

# The Sedona Conference WG1

## Draft Primer on eDiscovery Implications of the Internet of Things

### **Drafting Team Members**

Kevin Clark	Sean Cotulla
Warren Kruse	Sara Lockman
Kyle Pozan	Dan Regard
Christopher Suarez	Hon. Juan Villaseñor
Josh Zylbershlag	

### **Team Leaders**

David Gaston	Steven Teppler
--------------	----------------

### **Steering Committee Liaisons**

Ross Gotler	Greg Kohn
Jennifer Coleman	

Copyright 2021, The Sedona Conference. All rights reserved.



## Summary and Outline

### **The Sedona Primer on the eDiscovery Implications of the Internet of Things The Sedona Conference Working Group 1 – October 2021**

Following on the work of a brainstorming group, The Sedona Conference Working Group 1 formed a drafting team to author a paper on the eDiscovery implications of the Internet of Things (IoT). The charter for this IoT drafting team is to develop a primer that (i) addresses the unique discovery challenges posed by IoT data; (ii) considers the Federal Rules that may apply to the preservation and discovery of IoT data; (iii) discusses how The Sedona Principles and other Sedona publications apply to IoT data; (iv) provides guidance on the hot button issues related to IoT data; and (v) develops best practices that courts, counsel, and clients can follow regarding discovery practice and, in particular, handling requests for IoT data.

The outline that follows represents the work of the drafting team to date and sets forth the proposed structure and content for the primer.

As part of the 2021 Sedona Working Group 1 Annual Meeting, the drafting team requests feedback from WG1 members on the outline, both generally and specifically with respect to the following:

- 1) What guidance on eDiscovery and the IoT would be of most practical use to the bench, bar, and parties? The topics we plan to cover are listed below, with more detail in the outline. Does the WG1 membership think any topics should be added or removed?
  - a. Background on the IoT and IoT ESI.
  - b. IoT ESI and Federal Rules of Civil Procedure 34 and 45 – preservation, parties and non-parties, format, possession, custody, or control.
  - c. IoT ESI and Federal Rule Civil Procedure 26(b) and 26(f) – discovery scope, proportionality, meet & confer discussions, custodians, ESI protocols.
  - d. IoT ESI and Admissibility – authentication, Rule 104(a) hearings, hearsay, Daubert/Frye and experts, forensic acquisitions.
- 2) The drafting team is intending that the final work product be a primer. Does the WG1 membership agree that a primer is the appropriate type of Sedona paper for these topics at this time, or would a more in-depth commentary be preferred?
- 3) We intend to provide additional content in appendices. The current proposed content of the appendices is listed below, with more detail in the outline. Does the

WG1 membership think any content should be added to or removed from the appendices? Should any content from the main body of the paper be moved to the appendices, or vice versa?

- a. A more in-depth technical discussion of the IoT and IoT devices.
  - b. Details on IoT sensor data and export of data.
  - c. Collection and delivery mechanisms of IoT ESI.
  - d. Transformation of IoT ESI into smaller data sets.
  - e. Where does the data go? Explanation of connectivity considerations like third party applications, integrations, or other 'downstream' locations.
- 4) With the pace of technological advances, how should we ensure the ongoing relevance and applicability of this paper? Would Sedona's Technology Resources Panel (TRP) be useful in helping develop a "technology education" component and supplementing the paper in the years to come as technological advances modify existing IoT technologies?

## **Outline**

### **I. Introduction**

The universe of discoverable electronically stored information (ESI) has been significantly expanded by the emergence of tens of billions of connected devices, commonly known as the Internet of Things (or “IoT”).

The emergence and ubiquity of these devices (and the potentially discoverable information generated, collected, transmitted and stored in association with them) pose unique discovery challenges which may not fit neatly into the current discovery regime of the Federal Rules of Civil Procedure and associated decisional authority.

In this primer, we offer information and guidance to parties, the bench, and the bar on the intersection of e-discovery law and the Internet of Things.

### **II. Background**

#### **A. What is the IoT and what are IoT devices?**

As previously defined by The Sedona Conference in the Commentary on ESI Evidence & Admissibility, the IoT “is a network of computing devices and sensors embedded in everyday objects that create, collect, and share data through the internet. Some examples include wearables that track our steps and sleep, appliances that track our consumption, and thermostats that adjust to our habits. The data that these devices create is often stored in structured databases and may be stored in multiple locations in the cloud.” IoT devices have become commonplace in the consumer, commercial, and industrial contexts.

