

September 2024 Draft: The Sedona Conference Primer on the eDiscovery Implications of the Internet of Things (IoT)

Drafting Team Members

Mikaela Bock	Kevin Clark
David Gaston	Warren Kruse
Sara Lockman	Kyle Pozan
Dan Regard	Christopher Suarez
Hon. Juan Villaseñor	Sean Zacharias

Team Leaders

Greg Kohn	Josh Zylbershlag
-----------	------------------

Steering Committee Liaisons

Lea Bays	Ross Gotler
Claire Hass	Laura Hunt

Copyright 2024. All rights reserved.



This working draft document was created for discussion purposes only for the 2024 Annual Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to

comments@sedonaconference.org

**The Sedona Conference Primer on the eDiscovery Implications
of the Internet of Things (IoT)
September 2024 Draft**

TABLE OF CONTENTS

I.	Introduction.....	3
II.	Categories of IoT ESI.....	3
A.	ESI generated by IoT devices.....	4
B.	Communication devices used to remotely activate or control the IoT device (“User Activation Devices”).....	4
C.	Web-based Management Platforms (WMPs) for IoT devices.....	4
D.	Local and cloud storage repositories of IoT ESI	5
E.	Downstream locations of IoT ESI.....	5
III.	The Impact of IoT ESI on Key Discovery Practice Topics	5
A.	Initial disclosures; Rule 26(f) meet-and-confer.....	5
B.	Scope of discovery and proportionality	7
C.	Limitations on discovery	8
D.	Possession, custody, and control	9
1.	Who is the owner of the IoT ESI?.....	9
2.	Considerations for determination of possession, custody, or control.....	10
E.	Non-party discovery	11
F.	Privacy.....	11
1.	The Impact of data privacy and protection laws.....	12
2.	Potential solutions	12
IV.	The Impact of IoT ESI on the eDiscovery Process	13
A.	Identification of IoT ESI	13
B.	Preservation of IoT ESI.....	14
1.	Preservation obligation considerations.....	14
2.	The preservation process.....	15
C.	Collection of IoT ESI.....	15
1.	Accessibility and format.....	17
2.	Physical collection of IoT devices and user activation devices.....	18
3.	Downstream ancillary systems.....	18
4.	Collection, search, and export best practices.....	18
D.	Processing IoT ESI.....	20
1.	Extraction methodology	20

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to

comments@sedonaconference.org

2.	Loading into destination systems	20
3.	Transformation and storage	20
4.	Quality Control during transfer	21
E.	Analysis and searching of IoT ESI	21
1.	Filtering	21
2.	Sequencing	21
3.	Calculating	21
F.	Review and production of IoT ESI	22
V.	The Impact of the IoT on Admissibility of ESI	23
A.	Introduction	23
B.	Chain of Custody for IoT ESI	24
C.	Proof of Origin	24
D.	Proof of Reliability	24
E.	Importance in Litigation	24
F.	IoT ESI authentication techniques and hurdles	25
1.	Authentication under Federal Rules of Evidence, Rule 901	25
2.	Self-authentication of IoT ESI under Federal Rule of Evidence 902(13)	26
3.	Potential IoT hearsay issues	27
4.	Daubert/Frye applicability and experts	28
5.	Forensic acquisitions and consulting	28

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to comments@sedonaconference.org

I. Introduction

In the digital age, the Internet of Things, or IoT, has emerged as a transformative force, knitting together billions of devices in a vast web of connectivity that continuously generate, communicate, and store data. This revolution has ushered in a new frontier in the legal landscape, especially in the realm of electronically stored information (“ESI”) derived from IoT devices (“IoT ESI”). Whether it’s data from a fitness wearable providing crucial evidence in a criminal investigation or home security systems like Nest and Blink capturing events in unprecedented detail, the integration of IoT ESI in legal proceedings is inevitable. However, as with any profound technological shift, this integration is not without its complexities. As IoT ESI introduces sources of evidence, it also introduces new challenges to the eDiscovery process.

This *Primer* explores eDiscovery implications of IoT ESI, including issues relating to data integrity, evidence authentication, preservation, and production—all parts of the intricate interplay of technology and law.

II. Categories of IoT ESI

The term Internet of Things refers to a broad array of electronics like smart home devices, wearables, connected electric vehicles, point-of-sale devices, Wi-Fi network hardware, traffic sensors, and other devices connected to the internet that generate, collect, store, and/or share information.¹ It has been defined as “being a system of interrelated computing devices, mechanical and digital machines or objects that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. These devices are not limited to a particular type of data storage medium or format.”² Basically, any modern, special-purpose device that connects to the internet likely falls under the umbrella of IoT. Traditional computers and smartphones are not considered IoT devices because they are general-purpose devices that are made for human-to-human or human-to-computer communications, although they may have components that increasingly behave like IoT devices.

To better understand the eDiscovery challenges associated with IoT ESI, it is crucial to recognize the various categories of IoT data likely to be relevant in litigation. The legal implications of IoT ESI, including licensing, privacy, access, and control, can vary significantly depending on where the data is stored, the format in which it is stored, and how it is accessed and collected. Legal professionals who can distinguish between these categories and account for these factors are better equipped to navigate the eDiscovery process, ensure regulatory compliance, and address the legal challenges posed by IoT data. Failing to account for these complexities could lead to missed evidence, compliance failures, or legal disputes.

¹ *The Sedona Conference Glossary: eDiscovery and Digital Information Management, Fifth Edition*, 21 SEDONA CONF. J. 263 (2020).

² SWGDE Technical Notes on Internet of Things (IoT) Devices Version: 1.0 (September 17, 2020)

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to comments@sedonaconference.org

A. ESI generated by IoT devices

IoT devices generate ESI, but the amount varies by device.³ Examples of consumer IoT data include video recorded by a smart doorbell or workout metrics captured by a wearable fitness device. For commercial IoT data, examples include telemetry from a pacemaker sent to a doctor, or location and driving telemetry from a vehicle sent to a logistics management system.

Examples of ESI intended for technicians or engineers engaged in troubleshooting or performance assessment include acceleration data from a smart car or fault-tolerance logs maintained by assembly robot in a car factory.

B. Communication devices used to remotely activate or control the IoT device (“User Activation Devices”)

Many IoT devices are designed to be accessed, controlled, or operated through interaction with another device. These “User Activation Devices” are among the most common types of IoT devices, particularly those used by the general public. Examples include a wide range of home automation devices that are controlled via applications installed on multipurpose devices such as computers, smartphones, tablets, and wearables. These include TVs, lighting systems, HVAC controls, home appliances, vacuums, door locks, garage door openers, lawn sprinklers, and more. Some IoT devices are exclusively controlled by another device; for instance, Apple’s AirTag lacks physical buttons and is configured and operated solely through an iPhone, iPad, or Mac. Other devices can function independently, but pairing them with a smartphone or tablet unlocks data and functionality that cannot be accessed directly. For example, modern thermostats can connect to smartphones, enabling users to view energy consumption and usage data that is unavailable directly from the thermostat.

