or derived by a smartphone or smartwatch application, or stored on a user's apps or on platforms managed by Peloton. Here, the ESI from a Peloton exercise bike might be under the control of both the user (who purchased the bike or holds the account) and the service provider (Peloton). Analyzing these layers helps identify access points and determine who controls the ESI at various stages within the IoT ecosystem.

A real-world example can be seen in *Garner v. Amazon.com, Inc.*[17] In this matter, the defendants moved to compel the plaintiffs to identify recordings from their Amazon Alexa devices that they claimed were private and confidential. The plaintiffs argued Amazon had not produced all relevant recordings and the parties were negotiating a production process when Amazon filed the motion to compel. The court found most plaintiffs could access their recordings through the Amazon portal or Alexa app and must identify the relevant recordings. However, three plaintiffs' claims involved recordings by Amazon Alexa devices owned by non-parties. For these plaintiffs, the court acknowledged they could not access the necessary information and excused them from this requirement.

In determining possession, custody, or control of IoT ESI in particular, additional considerations can include:

- The existence and substance of legal agreements, contracts, terms, or conditions specific to data collection, usage, transfer, and sale of IoT data.

- National, regional, or local privacy laws that may provide avenues for end users, corporations, consumers, or employees to request copies of ESI generated by an IoT device or system.

---

16 FED. R. CIV. P. 34(a)(1). While this topic is explored in The Sedona Conference, *Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control*," 25 SEDONA CONF. J. 1 (2024), IoT ESI presents some distinct considerations.

17 Garner v. Amazon.com, Inc., No. C21-0750RSL, 2022 WL 4753013 (W.D. Wash. Oct. 3, 2022).

- The physical and digital access a party has to the IoT device, related software, or system components, and whether relevant data may be reasonably accessible through multiple endpoints or access points within the IoT ecosystem.

- The retention policies associated with the data generated by the IoT device, storage locations, or related systems.

- An understanding of any monitoring or logging resources that aggregate, summarize, or otherwise process IoT device data.

- Backup, synchronized, secondary, or duplicate resources that store data created by the IoT device.

If a party does not have possession, custody, or control over the IoT ESI at issue, discovery from non-parties may be appropriate.[18]

D. Privacy

IoT ESI may be more likely to raise privacy concerns than many other ESI sources since IoT devices can collect highly detailed, real-time personal information about individuals' activities, behaviors, and even physical conditions. For example, fitness trackers monitor health metrics, smart home devices track daily routines, and smart speakers may record conversations Peloton data that can be sensitive and personal. Unlike more traditional data sources, IoT devices can operate continuously and collect data passively, often transmitting it to cloud-based systems where users have limited visibility or control over how it is stored, shared, or sold. Additionally, the interconnected nature of IoT systems means data from multiple devices can be aggregated, creating more comprehensive and potentially invasive profiles of individuals, which raises significant privacy concerns, especially when third-party access is involved. Given the potentially personal and private nature of IoT ESI, numerous local, state, federal, and international privacy and data protection regulations may regulate its discoverability.[19]

Additionally, the varied storage locations of IoT ESI, whether on the IoT device itself, on domestic or international servers, or any combination thereof Peloton especially considering that large cloud storage providers may operate globally Peloton may raise cross-border data transfer issues.

Privacy concerns and regulations, though, do not necessarily act as an absolute barrier to discovery. Instead, they serve as aspects for evaluating and balancing privacy laws and concerns with discovery

---

[18] For a discussion of non-party discovery, please *see* The Sedona Conference, *Commentary on Rule 45 Subpoenas to Non-Parties, Second Edition*, 22 SEDONA CONF. J. 1 (2021).

[19] For example, General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), Children's Online Privacy Protection Rule (CPPA), and state privacy acts in California, Colorado, Connecticut, Utah, and Virginia.

obligations. Decisions limiting or denying discovery are not often based strictly upon privacy considerations, as the appropriate means of addressing privacy concerns about otherwise relevant and proportional documents is through a protective order.[20] In certain cases, additional protections used to address privacy concerns with other sensitive data, such as security measures, data minimization,[21] data summarization, and data anonymization, may be appropriate.[22]

IV. THE IOT RAISES UNIQUE ELECTRONIC DISCOVERY PROCESS ISSUES

In this section of the *Primer*, we move from electronic discovery practice to electronic discovery process, addressing various novel impacts of IoT devices and IoT ESI. Again, our focus will be on specific impacts of IoT, as opposed to a broader discussion of the electronic discovery process.