IoT devices are broadly defined as physical objects that embed a technology (e.g., Bluetooth, RFID, cellular modem) that allows them to communicate with the Internet, other networks (e.g., home LAN, and other devices). In this, IoT devices are differentiated from digital objects (e.g., a database, photo, webpage) which can also communicate with the Internet, other networks, and devices. An IoT device can generate, receive, analyze, and store ESI.

## B. Categories of IoT ESI

Here we outline five categories of electronically stored information relevant to IoT and IoT devices – IoT ESI.

### 1. Data generated by the IoT device itself

IoT devices generate ESI, sometimes a voluminous amount of it. Some of the ESI may be intended for easy review by the end-user while other ESI may only be intended for rare instances when a technician or engineer needs to review the performance of the device but not otherwise meant for end-users to ever access. Examples of the former include video recorded by a Ring doorbell for review by the homeowner or workout metrics captured by a Fitbit device which are meant for the wearer to review on the device or on an associated app. Examples of the latter include logs maintained by a car's onboard computer which record engine performance, or an Apple Watch maintaining a record of app crashes.

As regulatory and consumer attention has focused on privacy concerns related to the information created by IoT devices, manufacturers of such devices have begun to provide consumers with greater insight and control over ESI maintained by the devices. For example, some car manufacturers now provide consumers with granular control over how data from the onboard computers systems is used. Consumers can choose whether driving metrics are shared with insurance companies or can decline to do so.

### 2. User communication devices used to remotely activate or interact with the IoT device ("User Activation Device")

Many IoT devices are designed to be accessed, controlled, or used through communication with another device. Examples include a wide-variety of home automation devices that are controlled from smart phones. These can include lights, heating and air-conditioning systems, lawn sprinklers, and many others. Some IoT devices are designed to only be controlled via another device. For example, Apple's AirTag doesn't include any buttons. Consumers configure and use these devices via their phones. Other devices can be operated without the use of another communication device but connecting them to a phone or tablet provides access to functionality that cannot be accessed directly from the IoT device. As an illustration of

this point, many modern air-conditioners can connect with smart phones and then provide consumers with details around usage and energy consumption which cannot be accessed directly from the air-conditioner.

3. Web-based management platform or system for a device or devices.

Web-based management systems often store ESI generated by a single or multiple IoT devices. A foreperson monitoring the work of a host of factory floor robots can use a web interface to assess the operation of the robots and provide control input from such an interface. A consumer can access their broadband provider's website and then review and control a variety of devices connected to their home network.

4. Repository (local – the device itself – or cloud based) used to store data

The vast quantities of ESI generated by IoT devices are often gathered and stored on local or cloud-based storage repositories. A typical Apple Watch contains 16GBs of storage space which can include both data intentionally placed there by the user (e.g., music, notes, photos) or maintained by the device as part of its ordinary operation. However, the same Apple Watch is usually integrated with the owner's iCloud account and historical information can often reside there for years. Another example is the Amazon cloud where users of Alexa devices can find (and delete) audio recordings created every time they activated the Alexa voice assistant on their devices (both intentionally and unintentionally).

An example of the unintentional consequences of storing and utilizing IoT derived data made headlines in 2018 when a data visualization heatmap of user activity released by a fitness app company revealed the location of secret US military installations in Syria.

5. Third party applications, systems integrations, or 'downstream' locations that connect to the WMP or storage repository.

Much of the success and power of IoT devices relies on their inter-connectivity with a host of other devices, networks, and platforms. Fitness trackers for instance, not only provide consumers with workout and health metrics, but can also connect to wellness platforms maintained by

insurance companies which then reward the consumers based on their activity levels. Such downstream repositories can contain ESI from millions of devices with differing levels of anonymization and accessibility.

C. Example(s) of an IoT ESI ecosystem

1. Home automation and control

Examples: locks, thermostat, lights, security cameras, garage door opener, lawn sprinkler controller, home speaker / assistant, mobile apps.



2. Industrial Internet of Things

Examples: smart robotic arm, inventory tracking using RFID tags, GPS based logistics, Enterprise Resource Planning dashboards, facility security, augmented reality glasses





D. Some Unique Attributes of IoT ESI

1. The end user could be in the possession, custody and control of a physical IoT device.
2. IoT manufacturers and data service providers might be in possession, custody, or control of IoT data relevant to the dispute.
3. It is typically highly proprietary and difficult to collect and process using standard e-discovery tools and workflows.
4. It can present unique chain-of-custody and authentication issues.
5. It can be extremely voluminous and present challenges when trying to extract relevant information.
6. It can be ephemeral and volatile.