User Activation Devices may grant access to ESI stored on the IoT device, provide dashboards that summarize or analyze IoT data, or capture and store ESI originating from the IoT device. For instance, a home weight scale may transmit daily weight data to a health management app on a smartphone, while a robotic vacuum could send usage and maintenance details to the user, along with room layout and diagnostics data to the manufacturer.

C. Web-based Management Platforms for IoT devices

Web-based management platforms (WMPs) often serve as repositories for ESI generated by one or more IoT devices. For example, a factory supervisor can utilize a web interface to monitor and control the performance of multiple robots on the production floor. Similarly, a consumer can log into their router’s web portal to review and manage settings for devices connected to their home Wi-Fi network. WMPs frequently aggregate and summarize large volumes of data from various IoT

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. [cite report - Worldwide Global DataSphere IoT Device and Data Forecast, 2019-2023]

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to comments@sedonaconference.org

devices, offering users valuable insights through trend analysis or by highlighting deviations from expected norms.

D. Local and cloud storage repositories of IoT ESI

The ESI generated by IoT devices is often collected and stored in cloud or local storage repositories. For example, an Apple Watch, which now typically offers 32GB of storage, may hold both user-placed data (such as music, notes, and photos) as well as information generated during the device's normal operations. However, much of this data is also synchronized with the user's iCloud account, where historical information from the device can be stored for years. Similarly, users of Amazon's Alexa smart speakers can access their Amazon cloud account to find and delete audio recordings created whenever the Alexa voice assistant was activated, whether intentionally or inadvertently.

E. Downstream locations of IoT ESI

A significant portion of the success and utility of IoT devices stems from their capacity to collect data and integrate it with other devices, networks, and platforms. As a result, third-party applications, system integrations, and external repositories often receive and store IoT ESI. For instance, fitness trackers not only provide users with personal health and workout data but also connect to wellness platforms managed by insurance companies, which may offer premium discounts based on the user's activity levels. These downstream repositories can house ESI from millions of devices, with varying degrees of anonymization and accessibility.

III. The Impact of IoT ESI on Key Discovery Practice Topics

The Federal Rules of Civil Procedure (FRCP) and the Federal Rules of Evidence (FRE) expressly address the discovery and admissibility of electronically stored information (ESI), and data from IoT devices is generally considered discoverable. While IoT ESI presents unique challenges compared to traditional forms of ESI, many of the underlying principles remain the same. The type of IoT device, and what data can be retrieved or may be impossible to obtain, will vary significantly. Legal practitioners should carefully assess how the presence of IoT ESI will affect the overall discovery process.

A. Initial disclosures; Rule 26(f) conferences

IoT devices, and the data they generate, are playing an increasingly integral role in daily life and will continue to do so. These devices collect vast amounts of data, much of which may become relevant in legal disputes and investigations. As a result, the discovery process faces new challenges and opportunities with respect to IoT ESI. Discussions surrounding the preservation, collection, review, and production of IoT ESI are becoming more complex. Accordingly, when IoT data falls within the scope of discovery, parties should address related issues early and proactively as part of their discovery plans and ESI protocols, consistent with requirements such as those in FRCP 26(f).

Data obtained from IoT devices is often unstructured and can be too large to produce in its entirety. Engaging technical and business experts early on to address key questions is essential for

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to comments@sedonaconference.org

effectively navigating Rule 26(f) conferences and meet-and-confer discussions. These experts can help develop a practical, proportional approach to IoT ESI discovery. For example, in some instances, the responding party may need to educate the requesting party on specific IoT data sources, available collection methods, and any associated challenges—such as time, cost, volume, or control over the data—that may complicate or delay the discovery process. Efforts like these, combined with input from the requesting party on their need for the IoT ESI and how they intend to use it, can facilitate negotiations over the scope of discovery and streamline the process of reaching an agreement.

Notably, this approach aligns with the Sedona Conference Database Principles, which similarly advocate for practical, proportionate strategies to handle complex data sources during discovery.⁴

Rule 26(a)(1)(A)(ii) imposes a duty on parties to disclose sources of ESI, including IoT ESI, that they may use to support their own claims or defenses. But practitioners should keep in mind that Rule 26(a) does not impose any obligations to disclose information or documents to support an adverse party's claims or defenses. Therefore, practitioners should take proactive steps to educate themselves on the adverse party's IoT infrastructure through additional discovery methods. This can begin during the Rule 26(f) conference, where the parties are required to address “any issues about disclosure, discovery, or preservation of electronically stored information, including the form or forms in which it should be produced.”⁵ Such issues should then, if appropriate, be included the case management order or scheduling order.

The term IoT encompasses a wide range of technologies, and the types of ESI implicated in litigation can vary significantly based on how the technology was designed, how it functions, and how it interacts with other systems. Drawing on relevant Sedona Conference publications and established best practices, parties should consider key concerns related to meet-and-confer discussions at the earliest possible stage to determine (and agree upon) the appropriate scope of discovery under Rules 26(b) and 26(f). During the Rule 26(f) conference and subsequent meet-and-confer sessions, parties should make informed, good-faith efforts to reach initial agreements on how to approach IoT ESI discovery, taking into account the unique challenges posed by these devices, as outlined in this *Primer*.

Effective planning and preparation are essential to conducting successful meet-and-confer activities regarding IoT ESI. In certain cases, engaging technical experts familiar with the specific IoT ecosystems at issue, along with the business owners who rely on the data for their operations, may prove beneficial. As part of these discussions, understanding how the requesting party intends to use IoT data can aid in evaluating the burden versus benefit aspects of proportionality considerations. By way of example, see *The Sedona Conference Database Principles* (2014 Edition), Comment 6.A.:

⁴ The Sedona Conference, *Database Principles: Addressing the Preservation and Production of Databases and Database Information on Civil Litigation*, 15 SEDONA CONF. J. 171 (2014).

⁵ FED. R. CIV. P. 26(f)(2)

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to

comments@sedonaconference.org

Comment 6.A. Discussing the Intended Reasonable and Legitimate Uses of Database Information Can Result in a More Useful Production Format

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.

B. Scope of discovery and proportionality

Once parties have identified the relevant sources of IoT ESI, they should collaboratively evaluate the associated benefits and burdens of each source. This second stage often includes the following key considerations:

- What triggers the entry (or creation) of data? Is it initiated by human action, or does it result from an automatic event or threshold?
- How is the data entered? Is it generated directly by the device, or is it manually input by a human?
- What type of data is being collected?
- Is the data structured (e.g., predefined values or pick lists), or unstructured (e.g., free-form text, or video, or audio)?⁶

Requesting and producing parties determining the proportionality of IoT ESI should also consider:

- **Reliability.** When considering proportionality, the more reliable the data, the greater the value of the data.

IoT data varies in reliability depending on the development of technology, the underlying data that is sought, and its intended use in litigation. A request

⁶ Until now, it has been assumed that free-form text would come from human input. However, with the advent of Generative A.I., we now see free-form text being generated algorithmically, such as automated summaries of video-conference calls.