A. Identification of IoT ESI

An initial stage of electronic discovery is the identification of potential sources of data that may be relevant to the litigation. In addition to methods applicable to traditional ESI, such as custodial interviews, some additional IoT considerations could include:

- Inventory of network-connected devices: Conducting an inventory of all network-connected devices can help identify potential IoT devices that may be relevant for discovery.

- Review of IoT device manufacturer documentation: Reviewing device manufacturer documentation for IoT devices can help identify potential data sources (as well as the data's location and who possesses or controls it).

- Data mapping: Conducting a data mapping exercise can help identify where IoT data is being collected, stored, and processed within an organization's systems and processes.

- Review of third-party contracts: Reviewing third-party contracts can help identify potential data sources and clarify data ownership and control rights for IoT data.

- Shadow IT analysis: Conducting an analysis of shadow IT, or unauthorized devices or software being used within an organization, can help identify potential IoT devices that may be relevant for discovery.

---

20 *In re* Broiler Chicken Antitrust Litig., No. 1:16-cv-08637, 2017 WL 6569720, at *2 (N.D. Ill. Dec. 22, 2017) ("Plaintiffs already have agreed all phone records can be designated as confidential under the Agreed Confidentiality Order, which provides adequate protection by limiting the use and disclosure of confidential information to certain persons and for certain purposes.").

21 *See, e.g.*, Cory v. George Carden Int'l Circus, Inc., No. 4:13-CV-760, 2016 WL 3460781, at *3 (E.D. Tex. Feb. 5, 2016) (allowing the extraction of limited data but denying a full imagining of a device citing privacy concerns).

22 For additional information, please *see* The Sedona Conference, *Commentary on Proportionality in Cross-Border Discovery*, 25 SEDONA CONF. J. 669 (2024).

B. Preservation of IoT ESI

Preservation of potentially relevant data sources is a critical stage of the discovery process.[23]

Timing is crucial for preserving IoT ESI, as it may have short retention periods based on user needs or device functions. Some IoT devices capture real-time data at a high volume and velocity, which could result in shorter retention periods to prevent high storage costs. Rapid technological advancements can also render IoT data inaccessible before case resolutions. In the context of a reasonable and proportional discovery process, responding parties should consider potential needs to act quickly to preserve IoT ESI, including possible early data collection or periodic snapshots of relevant data to mitigate spoliation risks. Some examples of unique preservation challenges posed by the nature or environment of IoT devices include:

- **Difficulty in Identifying Relevant Data Sources**: In a case involving a smart building with numerous IoT devices such as HVAC systems, lighting controls, and security sensors, identifying which devices have relevant data can be challenging. Each device may generate logs and metadata but determining which specific data points are pertinent to the litigation requires significant effort and expertise. The sheer volume and diversity of devices can complicate the identification and preservation process.

- **Rapid Evolution and Obsolescence of Devices**: In a product liability case involving a wearable health device, the rapid pace of technological advancement can pose preservation challenges. If the device model in question is quickly replaced by newer versions, the data formats and storage methods may change, making it difficult to access and preserve data from older models. Additionally, manufacturers may discontinue support for older devices, further complicating data retrieval.

- **Complexity of Data Formats**: In environmental litigation involving IoT sensors monitoring air quality, the data may be stored in complex, proprietary formats. These formats might require specialized software or expertise to interpret, and converting the data into a usable format for litigation purposes can be time-consuming and costly. The complexity of the data formats can hinder the preservation process and increase the risk of data loss.

- **Potentially Fleeting Nature of IoT ESI**: In a personal injury case involving a fitness tracker, the data may be ephemeral, with the device only storing detailed logs for a brief period before overwriting them. If the data is not promptly synchronized to a cloud service or backed up, it can be lost. The transient nature of such data necessitates immediate action to preserve it, which may not always be feasible.