III. **IoT ESI and Federal Rules of Civil Procedure 34 and 45**

With reference to and reliance on existing Sedona papers, here we will address and compare preservation and discovery duties for IoT ESI for parties and non-parties.

A. Is there a duty to preserve at all?

Yes. There is a pre-litigation obligation to preserve discoverable information, including ESI, when litigation is known or reasonably anticipated. And ESI was defined by the committee to the 2006 amendments to Rule 34 to the Federal Rules of Civil Procedure to include the types of “dynamic databases” inherent to the function of IoT devices.



Those changes signaled a new era where all ESI with potential evidentiary value, including the diverse datasets created by smart, Internet-connected devices, must be preserved.

B. Is there a pre-litigation obligation to preserve?

In general, yes. But when it comes to specific devices or data, that question is complicated by issues of possession, custody, or control, reasonable accessibility, and proportionality.

Possession, custody, or control are discussed below, but the smart thermostat is illustrative of the issue. An individual may have a smart thermostat in their possession and some of the data may reside on their phone, but the majority of the data may be in the cloud and unavailable to the individual through normal channels (e.g., contacting customer support). Obtaining that data may require a subpoena to the service provider.

Even if all of the data generated by the IoT device is in the individual's or entity's possession, custody, or control, obtaining the data can be complex, difficult, or beyond what may be considered "reasonably accessible because of undue burden or cost" under Rule 26(b)(2)(B), or proportional to the needs of the case under Rule 26(b)(1).

In such circumstances, it is the burden of the device manager or party with possession, custody, or control to demonstrate why native preservation is an undue burden or disproportionate, submit specific information to define this burden, and offer alternate means of effective preservation, which may include the use of separate media or off-device storage.

Preservation also depends on the type of data and who owns or maintains it. Retention policies should be in place for those that administer and maintain the data. However, it becomes complicated when trying to determine possession, custody, and control.

Those that administer and maintain the data and or its storage locations need to be transparent about their retention policies to the end users.

- C. What considerations are there relating to possession, custody, or control? Does this vary based on IoT ESI category and what data is readily accessible to a party?

The explosion of distributed or “cloud” computing, remote hosting, Software as a Service, mobile data platforms, wearables, smart home devices, and other Internet-connected devices means that the question of possession, custody, or control necessitates a case-by-case evaluation. Principal issues to consider are:

1. The physical location of the device and the data it creates.
2. The location of the data created by the device.
3. The reasonable access a party has to the device and the data it creates.
4. The retention policy of the manager of the device and the data it creates.
5. The reasonably accessible data physically held on the device and the data it creates.
6. The reasonably accessible data on local network-attached storage.
7. The reasonably accessible data stored offsite/in the cloud.
8. Who possesses the data stored offsite/in the cloud?
9. Who created the data, user or device based on default settings?
10. Who can authenticate? Data that the user created can be captured by the user and authenticated. Data they did not create, like metadata, cannot be captured nor can they authenticate it.
11. The function within the ordinary course of business (in the context of Rule 34) of the device and the data it creates.
12. Any resources that aggregate or otherwise log and/or process information from the device.
13. Any resources that duplicates data created by the device.

The considerations should not vary based on IoT ESI category or whether the data is readily accessible as those are separate considerations—namely, those raise the question of proportionality.

- D. Are there differing preservation burdens for parties vs non-parties?

This is a larger question of the conflict of Rule 34 vs Rule 45 and the complications introduced by “possession, custody, or control” in Rule 26.

It also depends on the jurisdiction, as some jurisdictions have held that non-parties have no duty to preserve ESI unless there is a subpoena or obligation to preserve it.

E. Is IoT ESI considered ephemeral?

Not inherently, no. IoT data can be ephemeral or may persist per the needs of the user, the function of the device, or the relevant records management policy.

However, ESI from an IoT device may be functionally ephemeral depending on the design and function of the device.

IoT data may also be ephemeral on the device itself where the primary retention of the device data is intended to be maintained elsewhere, such as on paper (the short term memory of a copy machine) or in a centralized server (a fitness step counting device).

If information is functionally ephemeral the burden should be on the producing party to demonstrate this and offer means of early collection, remediation, or alternative data sets that capture the discoverable information in question. As an example, a preserving data from a program that captures step data daily from a device could be used as a substitute to preserving the data on the actual device.