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to comments@sedonaconference.org

for relevant and highly reliable data is more likely to overcome a burden objection than a request for data that is unreliable.⁷

- **Readability.** IoT data can be structured with standard and uniform formats and content. This lends itself to grouping and analysis much more so than unstructured content gathered from more traditional sources.
- **Compound Value.** In addition to the richness and granularity of any individual data source, when IoT data sources are combined, then the value can be magnified. This is because two different sources can complement each other, allowing better understanding of the overall data picture where different sources partially overlap, and better continuity where one set has a gap. For example, IoT ESI from internet-connected motor vehicles, smart home devices, and wearables can be combined to determine an individual's consolidated location and activity level.

C. Limitations on discovery

Depending on the category of IoT ESI at issue, accessibility may vary. And as understanding, tools, and techniques improve for IoT ESI, parties can expect shifts in the calculation of what constitutes undue burden or cost with respect to the accessibility of IoT ESI.⁸

IoT ESI may also raise privacy concerns—and in some cases may even violate privacy regulations. However, this does not act as an absolute barrier to discovery; instead, serving as guidelines for evaluating data discoverability along a spectrum. In certain cases, it may also impose additional requirements, such as considering alternative approaches to meet privacy obligations, rather than acting as outright prohibitions on access to the data.

This approach enables parties to balance the competing interests of accessibility, privacy, and the need for relevant evidence within the context of Rule 26(b)(2)(B): not reasonably accessible.

⁷ See *In re 3M Combat Arms Earplug Prods. Liab. Litig.*, 2023 WL 4448917 at *5-6 (N.D. Fla. Sept. 23, 2022) (holding, in a case alleging hearing loss due to defective earplugs, the burden of collecting hearing and hearing health data with questionable reliability from the plaintiffs' smartphones outweighed any usefulness of the data itself because "the difference between hearing data registered while using Apple earplugs and for example hearing data registered while the device was connected to speakers outside at a family gathering or other event are situations that are worlds apart," and doubting "that any hearing expert would associate hearing loss with sound levels from a speaker where the user is not in close proximity to the connected device.").

⁸ *Garner v. Amazon.com, Inc.*, 2022 WL 4753013 at *2 (W.D. Wash. October 3, 2022) (plaintiffs whose at-issue data was in the control of non-parties were not compelled to produce it).

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to comments@sedonaconference.org

For guidance on this topic, please see Sedona Principle 8 and commentary from *The Sedona Principles, Third Edition*.⁹

“The primary sources of electronically stored information to be preserved and produced should be those readily accessible in the ordinary course. Only when electronically stored information is not available through such primary sources should parties move down a continuum of less accessible sources until the information requested to be preserved or produced is no longer proportional.”

D. Possession, custody, or control

FRCP Rule 34 allows parties to serve on other parties a request for documents within their “possession, custody, or control.” While this topic is discussed at length in *The Sedona Conference Commentary on Rule 34 and Rule 45 “Possession, Custody, or Control”*¹⁰ and *The Sedona Conference Commentary on Rule 45 Subpoenas to Non-Parties, Second Edition*,¹¹ IoT ESI presents some distinct considerations.

1. Who is the owner of the IoT ESI?

Determining the “owner” of IoT ESI for purposes of determining possession, custody, or control may present challenges and often depends on the specific IoT ESI requested and the circumstances surrounding its creation and storage.¹² While similar challenges apply with other forms of ESI, they may be amplified by the interconnected multilayered nature of IoT devices. For example, the “owner” may often be a combination of a user and a service provider.

Take, for instance, a Peloton exercise bike. The “owner” of the ESI may be a combination of the user (the individual who purchased the bike, or the account of one specific user) and the service provider (e.g., Peloton). It may be important to consider the original intent behind the collection of relevant data from an IoT device when determining ownership. IoT service providers may collect user activity data for business or marketing purposes that is not apparent to the individual who uses the bike for exercise purposes. Thus, where available, relevant service terms and conditions, often available in online user manuals, privacy consent notices, or account registration agreements, may be helpful to inform custody and control analysis.

Additionally, determining how, where, and when relevant data was created, copied, transmitted, or received can help inform possession, custody, or control. For example, data may be generated by the User Activation Device, Web-based Management Platform, the IoT device, or

⁹ *The Sedona Principles, Third Edition, Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, 19 SEDONA CONF. J. 1 (2028). Additionally, see *The Sedona Conference, Commentary on Preservation, Management and Identification of Sources of Information that are Not Reasonably Accessible*, 10 SEDONA CONF. J. 281 (2009).

¹⁰ *The Sedona Conference, Commentary on Rule 34 and Rule 45 “Possession, Custody, or Control,”* 25 SEDONA CONF. J. 1 (2024).

¹¹ *The Sedona Conference, Commentary on Rule 45 Subpoenas to Non-Parties, Second Edition*, 22 SEDONA CONF. J. 1 (2021).

¹² By instantiation, we mean the IoT ESI first generated by the program creating it.

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to comments@sedonaconference.org

some combination thereof. In the example of IoT data from a Peloton exercise bike, the IoT ESI may be generated by an application on the user's smartphone, the user's smartwatch, the Peloton exercise bike itself, or some combination of all three. This may help identify potential points of access that exist and determine the parties that have actual or practical control over the data generated at any point throughout the IoT ecosystem.

2. Considerations for determination of possession, custody, or control

The rapid proliferation of IoT ESI sources, including distributed or cloud computing platforms, SaaS, PaaS, IaaS and AaaS tools,¹³ mobile data platforms, wearable devices, smart home devices, and industrial and infrastructure sensors, presents challenges in determining possession, custody, or control. Each case requires a specific evaluation based on the nature of the requested ESI and the accessibility of that data to a producing party. In the case 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.
- Local privacy laws that may provide avenues for end users or corporations to request copies of ESI generated by an IoT device or system.
- Individual privacy consent preferences whereby an end-user can “opt in” or “opt out” of specific data collection, usage, and sharing preferences. This could determine whether sought-after IoT data was even captured or retained at all.
- The storage location(s) of the data—whether on the IoT device itself, on domestic or international servers, or any combination thereof—especially considering that large cloud storage providers may operate globally, raising cross-border discovery and data transfer issues.¹⁴
- 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.
- The intended or policy-based function(s) of the IoT device or the IoT ESI it creates within the ordinary course of business and its interplay with Rule 34.

¹³ Software-as-a-Service, Platform-as-a-Service, Infrastructure-as-a-Service, and Application-as-a-Service.

¹⁴ See *The Sedona Conference Framework for Analysis of Cross-Border Discovery Conflicts: A Practical Guide to Navigating the Competing Currents of International Data Privacy & e-Discovery*, available at [https://thesedonaconference.org/publication/Framework for Analysis of Cross-Border Discovery Conflicts](https://thesedonaconference.org/publication/Framework%20for%20Analysis%20of%20Cross-Border%20Discovery%20Conflicts).

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to comments@sedonaconference.org

- Any monitoring or logging resources that aggregate or process IoT device data.
- Backup or duplicate resources that store data created by the IoT device.