---

[23] For a full discussion of preservation, please *see* The Sedona Conference, *Commentary on Legal Holds*, *Second Edition: The Trigger & The Process*, 20 SEDONA CONF. J. 341 (2019).

- **Lack of Direct Control Over IoT Device ESI**: In a case involving a connected vehicle, the telematics data may be controlled by the vehicle manufacturer rather than the vehicle owner. The owner may not have direct access to the data and obtaining it may require cooperation from the manufacturer. This lack of direct control can complicate the preservation process and introduce delays or obstacles in securing the necessary data.

- **Environmental Factors Affecting Data Preservation**: In a maritime case involving IoT devices on a ship, environmental factors such as exposure to saltwater, extreme temperatures, and physical vibrations can affect the reliability and longevity of the devices. These harsh conditions can lead to data corruption or device failure, making it challenging to preserve relevant ESI.

These examples illustrate the unique preservation challenges posed by the nature or environment of IoT devices. Courts should consider these factors when determining whether a party took reasonable steps to preserve IoT ESI under Federal Rule of Civil Procedure 37(e).

Promptly identifying relevant IoT ESI and determining who has possession, custody, or control of the data can be essential to preservation. Preserving relevant IoT ESI may require a preservation letter to the party and a subpoena to a non-party. As an example, consider a homeowner's smart thermostat. While the physical device is in the homeowner's possession, data generated may be stored on the device, on the homeowner's phone and tablet, and in the cloud as managed by the thermostat manufacturer.

C. Collection of IoT ESI

Collection of ESI typically follows identification and preservation. It generally consists of targeting and moving ESI from its sources, possibly converting it into a format more usable in the discovery process, for future use as part of discovery processing, review, analysis, and production.

Sometimes, collecting IoT ESI is straightforward, using simple exporting features that are user accessible. Other times, however, IoT ESI can pose significant collection challenges, especially for IoT ESI that is not usually a target for discovery collection.

1. Location and Accessibility

IoT ESI may either be easily accessible to individual users or, conversely, highly proprietary and challenging to gather using traditional electronic discovery methods. Therefore, the method of IoT data collection can vary significantly based on the unique locations in which it is stored. For example, a physical smart thermostat stores local hardware configuration, display settings, and Wi-Fi connection data that is not available through the mobile application. Collection of this data, if required, likely involves specialized technical knowledge in the field of forensic collection to access the physical device's operating system and extract data from local memory storage. However, the end-user mobile application stores current temperature readings, pre-programmed schedules, preferred settings by room, and similar customized information specific to the assigned user's account and is

accessible with direct cooperation from the account owner. Once logged into these applications, the interface displays key data points, provides visual reporting (e.g., dashboards), and has raw data export options available in readable formats like Excel. The cloud server for the thermostat stores user account data, potentially serving as direct copy of the end-user mobile application information. It also can house unique data like historical temperature logs, user account activity logs, data transfer logs, and similar information that is useful to the software provider. It may be possible for the account owner to export or request access to all or part of this cloud data, but detailed application information would likely come directly from either the software provider who developed the application or the cloud service provider.

2. Content and Volume

The content of IoT systems varies. Some have well-regulated, uniform, fielded data, while others have unstructured hybrid content like voice and video recordings. Unstructured content can be labor intensive to collect and review. As with ESI generally, where IoT ESI volumes are large, consider sampling or limiting the time frame of the collection or search so the case team can review and validate the resulting data export(s). Sampling also presents an opportunity for the parties to learn about the data and collaborate on next steps.

3. Collection Documentation

As IoT ESI collections are completed, documenting the methodology used to perform the collection may assist in defending the collection approach and facilitate supplemental collections as necessary in the future. For example, consider documenting the specific data sources, the collection workflow, performing technician, any quality-control steps taken, and the date and time of the ESI acquisition. Additionally, reference information used to support the collection process, such as a data dictionary or IoT ESI data flow diagram, can be provided.

4. Expertise

Specialized technical resources and experts may be helpful in providing information on what search and collection capabilities are available across the IoT categories of ESI. Standard ESI search and retrieval methodologies may or may not be usable or applicable to IoT ESI. Device data may be easily exportable, or retrieval may require specialized applications. Not all vendors will have the ability to retrieve all IoT ESI. And, absent built-in search capabilities, data indices, or similar filtering functionality, the burden of identifying potentially relevant data within the raw data stores may increase.

D. Processing IoT ESI

The processing stage generally involves utilizing specialized electronic discovery software tools to convert collected ESI into a format to then be used with electronic discovery review software. However, due to its potentially unique, non-standard nature, traditional electronic discovery software may not be able to process IoT ESI as it can standard ESI such as email. Some IoT ESI may involve massive sets of large files, including audio and video files. Any processing and handling of such files

could potentially lead to significant time and cost expenditure. Parties may find it helpful, early in the electronic discovery process, to work with service providers and technology experts to optimize the collection process and then customize processing tools in an effort to reasonably and proportionally manage collection and processing of IoT ESI. Ongoing discussions between parties can be helpful here as part of a collaborative process that highlights and manages any potential complexities and costs relating to processing IoT ESI.

E. IoT ESI Analysis and Searching

In the Analysis and Searching stage, ESI is analyzed and searched to find information relevant to a matter. After collection and processing steps, some IoT ESI may then resemble traditional ESI, and be included in standard electronic discovery review tools for analysis and production. However, other IoT ESI may more closely resemble databases. In such situations, analysis may occur within a database environment, where the data is manipulated using scripts designed to retrieve, filter, sequence, and calculate information based on the specific needs of the case. Filtering involves selecting a subset of records based on internal or external criteria applied to focus on specific time frames, devices, or events captured within the IoT ESI. Sequencing refers to the ordering of records based on one or more fields, which can help in identifying patterns or trends over time. Calculating information for analysis may involve generating new values or content through the application of formulas across records and fields. This might include calculating averages, identifying outliers, or generating summary statistics that provide insights into the data. Highlighting patterns and aggregate data insights can be as crucial to a case as individual pieces of evidence. This shift underscores the importance of robust analytical tools and methodologies in handling the vast and complex datasets generated by IoT devices.[24]

F. Review and Production of IoT ESI

As noted above, IoT ESI at this stage may either resemble traditional ESI, database ESI, or potentially a combination thereof. Content and format play a crucial role in determining the best approach for reviewing IoT ESI. Exported content or format may be incompatible with traditional ESI review tools, making it necessary to consider alternative review methods. There will also be occasions where the relevance of the ESI is not limited to the ESI itself. These situations require the ESI plus proprietary transformations that may be affected by software, display, or context that build on the IoT ESI and may require additional considerations. For example, in a matter involving an accident in an electric car,[25] the court ordered the car maker to provide the plaintiff with a .csv file and additionally ordered access to a computer at which plaintiff could view, and take screenshots or pictures of relevant information through the car maker's proprietary software system.[26]

---

[24] For commentary on databases in electronic discovery, please *see* The Sedona Conference, *Database Principles: Addressing the Preservation and Production of Databases and Database Information in Civil Litigation*, 15 SEDONA CONF. J. 171(2014).

[25] McLaughlin v. Tesla, Inc., No. 22-cv-07849-SVK, 2023 WL 9285052 (N.D. Cal. Nov. 2, 2023).

[26] *Id.* (order requiring Tesla to provide plaintiff access to APViz tool to view Snapshot data).

For IoT ESI, the original format as maintained by the responding party may not always be practical or usable without deploying additional resources, highlighting the importance of early agreement between parties on collection efforts and the format of production.

Ultimately, planning early in the discovery process and defining clear parameters for IoT ESI production can help mitigate these challenges and ensure the data is manageable, reviewable, and usable in a litigation setting.