These factors are applicable to any IoT ESI category and will play an important role in a party's determination to produce or, alternatively, in a court's determination whether to grant a motion to compel or protective order. The significance of these factors will depend on whether the court applies the legal-right test or the practical-ability test in determining possession, custody, or control.

E. Non-party discovery

Production is always preceded by preservation. Parties have an affirmative duty (the scope of which is determined by matter-specific circumstances) to preserve IoT data triggered by a reasonable anticipation of litigation, litigation hold, or government investigation. In the case of IoT ESI preservation, time is of the essence. IoT devices can capture real-time data at a high volume and velocity, which could result in shorter retention periods to prevent high storage costs. Thus, promptly ascertaining what IoT ESI will be relevant to any claims and defenses at issue and determining who has possession, custody, or control of that data is critical to prevent potential loss of relevant ESI. For example, if a requesting party needs to determine, in a personal injury case, whether a Peloton bike was used on a certain date, the requesting party should promptly issue a preservation letter to the producing party. Additionally, if the requesting party's due diligence reveals the responding party may not possess all the IoT data and it therefore also needs to obtain data from Peloton itself, the requesting party should serve Peloton with a subpoena as soon as is practicable. And if a user's Peloton is linked to a personal fitness tracker (e.g., a Fitbit), both devices may contain relevant ESI, and both companies may need to be notified of their preservation duties. As mentioned above, non-party considerations in the discovery process are covered in detail in *The Sedona Conference Commentary on Rule 45 Subpoenas to Non-Parties, Second Edition*.¹⁵

F. Privacy

IoT data is more likely to raise personal privacy concerns because these devices often collect highly detailed, real-time information about individuals' activities, behaviors, and even physical conditions without their constant awareness. For example, fitness trackers monitor health metrics, smart home devices track daily routines, and smart speakers may record conversations—data that can be sensitive and personal in nature. Unlike traditional digital data sources, IoT devices operate continuously and collect data passively, often transmitting it to cloud-based systems where users have limited visibility or control over how it's 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. These privacy risks are compounded by varying levels of user consent and the potential for data breaches or misuse.

¹⁵ The Sedona Conference, *Commentary on Rule 45 Subpoenas to Non-Parties, Second Edition*, 22 SEDONA CONF. J. 1 (2021).

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to comments@sedonaconference.org

1. The Impact of data privacy and protection laws

Considering the potentially personal and private nature of IoT ESI, numerous local, state, federal, and international privacy and data protection regulations may regulate its discoverability. Some of the more significant ones are listed here:

- The EU General Data Protection Regulation (GDPR), which governs the processing of personal data.
- Health Insurance Portability and Accountability Act (HIPAA), which establishes standards for the protection of certain health information.
- Children’s Online Privacy Protection Rule (COPPA), which imposes certain requirements on operators of websites or online services directed to children under 13 years of age.
- U.S. state privacy acts such as those in California, Colorado, Virginia, Connecticut, Utah, Virginia, and more.¹⁶

Outside of specific laws and regulations, the rise of nonstatutory privacy considerations generally has led to efforts to impose limits on or deny discovery on claims of privacy, typically as to individual phone records, cell phones, email, or social media accounts. Most often, decisions limiting or denying discovery are based on relevance or proportionality, not strictly privacy considerations, as the appropriate means of addressing privacy concerns about otherwise relevant and proportional documents is through a protective order that limits disclosure of potentially sensitive materials.¹⁷

2. Potential solutions

IoT ESI may include information that directly or indirectly informs on extremely personal information, including health, religion, sex, finances, politics, race, and more. Some common solutions for addressing privacy concerns are as follows:

- Protective orders: These can protect access and control who can work with data productions. Typically, this also provides parties with the conditions and methods of asserting stronger controls over portions of the data.

¹⁶ See *Bartis v. Biomet, Inc.*, 2021 WL 2092785 (E.D. Mo. May 24, 2021) (allowing for the redaction of certain biometric data citing privacy concerns).

¹⁷ *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.”).

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to comments@sedonaconference.org

- Filing under seal: Like any case without IoT data, filing under seal can provide additional protections but needs to be weighed against the public interest of having a transparent legal system.
- Data minimization: The principle of only collecting and producing the minimum necessary to address the issues. This approach anticipates limits on data fields, custodians, and dates and/or time frames.¹⁸
- Data anonymization: Individual values, such as names, credit card numbers, social security numbers, or birthdays, can be removed so that data cannot be attributable to an individual. This substitution can be permanent (true anonymization) or reversible (pseudo-anonymization).
- Data encryption: Data encryption on a field level is comparable to pseudo-anonymization—it is illegible for now but can be reversed. Data encryption can also be applied at the file level so that all is encrypted (or unencrypted) for transfer and transport purposes. Some databases can also provide for “encryption-at-rest.”¹⁹
- Redaction: IoT ESI is typically produced as structured data files. Just like documents, structured data can be redacted. This usually means individual records having individual field values replaced with redaction text, or redaction designated values.²⁰

IV. The Impact of IoT ESI on the eDiscovery Process

A. Identification of IoT ESI

The first stage of an IoT ESI inquiry should be to identify all potential sources of data that may be relevant to the litigation. All potential sources should be identified first, with any limitations to be considered second.

There are several methods for determining the full range of devices and data source candidates. In addition to methods applicable to traditional ESI, such as custodial interviews and observations, some additional IoT considerations could include:

¹⁸ See, e.g., *Cory v. George Carden Int’l. Circus, Inc.*, 2016 WL 3460781 at *3 (E.D. Tex. Feb. 5, 2016) (allowing the extraction of limited data but denying a full imaging of a device citing privacy concerns).

¹⁹ Encryption at rest is encryption that is used to help protect data that is stored on a disk (including solid-state drives) or backup media.

²⁰ See *Bartis v. Biomet, Inc.*, 2021 WL 2092785 at *3 (E.D. Mo. May 24, 2021) (allowing for the redaction of certain biometric data citing privacy concerns).

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to comments@sedonaconference.org

- 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.

B. Preservation of IoT ESI

1. Preservation obligation considerations

The ubiquity of IoT data, as described throughout this paper, adds complexity to a party's obligation to preserve ESI. It is important to define clear parameters for preservation efforts, which, to mitigate the burden or the potential expense of overpreservation, should be driven by reasonableness and proportionality. Possession, custody, or control considerations play a major role in preservation decisions as well and are discussed in more detail in Section III.D.

Preservation considerations for IoT ESI can be illustrated using a "smart" thermostat as an example. A homeowner may own and install a smart thermostat. While that physical device is considered to be in the homeowner's possession, some data generated by the thermostat may be recorded locally on the physical device, and some may be stored in a structured database in multiple geographic locations, or in the cloud. Therefore, preserving the thermostat's IoT ESI may require the service of several Rule 45 subpoenas to non-parties in addition to a preservation letter to the party who owns the thermostat.

The thermostat example demonstrates how preservation can present challenges for IoT data. The questions of who has possession, custody, or control of the IoT ESI, and who has an obligation to preserve IoT ESI, will vary by device and may include more than the producing party. The potential number of entities involved in utilizing, manufacturing, and operating IoT ecosystems, as well as hosting the IoT data, presents challenges that further underscore the need for early attention to these issues in litigation.

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to comments@sedonaconference.org

2. The preservation process

Once a preservation obligation has been determined to exist, there are key avenues of inquiry that will provide helpful context for making preservation decisions effectively.²¹ Preservation obligations uniquely applicable to ESI are discussed below.

IoT ESI is not inherently ephemeral (digitally fleeting), but it can be functionally ephemeral or may only persist per the needs of the user, the function of the device, or the relevant records management policy. IoT data may also be ephemeral as to a device or location, with the primary retention of the ESI maintained elsewhere, such as a cloud-repository maintained by the vendor. Similarly, IoT ESI may become inaccessible over time due to the dynamic nature of the ecosystem's components or changes in IoT technologies over time, which could evolve at a pace much faster than the resolution of a case.

In these instances, responding parties may be well-served to determine when and where potentially relevant IoT data categories were deleted during the normal course of business prior to a preservation trigger and to document those historical processes. They may also want to consider means of early collection or otherwise conduct periodic “snapshots” of potentially relevant data categories to mitigate spoliation risk where present or future IoT ESI could be relevant.

Consideration thus needs to be given to the burden of preservation. The burden may increase if the data is stored in proprietary or encrypted formats that require substantial time and cost to collect. Whether the burden is proportional to the need depends on the case, and any challenges to preservation presented by default parameters, data formats, or the ephemeral nature of the data should be addressed during the Rule 26(f) conference.

C. Collection of IoT ESI

To the extent IoT ESI is relevant, proportional, and not privileged, it is within the scope of discovery under the Federal Rules of Civil Procedure. After the sources of IoT ESI have been identified and requested, they must be collected. Sometimes, collecting IoT ESI is straightforward, using simple exporting features that are user accessible. Other times, however, IoT ESI can pose collection challenges that should be considered when determining scope and proportionality. Some factors to consider when collecting IoT ESI include:

- **Mixed content:** 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 and may not be proportional to the needs of the case.
- **Third-party control:** Even if one of the litigants “owns” the device, the data from the device is often not retained on the device, but instead is

²¹ 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) and The Sedona Conference, *Commentary on Preservation, Management and Identification of Sources of Information that are Not Reasonably Accessible*, 10 SEDONA CONF. J. 281 (2009).

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to

comments@sedonaconference.org

immediately transferred to a cloud-based system. Once there, it may be under the custody and control of the vendor or system provider and not easily accessible to the producing party. The producing party's ability to directly access requested data can be determinative of its ultimate production.²²

- Data privacy concerns: Privacy interests, and the burden of complying with various privacy regulations (including, for example, the EU's General Data Protection Regulation) should be considered when determining privacy issues of IoT ESI in a particular case.²³
- Data Collection and Imaging: IoT ESI may either be easily accessible to individual users or, conversely, highly proprietary and challenging to gather using traditional eDiscovery methods. Therefore, the method of IoT data collection can vary significantly based on the relevance of the data and the unique locations in which it is stored. To illustrate the potential complexity of data storage locations, we can revisit our theoretical "smart" IoT thermostat ecosystem collection:

The 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 requires specialized technical knowledge in the field of forensic collection to access the physical device's operating system and extract data from local memory storage.

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. Alternatively, counsel can work with the user to take screenshots of how the data is displayed within the application, versus

²² See, e.g., *Garner v. Amazon.com, Inc.*, 2022 WL 4753013 (W.D. Wash. October 3, 2022). If a party is unable to access requested data, it can subpoena non-parties to preserve or produce it. In *Tracey v. Fabian*, No. 3:22-CV-189, 2024 WL 665926, at *13 (W.D. Pa. Feb. 16, 2024), the producing party was unable to obtain Ring camera footage from his own account and offered to serve a subpoena on Ring LLC to obtain it. In *McBryde-O'Neal v. Polichetti*, No. 23-CV-10113 (JPC) (RFT), 2024 WL 195571, at *2 (S.D.N.Y. Jan. 17, 2024), the court found good cause to issue a preservation subpoena of Ring Camera footage because Ring LLC, by its own policies, would typically delete any stored camera footage within 60 days, permanently eliminating material evidence. Similarly, in *Akimoto v. Apple Inc.*, No. 22-MC-80056-DMR, 2022 WL 1157496, at *4 (N.D. Cal. Apr. 19, 2022), the court ruled Apple could be subpoenaed to produce IoT ESI regarding location data and operational details of the Health app on defendant's iPhone to support his defense in an ongoing appeal of his foreign criminal conviction.

²³ Privacy considerations, protective orders, and associated special handling for IoT ESI that may be worth considering during the course of discovery are out of scope for this paper but covered in other publications including *The Sedona Conference Data Privacy Primer*, 19 SEDONA CONF. J. 273 (2018).

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to comments@sedonaconference.org

exporting the raw data itself, which could be sufficient depending on the need.

The cloud server data stores user account data, serving as direct backup (or copy) of the end-user mobile application information. It also houses unique data like historical temperature logs, user account activity logs, data transfer logs, and similar information that is more 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.

A real-world example of these considerations comes from *Garner v. Amazon.com, Inc.*²⁴ There, the defendants moved to compel the plaintiffs to identify the recordings from their Amazon Alexa devices that they alleged were private and confidential. While the plaintiffs argued that Amazon had not produced all relevant recordings and the parties were still negotiating a production process when Amazon filed the motion to compel, the court found that most of the plaintiffs could access their recordings through the Amazon portal or Alexa app and must therefore identify the relevant recordings. Notably, however, there were three plaintiffs whose claims involved recordings by Amazon Alexa devices owned by non-parties. For those plaintiffs, the court acknowledged they could not access the necessary information and excused them from this requirement.

To address these complexities and aid in IoT ESI collection planning, below are considerations and questions for practitioners to leverage throughout the collection process.

1. Accessibility and format

In Section II, a list of IoT ESI categories were defined, providing a useful foundation to guide discussions with technical resources and develop a starting point for identification and collection activities. Once potentially relevant IoT data categories and respective technical experts are identified, below are some initial questions to help assess the legal and technical accessibility for each of those sources:

- Does accessing the data require compliance with privacy regulations (e.g., GDPR, CCPA)?
- Are there legal restrictions or privacy policies that limit data access or transfer?
- Is user consent needed to access or disclose the data?
- Who has possession, custody, or control?

²⁴ 2022 WL 4753013 (W.D. Wash. October 3, 2022).

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to comments@sedonaconference.org

- Who has permissions and credentials?
- Are the appropriate collection or export tools available?
- Do secondary copies exist that are more readily accessible and provide sufficient replication or proxy of the data sought?
- Is the effort to acquire the data proportionate to the anticipated utility of having the data?