V. IOT ESI ADMISSIBILITY

As technology advances, IoT ESI use in criminal and civil litigation is becoming more prevalent, sophisticated, and impactful. For example, in a 2022 murder trial, data from a fitness tracker revealed the victim's movements, leading to the husband's conviction and a 65-year sentence.[27] In another case, prosecutors used Fitbit data to disprove a rape allegation.[28] Similarly, in wage and hour cases, product liability cases, wildfire cases, and even anti-trust cases, IOT information is being used to establish the chronology of events, the locations of devices (and actors), weather conditions, and more.[29] This section explores issues related to the admissibility of IoT ESI in civil and criminal cases, including authentication, hearsay, expert testimony, and forensic consultants.[30]

A. Authentication

The admissibility of IoT ESI in a given case, and the type of authenticating witnesses required, will vary depending on the complexity of the IoT system involved. In some cases, a single witness may be sufficient to authenticate both the existence of the IoT device and the ESI it generates, particularly if that ESI is readily accessible via consumer-level devices like smartphones or tablets. However, for more complex systems, testimony from a witness with technical expertise in those systems may be necessary to properly authenticate the data.[31]

The chain of custody for IoT ESI, or indeed most ESI, differs significantly from traditional physical evidence due to the unique nature of digital evidence. Unlike traditional evidence, where the chain of custody often involves human actors at every stage, IoT ESI originates from machines and its authenticity is often based on system logs, automatic processes, and data transmission records. While

---

27 Press Release, State of Connecticut, Division of Criminal Justice, *Richard Dabate Sentenced to 65 Years in Prison for the December 2015 Murder of His Wife, Connie Dabate* (May 21, 2024), https://portal.ct.gov/dcj/press-room/press-releases/08182022dabatesentencing.

28 Myles Snyder, *Police: Woman's fitness watch disproved rape report*, abc27.com (June 19, 2015), https://www.abc27.com/news/police-womans-fitness-watch-disproved-rape-report/.

29 Plaintiffs ordered to produce metadata and also identify personal devices. *See* Discovery Order, Maddy v. Gen. Elec. Co., No. 1:14-cv-00490 (D.N.J. July 22, 2016), ECF No. 262.

30 For a detailed discussion on ESI admissibility, please *see* The Sedona Conference, *Commentary on ESI Evidence & Admissibility, Second Edition*, 22 SEDONA CONF. J. 83 (2021).

31 Parties may come to an agreement that helps clear the path for IoT ESI admissibility.

traditional evidence requires a detailed, step-by-step handling record, IoT ESI offers an alternative approach through the use of cryptographic hashing (e.g., MD5, SHA-1, or SHA-256), which can verify that the ESI remains unchanged from its original content. Hashing can ensure data integrity without requiring a complete traditional chain of custody.

IoT authentication begins with proof of origin. Proof of origin ensures that the ESI is reliably traced back to its source. For IoT ESI, this can encompass both the real-world technology stack, including devices, sensors, and communication networks, as well as the specific methods used to collect, filter, transform, and produce the ESI for legal purposes. Because IoT systems often involve multiple layers of hardware and software, proof of origin becomes essential to demonstrate that the ESI came from the correct device and was transmitted through the proper channels without interference or undocumented alteration.

1. Authentication under Federal Rule of Evidence 901

As with any evidence, IoT ESI carries the risk of being corrupted or manipulated—whether after it is collected, while stored in the cloud, or during retrieval and processing. However, the mere potential for manipulation should not preclude *admissibility*. In the simplest scenario, the wearer, owner, or controller of the IoT device can testify to authenticate the ESI under Federal Rule of Evidence 901(b)(1), as a witness with personal knowledge. Federal Rule of Evidence 901 requires the proponent of evidence to "produce evidence sufficient to support a finding that the item is what the proponent claims it is."[32] This can be achieved using a non-exhaustive list of examples recited in Rule 901(b), which includes testimony of knowledgeable witnesses, distinctive characteristics, and comparisons made by expert witnesses.[33]

a. Knowledgeable fact witnesses

Authentication might require the procurement of witnesses knowledgeable about the IoT ESI, as well as its creation, processing, storage, and use. This may involve a party witness, or it may require subpoenas to an organization that processes, collects, and stores IoT ESI. The technical questions associated with authenticating and understanding IoT ESI are not necessarily issues that judges are familiar with, or accustomed to, and this may create additional hurdles for authentication that are not present with more typical documents such as emails or run-of-the-mill corporate records. Therefore, opposing counsel may not be willing to undertake stipulations as to authentication that may occur in the more typical case. It is prudent, therefore, for counsel to educate themselves on the creation, processing, storage, and use of the IoT ESI and to be prepared to educate the presiding judicial officer as to any case-specific technical intricacies that may arise.