2. Physical collection of IoT devices and user activation devices

Where data on the physical IoT device is unique or otherwise required for collection, additional technical considerations may emerge. Specialized IoT devices may be difficult to gain physical access to, such as sensors embedded into larger machines, appliances, or ecosystems, rendering them problematic to isolate and directly retrieve their data. To perform the collection, it may be necessary to take the device offline or otherwise disrupt the IoT system and prevent it from performing its intended function. This could be a particularly important consideration for IoT devices supporting applications like transportation, safety, or healthcare. The number of devices is another factor, such as multiple sensors working together across a large system, as it would be time consuming to collect data from each one.

Fortunately, the very nature of IoT devices—that they are connected to the internet—means direct collection from individual devices is rarely necessary.

3. Downstream ancillary systems

Like any database, the data generated can be fed directly and indirectly to a wide variety of systems. These could be considered “upstream” or “downstream” systems depending on the context. However, since IoT devices are largely “end-point” devices, they are more likely to be sending data to a system of record (downstream data) than receiving data from other devices (upstream data).

Returning once again to the hypothetical “smart” thermostat, the cloud server that stores user account data and serves as system of record for the end-user mobile application information is an example of a “downstream” system. These can vary considerably in ownership, retention, organization, and accessibility. When these systems are known, they may be candidates for primary production sources. When they are not known, a common methodology to identify them is to “map” the data flows within the IoT ecosystem.

4. Collection, search, and export best practices

With consideration given to the results of the meet-and-confer process to determine relevance, the responding party should determine an effective collection and search methodology that can further inform proportionality.

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to comments@sedonaconference.org

Where the requested data is relevant and proportional to the needs of the case, it should be produced.²⁵ However, where IoT data would not be relevant, useful, or reliable its production is unwarranted. In *Spoljaric v. Savarese*, the court denied a motion to compel 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.²⁶ The court saw the request as an overly broad “fishing expedition” without a substantial basis.²⁷ The finding was similar in *In re 3M Combat Arms Earplug Products Liability Litigation*.²⁸ There, the court held that the “reliability and usefulness” of hearing data from Apple Health App was “diluted” and declined to compel its production.²⁹

The available supporting resources (e.g., internal information technology (IT), system users, third-party discovery consultants) may be useful to provide estimates as to the time and cost to address the challenges that may come into play when collecting IoT ESI. As with ESI generally, where IoT ESI volumes are large, consider sampling or limiting the timeframe of the collection or search so the case team can review and validate the resultant data export(s). Sampling also presents an opportunity to vet results with the requesting party to manage their expectations or otherwise educate them on the IoT ecosystem challenges early on where necessary. Again, as with ESI generally, transparency will benefit discussions with the requesting party and the process generally.

At the same time, IoT is largely structured data. And structured data has different costs and burdens than the emails and loose documents practitioners are familiar with.

As ESI searches and exports are generated by technicians or system owners, the results should also be reviewed to confirm they are readable, can be produced in a usable format, and capture the intended scope of ESI that is relevant to the discovery request. For IoT systems that have not previously been in scope for litigation, expect the search and collection testing process to take several iterations, including detailed feedback discussions between IT personnel and legal resources before a final search and collection method can be decided upon. There are also various best practices when conducting collections to ensure the accuracy and repeatability of the IoT ESI collection process. This includes avoiding manual processes, testing the systems under controlled scenarios and comparing the data collected to the tests, and also applying data export, transfer, and import quality-control techniques to verify record counts and field formats.

As IoT ESI collections are completed, documenting the methodology used to perform the collection may assist in defending the approach and facilitate supplemental collections as necessary

²⁵ 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).

²⁶ *Spoljaric v. Savarese*, 66 Misc. 3d 1220(A), 121 N.Y.S.3d 531 (N.Y. Sup. Ct. 2020).

²⁷ *Id.* at *2.

²⁸ *In re 3M Combat Arms Earplug Products Liability Litigation*, No. 3:19-MD-2885, 2022 WL 4448917, (N.D. Fla. Sept. 23, 2022).

²⁹ *Id.* at *5.

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to comments@sedonaconference.org

in the future. For example: 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 documented to record the state of the system at the time of collection.

Additional technical resources may provide information on what search and collection capabilities are available across the IoT categories of ESI. In many situations, 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

Like traditional documentary ESI (such as scanned paper, loose files, emails, and text messages), processing IoT ESI requires strict adherence to data integrity principles to ensure that the information remains unaltered during extraction, transfer, and analysis. However, processing IoT ESI presents unique challenges and processes distinct from those associated with traditional ESI.

The "processing" of IoT ESI begins with the extraction of data from specialized application databases and its subsequent migration to a generic, blank database, ensuring that this transfer and any subsequent analysis maintain the integrity of the data. IoT data is often stored and exchanged in precise formats such as comma-separated values (.CSV), which necessitates careful handling to preserve data accuracy throughout the process.

The classic terminology for handling structured data is to subject it to an ELT, which stands for Extraction, Loading, and Transformation. Here are additional details for the ELT process for IoT ESI in a litigation setting:

1. Extraction methodology

The process starts with the extraction of data from the source database. This involves creating extraction scripts or queries that can accurately pull the necessary data without alteration. Documentation of the extraction process is critical, as it provides a record of how the data was obtained, ensuring transparency and reproducibility.

2. Loading into destination systems

Once the data has been transferred, it is imported into a generic destination database. Here, the integrity checks continue, using row counts and field checksums to verify successful importation and proper formatting of the data.

3. Transformation and storage

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to comments@sedonaconference.org

IoT data formats will vary from one system to another. Different IoT data will have different structures, formats, schema, and storage technologies. Often, the data will be in formats uncommon to those who work outside of IT systems; for example, some common transfer formats are JSON, XML, and CSV. The goal of processing IoT ESI is to convert the data into a usable format that facilitates storage, management, retrieval, and analysis. This may involve creating new fields or tables within the destination database to house derived values or calculations, all of which should be clearly labeled and documented. Best practice is to have any analysis conducted on this data driven by scripts that can be later tested, verified, and produced if necessary.

4. Quality Control during transfer

During the export, loading and transfer, and loading phases, quality-control mechanisms should be implemented to maintain data integrity. These can include using field listings, row counts, and checksum numbers to verify that data is accurately transferred from the source to the destination. Additionally, the use of hash values before and after transport can confirm that the data remains unchanged during the process.

Overall, while the processing of IoT ESI shares the same goals as traditional ESI processing—namely, the preservation of data integrity and the conversion of data into an analyzable format—the specific methods and challenges differ due to the nature of IoT data and the systems from which it originates.

E. Analysis and searching of IoT ESI

The analysis of IoT ESI typically occurs 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.

Key analytical processes include:

1. Filtering

This involves selecting a subset of records based on internal or external criteria, allowing for targeted analysis. Filters may be applied to focus on specific time frames, devices, or events captured within the IoT data.

2. Sequencing

Sequencing refers to the ordering of records based on one or more fields, which can help in identifying patterns or trends over time. For example, IoT data might be sequenced to reveal the timeline of events leading up to a critical incident.