---

32 FED. R. EVID. 901(a).

33 FED. R. EVID. 901(b)(1), (b)(3), (b)(4).

b. Distinctive characteristics

Aside from fact witnesses, it may be possible to authenticate IoT ESI based on the distinctive characteristics of the data. IoT ESI could have unique or distinct metadata (as confirmed by a witness), or it could be characterized by unique security features or fingerprints. Section III.B. of The Sedona Conference*, Commentary on ESI Evidence & Admissibility, Second Edition* has a thorough review of how concepts such as hashing, encryption, metadata, computer forensics, and blockchain can authenticate data generally and may assist in the authenticating IoT ESI. In all cases, the legal professional, with involvement of technical experts as needed, should understand the methods used to authenticate the IoT ESI, the substantive impact it has on the case, and potential drawbacks the authentication process may introduce. IoT ESI can be highly technical and require extensive explanations to demonstrate its weight in a matter; this process should be considered against the evidentiary and dispositive value of the IoT ESI in question.

c. Technology experts

Given the complexity of IoT ESI and how it is generated, distributed, retained, and stored, the sheer reliance of lay witnesses or distinctive characteristics may be insufficient for its authentication. The same expert who collects the IoT ESI can often serve as a witness to testify about its authenticity, providing a comprehensive solution for both the technical and legal aspects of IoT ESI handling. Over time, and with the help of experts, practitioners will better understand the nuances of IoT ESI, how and where it is stored on servers, and what signatures, metadata, or other unique attributes will be associated with such ESI. Technology experts who can authenticate a particular type of IoT ESI could provide additional insights into its evidentiary value, akin to how a handwriting expert is able to authenticate the veracity of an ink signature. These experts would have to testify on how the IoT ESI generates records through an electronic process or system that then produces an accurate result that can be accurately interpreted: that steps equal actual steps, that speed equals actual speed, and that time stamps represent when an activity started as opposed to when an activity stopped. Experts may specialize in specific IoT applications such as supply chains or connected cars. These areas involve complex systems producing large amounts of IoT ESI. For example, supply chains use IoT in manufacturing and transportation, while connected cars use various sensors for driving and automation. Expert knowledge in these fields is crucial for determining the authenticity and interpretation of IoT ESI as it relates to industry practices.

2. Self-authentication of IoT ESI under Federal Rule of Evidence 902(13)

Federal Rule of Evidence 902(13) states that "[a] record generated by an electronic process or system that produces an accurate result, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12)" is self-authenticating. This rule provides an opportunity to authenticate ESI "other than through the testimony of a foundation witness," as the comments to the rules confirm.[34] The purpose of the rule is to avoid the unnecessary expense of

[34] FED. R. EVID. 902 advisory committee's notes to 2000 amendment & 2017 amendment.

procuring foundation witnesses when parties are likely to stipulate to the authenticity of the evidence anyway.

In certain cases, IoT ESI may be authenticated without the need for live testimony. Experts can attest to various IoT ESI characteristics, confirm its chain of custody, and certify that the ESI is authentic—because it is generated by an electronic process that produces an accurate result. Indeed, the purpose of Rule 902(13) is to create a "procedure under which the parties can determine in advance of trial whether a real challenge to authenticity will be made, and can then plan accordingly."[35]

As recognized sources of IoT ESI become more mainstream, certifications may be accepted to authenticate IoT ESI as a matter of course, or certification authorities may adopt standardized procedures for providing certifications under Rule 902(13). Just as such procedures could obviate the need for authentication depositions or live testimony at trial, they might also render Federal Rule of Evidence 104(a) hearings unnecessary.

Despite the availability of self-authentication, practitioners should always be prepared to demonstrate the authenticity of IoT ESI (or any other potential evidence) if challenged. Authentication under federal and most state evidence rules is a prerequisite for admissibility of such evidence and, as the advisory committee's note points out, a party objecting to that evidence "remains free to object to admissibility of the proffered item on other grounds—including hearsay, relevance, or in criminal cases the right to confrontation."[36] Moreover, even if the evidence is admitted at the hearing or trial, that does not create a presumption of credibility for the finder of fact; it allows the finder of fact to consider that item and to weigh its credibility. To prepare, practitioners should retain a backup plan in case self-authenticated IoT ESI is questioned. Suggested resources include (1) trusted documentation to certify the IoT ESI, such as from the IoT device manufacturer, (2) experts prepared to testify as to the authenticity of the IoT ESI, (3) witness corroboration of the IoT ESI, or (4) triangulation with other data sources to corroborate the IoT ESI.

B. Potential IoT Hearsay Issues

Hearsay issues may arise in the context of IoT ESI. The fundamental question that must be asked is whether the IoT ESI is a "statement of a [human] declarant" —is it "a person's oral assertion, written assertion, or nonverbal conduct, if the person intended it as an assertion"?[37] Some IoT ESI may obviate the statement analysis, as it exclusively engages machine-based recordkeeping. For instance, biometric ESI recorded on an Apple Watch during a workout may not be statements at all. It could be reasonably argued that heart rate, pulse, steps taken, calories burned, and other such data recorded during a workout are not assertions by the person recording them, rather they are machine-based measurements reliably captured and stored as digital information. Conversely, a Ring or Nest

---

35 FED. R. EVID. 902 advisory committee's note to 2017 amendment.

36 *Id.* Recognize that some of these objections would not apply to structured data collected from electronic monitors and other devices.

37 FED. R. EVID. 801(a).

doorbell camera that records an event involving people talking to one another will likely involve statements intended as oral assertions and other nonverbal conduct, thus requiring additional legal analysis under Federal Rules of Evidence 801, 802, and 803. IoT ESI will need to be analyzed on a case-by-case basis to determine the hearsay implications.

IoT ESI can also be hybrid. The steps recorded on an Apple Watch may be presumptively considered to be steps. But it may have been the user (or an algorithm) that chose to record activity as an "Outdoor Walk" —which does not mean that it was an Outdoor Walk.

Analyzing IoT ESI for hearsay requires a precise identification of how the IoT ESI in question was collected, stored, processed, and used as evidence. IoT devices are listening devices (sensing inputs) and actuating devices (responding with outputs). Amazon's Alexa hears information, stores the audio, and sends actuating information to other resources in the IoT universe. Other resources (devices or software) detect movement, temperature, and other measurements. All this information can then be processed, and the output can be considered another type of IoT ESI and offered as evidence in criminal or civil litigation, just as someone who overhears a conversation might testify about an overheard conversation at trial. There will be legitimate questions about whether such overheard information is sufficiently reliable to overcome hearsay or other evidentiary objections. Evidentiary tools such as the business-records exception might be used to overcome these objections. But this may in turn require further inquiry into whether non-parties maintain such data in the ordinary course of business, what their procedures are for maintaining and collecting such data and whether a party opposing the admission of IoT ESI asserts that the source of IoT ESI sought to be admitted under that exception, or the method or circumstances of preparation, indicate a lack of trustworthiness under Federal Rule of Evidence 803(6)(E).

VI. CONCLUSION

As IoT devices continue to proliferate, generating vast amounts of data across various contexts, legal professionals must adapt to the unique challenges and opportunities presented by IoT ESI.

It is essential to understand the unique characteristics of IoT ESI, including its volume, variety, and velocity. This *Primer* discusses the implications of the IoT and various techniques for addressing its impact. These include early and collaborative discovery planning, incorporating technical expertise, and focusing on flexible and proportional approaches. By examining and understanding the complexities and challenges introduced by IoT to traditional law and process considerations, judges, practitioners, and parties will be better equipped to manage the implications of the IoT on electronic discovery.