3. Calculating

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to comments@sedonaconference.org

In many cases, analysis involves 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.

For IoT ESI, the focus of analysis often shifts from individual records to broader trends and distributions. Unlike traditional ESI, where a single piece of evidence might be the "smoking gun," IoT ESI analysis is more likely to reveal patterns that indicate ongoing behaviors or conditions. These analyses often result in visual representations, such as charts or graphs, that depict trends over time or across different variables.

In the realm of IoT ESI, the "smoking gun" is replaced with the "smoking trend," highlighting how 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.

F. Review and production of IoT ESI

The format of IoT ESI after collection plays a crucial role in determining the best review approach. The exported format may be incompatible with traditional ESI review tools, making it necessary to consider alternative review methods or even producing the data without conducting a review. This is especially important given the complexities posed by the FRCP 34(b)(2)(E)(ii) requirement that "if a request does not specify a form for producing electronically stored information, a party must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms."

For IoT ESI, the "ordinarily maintained" format may not always be practical or usable without deploying additional resources, highlighting the importance of early agreement between parties on the format of production. IoT data is often structured and can be reviewed in spreadsheet formats like Excel, but as the data volume grows, more robust formats like CSV and JSON may be required for large data sets.

Review environments such as databases (e.g., SQL Server, MongoDB) or data analytics tools (e.g., R, SAS, SPSS) may be more appropriate than traditional document review platforms. When dealing with large volumes of structured data, it's important to realize that you will want methods to define a "document" or "record" for production, review, and use in legal proceedings.

For example, temporal metadata used to define time-bound documents, a common approach in social media data review, may be adaptable for IoT data. Another consideration is adding Bates numbers or row identifiers to individual records, enabling cross-referencing during trial or depositions.

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.

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to comments@sedonaconference.org

Another concern is cross-reference and Bates labeling. It can be useful to add individual Bates numbers or row numbers to individual records to provide a cross-reference capability on the trial record (e.g., “Let the record reflect that the witness is referring to file XXX, record YYY, and value ZZZ.”).

There are occasions where the relevance of the data is not limited to the data itself. It involves the data and proprietary transformations that may be affected by software, display, or context that build on the IoT data, but may require additional considerations.

V. The Impact of the IoT on Admissibility of ESI

A. Introduction³⁰

As mentioned earlier, the Internet of Things includes billions of interconnected devices that are increasingly significant in legal cases. 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.³¹ In another case, Fitbit data was used by prosecutors to disprove a rape allegation.³² As technology continues to advance, the use of IoT ESI in both criminal and civil litigation is becoming more prevalent, sophisticated, and impactful. IoT ESI is now commonly found in vehicles, safety equipment, personal devices, and a wide array of commercial systems.

This section explores the admissibility of IoT ESI in civil and criminal cases, assuming a duty to preserve and produce such data. 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 data under Federal Rule of Evidence 901(b)(1), as a witness with personal knowledge. Additional methods for authenticating IoT data include expert testimony (Rule 901(b)(3)), circumstantial evidence (Rule 901(b)(4)), demonstrating that the system or process reliably produces accurate results (Rule 901(b)(9)), and using certified records generated by an electronic system (Rule 902(13)) or certified data from electronic devices (Rule 902(14)).

The admissibility of IoT ESI in a given case will depend on the specific facts and circumstances, 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 data it generates, particularly if that data is stored on readily accessible consumer-level devices like smartphones or tablets. However, for more

³⁰ Some of the below content is taken directly or derived from *The Sedona Conference Commentary on ESI Evidence & Admissibility, Second Edition*, 22 SEDONA CONF. J. 83 (2021).

³¹ Connecticut State Division of Criminal Justice Press Release, Richard Dabate Sentenced to 65 Years in Prison for the December 2015 Murder of His Wife, <https://portal.ct.gov/dcj/press-room/press-releases/08182022dabatesentencing> (May, 21, 2024).

³² *Police: Woman's fitness watch disproved rape report*, ABC27.COM, <https://www.abc27.com/news/police-womans-fitness-watch-disproved-rape-report/>

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to comments@sedonaconference.org

complex systems, testimony from a witness with technical expertise in those systems may be necessary to properly authenticate the IoT data.

Regardless of the circumstances, legal practitioners should ensure they engage individuals who have direct knowledge of the IoT device, the data it produces, and the systems used for its retrieval. While technical expertise may not always be required, familiarity with the specific IoT ESI and its relevance to the case is crucial.

B. Chain of Custody for IoT ESI

The chain of custody for IoT ESI differs significantly from traditional digital evidence due to the unique nature of IoT systems. While traditional evidence requires a detailed, step-by-step record of the evidence's handling, IoT data offers an alternative approach through the use of cryptographic hashing, which can verify that the data remains unchanged from its original form. Hashing can ensure data integrity without requiring a complete traditional chain of custody. However, when dealing with IoT ESI, two critical elements still need to be addressed: **proof of origin** and **proof of reliability**.

C. Proof of Origin

Proof of origin ensures that the data 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, and produce the data for legal purposes. Because IoT systems often involve multiple layers of hardware and software, proof of origin becomes essential to demonstrate that the data came from the correct device and was transmitted through the proper channels without interference or alteration.

D. Proof of Reliability

Proof of reliability ensures that the data accurately reflects what it purports to represent. Due to the novel and often untested nature of many IoT systems, determining the reliability of data may require controlled testing, validation procedures, or expert testimony. For example, data from a smart thermostat may need to be tested in controlled environments to confirm that it measures temperature or user inputs as expected. Over time, as specific IoT systems become more widely adopted and understood, their reliability may be more easily established. However, until such systems are well-known, expert validation will remain a key part of proving reliability.

E. Importance in Litigation

Unlike traditional ESI, where the chain of custody often involves human actors at every stage, IoT data originates from machines, and its authenticity is often based on system logs, automatic processes, and data transmission records. Therefore, courts may place more emphasis on the provenance of the data (proof of origin) and its trustworthiness (proof of reliability) rather than requiring a detailed chain of custody. Properly documenting the technology stack and collection methods, along with verifying the accuracy of the data through expert analysis, is critical to ensuring IoT ESI is admitted and given appropriate weight in legal proceedings.

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to comments@sedonaconference.org

By addressing both proof of origin and proof of reliability, legal practitioners can demonstrate that IoT ESI is authentic, trustworthy, and admissible, even without the need for a traditional chain of custody.

F. IoT ESI authentication techniques and hurdles

There are several techniques for authenticating IoT ESI evidence and data that should be discussed in additional detail. The following paragraphs address some of the techniques, hurdles, and opportunities that come with authenticating IoT-related evidence.

1. Authentication under Federal Rules of Evidence, Rule 901

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.” This can be achieved using a nonexhaustive 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

As noted above, authentication might require the procurement of a witnesses knowledgeable about the IoT ESI, as well as its creation, processing, storage, and use. In some instances, this may involve a party witness. But in some instances, it may also require non-party 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 may be 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, adverse 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.

(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* has an extensive and detailed review of how concepts such as hashing, encryption, metadata, computer forensics, and blockchain can be used to authenticate data generally and may assist in the authentication of IoT ESI. In all cases, the legal professional 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, and distracting, explanations to demonstrate its

³³ FED. R. EVID. 901(b)(1), 901(b)(3), 901(b)(4). See also The Sedona Conference, *Commentary on ESI Evidence & Admissibility*, Second Edition, 22 SEDONA CONF. J. 83 (2021), at 132–33.

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to comments@sedonaconference.org

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, kept, and stored, the sheer reliance of lay witnesses or distinctive characteristics may not be sufficient for its authentication. 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 data. 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. A cottage industry of IoT ESI forensic experts is already developing that will likely be useful for such purposes.

2. Self-authentication of IoT ESI under Federal Rule of Evidence 902(13)³⁴

Rule 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)).” This rule provides an opportunity to authenticate ESI “other than through the testimony of a foundation witness,” as the comments to the rules confirm. The purpose of the rule is to avoid the unnecessary expense of 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 data 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.” 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 Rule 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. It is important to note that authentication under federal and most state evidence rules is a prerequisite for admissibility of such evidence and, as the advisory committee 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.”³⁵ Moreover, even if the

³⁴ *Id.* at 133.

³⁵ Advisory committee 2017 note to FED. R. EVID. 902 (2017). Recognize that some of these objections would not apply to structured data collected from electronic monitors and other devices.

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to comments@sedonaconference.org

evidence is admitted at the hearing or trial, that does not create a presumption of credibility for the finder of fact; rather, 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, and (3) witness corroboration of the IoT ESI.

3. Potential IoT hearsay issues³⁶

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 assertions, written assertion, or nonverbal conduct, if the person intended 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 heartrate, 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 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 Rules 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 that chose to record that activity as an “Outdoor Walk”—which does not mean that it actually 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 and stores the audio and sends actuating information to other resources in the IoT universe. Other resources (devices or software) detect the fact that you are moving, your temperature, and take 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 as to 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 such data, and whether a party opposing the admission of IoT ESI asserts that the

³⁶ The Sedona Conference, *Commentary on ESI Evidence & Admissibility, Second Edition*, 22 SEDONA CONF. J. 83 (2021), at 133.

³⁷ FED. R. EVID. 801(a).

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to comments@sedonaconference.org

source of IoT ESI sought to be admitted under that exception, or the method or circumstances of preparation, indicate a lack of trustworthiness under Rule 803(6)(E).

4. *Daubert/Frye* applicability and experts

Experts will likely be required to authenticate IoT ESI and pave the way for its admissibility. 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, i.e., 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 data. For example, supply chains use IoT in factories 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 data as it relates to industry practices. A qualified witness might need a broad understanding of IoT data across these systems to effectively testify about it.

5. Forensic acquisitions and consulting

In cases involving IoT ESI, it may be necessary to engage a forensic consultant or expert for collection. These specialists can handle the complex process of on-site acquisition and collection of IoT data, such as how experts assist with traditional electronic document retrieval. The intricacies of IoT ESI collection often exceed the understanding of opposing counsel or the court, making expert involvement crucial, especially in high-stakes cases. To ensure proper handling of IoT ESI, it's advisable to incorporate specific procedures for its storage, collection, retrieval, and use in an ESI protocol, or even develop a separate protocol dedicated to IoT data, much like those used for source code review and production. Importantly, the same expert who collects the IoT data 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.

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to comments@sedonaconference.org

Appendix I: Decision Tree for IoT ESI in Litigation

I. Step 1: Identification of IoT Data

1. **Are there IoT devices involved in the case?**
 - **Yes** → Proceed to Step 2.
 - **No** → IoT data not relevant; proceed with traditional ESI collection.
2. **Have all relevant IoT devices and data sources been identified?**
 - **Yes** → Document the devices and data sources.
 - **No** → Investigate potential IoT systems, sensors, or devices (e.g., wearables, smart home systems, industrial IoT).

II. Step 2: Preservation of IoT Data

1. **Is there a legal duty to preserve IoT data (triggered by litigation)?**
 - **Yes** → Issue legal holds and proceed to preservation strategies.
 - **No** → Monitor for changes, but no preservation is needed yet.
2. **Is IoT data continuously generated and overwritten?**
 - **Yes** → Implement immediate legal holds to stop auto-deletion or overwriting.
 - **No** → Standard preservation techniques apply.
3. **Who controls the IoT data (possession, custody, or control)?**
 - **Single Owner** → Notify the owner to preserve data.
 - **Multiple Owners** → Identify all relevant parties and notify each of their preservation responsibilities.

III. Step 3: Collection of IoT Data

1. **Where is the IoT data stored?**
 - **On device** → Forensic collection of device data.
 - **In cloud or distributed systems** → Coordinate collection with cloud providers and service platforms.

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to

comments@sedonaconference.org

2. Is the data format proprietary or standard?

- **Proprietary** → Work with experts to ensure compatibility with standard eDiscovery tools.
- **Standard** → Proceed with traditional collection methods.

3. Are there any third-party service providers involved?

- **Yes** → Contact and coordinate with third parties for data retrieval.
- **No** → Proceed with direct data collection.

4. Can the IoT data be efficiently sampled?

- **Yes** → Use sampling techniques to narrow the scope.
- **No** → Full data collection is necessary.

IV. Step 4: Review of IoT Data

1. Is the collected data structured or unstructured?

- **Structured (e.g., logs, sensors)** → Use database tools for efficient review.
- **Unstructured (e.g., media)** → Process the data through traditional eDiscovery review platforms.

2. Is the data voluminous?

- **Yes** → Apply filtering and culling strategies (e.g., date range, key terms).
- **No** → Proceed with full review.

3. Are there privacy or confidentiality concerns?

- **Yes** → Apply redaction and encryption before production.
- **No** → Proceed with full review.

V. Step 5: Production of IoT Data

1. Has the data been properly reviewed and filtered?

- **Yes** → Proceed to production.
- **No** → Complete review and apply necessary redactions.

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to comments@sedonaconference.org

2. In what format will the data be produced?

- **Standard format (e.g., CSV, JSON)** → Produce in structured format.
- **Proprietary format** → Convert to usable format or provide proprietary tools for data access.

3. Is there a negotiated production format with opposing counsel?

- **Yes** → Produce in agreed-upon format.
- **No** → Negotiate the format before production.

VI. Step 6: Use in Litigation (Authentication and Admissibility)

1. Has the data been authenticated?

- **Yes** → Proceed to admissibility discussions.
- **No** → Establish authentication via chain of custody, hash values, expert testimony, or proof of origin.

2. Is the data admissible under the Federal Rules of Evidence?

- **Yes** → Present data in depositions or court filings.
- **No** → Address admissibility issues (e.g., relevance, reliability, authentication).

3. How will the data be presented?

- **As evidence in depositions or pleadings** → Include in discovery documents and arguments.
- **As trial evidence** → Prepare exhibits, expert testimony, and visual aids for presentation.