RAM, cache, tmp and var files, are problematic. What about backup systems or disaster recovery systems? All data can be ephemeral or non-ephemeral depending on the configuration and intent of use.

F. To what IoT ESI does the duty apply?

All discoverable ESI should be considered, however, the "reasonably accessible" and proportionality standards comes into play.

Proportionality changes the longer a type of technology is used. Newly used technology may not be reasonable as there are no tools to collect or process. As technology ages this become less of a burden then the pendulum swings to the other side. As the technology ages out, less tools are available to collect and process.

G. How to preserve IoT ESI and in what format?

An early conversation about the objective of the request of IoT data should occur (such as during a Rule 26(f) conference) to provide notice of the need and discoverability of the data in question.

Early discussions need to be held with custodians or those responsible for the management of the IoT devices to identify relevant IoT data.

Preservation of IoT data should be keyed to its primary business function. If the IoT device data can be demonstrated to be stored elsewhere in the ordinary course of business (rule 34), that should be considered if not preferred.

This is dynamic as investigations and litigation can go on for years. If data is preserved only in the format it is kept in the usual course of business, there become a time it become too expensive to finally convert to a more usable format.

H. Is there a potential preservation conflict between “Reasonably Usable” and “Ordinarily Maintained,” as IoT ESI that is ordinarily maintained may not be reasonably usable?

Yes. Where information is used in the ordinary course of business in a format that is not reasonably accessible – such as in a proprietary database --accommodations should be made to convert it into usable data.

It is likely this will happen during the course of review and collection by the producing party. Production with the same functionality of search and review should be prioritized over native format where native format does not readily allow useful review with the ability to authenticate.

I. Does a preservation obligation require migration to non-obsolete format for legacy IoT ESI?

This is a case-by-case question that requires a proportionality analysis based on the facts, the costs, and the needs of the case.

Format should be determined by how the information is used in the ordinary course of business and how the information is collected, maintained, and reviewed by the producing party.

#### **IV. IoT ESI and Federal Rule Civil Procedure 26(b) and 26(f)**

With reference to and reliance on existing Sedona papers, this section of the paper will address concerns and best practices related to discovery scope, meet and confer discussions, and ESI protocols.

**A. What categories and types of IoT ESI are in scope?**

Refer to the categories defined above.

IoT is a broad term and the types of ESI implicated can vary greatly depending on how the technology was designed, how it functions, and how it interacts with other systems.

Leverage and expand on the existing Sedona Conference Commentary on ESI Evidence and Admissibility definition of IoT.

**B. FCRP 26**

1. To the extent IoT ESI is probative, not prejudicial, and not disproportionate, then it may be in scope. Refer to special considerations, such as for hearsay and privacy.
2. Proportionality and burden considerations for IoT ESI, including:
  - (a) Cost of collection activities that are unique to IoT ESI
  - (b) Burden of complying with data privacy laws
  - (c) Tools (hardware, software, processes) available
  - (d) Endpoint firmware considerations
  - (e) Large volume and short retention considerations
  - (f) Structured and unstructured data elements
  - (g) Metadata considerations
  - (h) Encryption and cybersecurity considerations
  - (i) Data location and category if IoT ESI
  - (j) 3<sup>rd</sup> party data
3. Meet and Confer planning
  - (a) Engaging technical experts to support in advance. Provide examples of key questions to ask when engaging business and IT experts

(b) Burden arguments and scope negotiations, topics include cost considerations, volume of ESI and sampling techniques.

C. Are there any special considerations relating to determining relevance of IoT ESI?

1. What was the intended IoT use and how the ESI relates to the credibility, claims, and defenses, or damages of a case?

(a) Data source considerations

- (i) Importance of understanding the originating source of the data being captured
- (ii) Sensor data from non-human activities
- (iii) Data capturing human activities or informing human decisions

(b) Data use and purpose considerations

- (i) Importance of understand the original intent or purpose of data collection
- (ii) Data used to inform human decisions
- (iii) Data used to inform AI/ML models

2. How does the requesting party intend to use the IoT ESI and the need for sufficient detail for requesting party to respond?

D. Do any of these determinations vary based on category of IoT ESI?

1. Category of IoT ESI may change the approach. Address specific considerations for each of the 5 categories listed above

E. Discovery Plan/ESI Protocol

1. Potential need for ESI protocol tailored proportionately to the needs of the case addressing custodians, repositories, formats, and preservation parameters.

(a) Specific scope requirements and limitations that address IoT ESI categories, custodians, repositories, formats, and preservation parameters

- (b) Reasonable readable production format specifications. Data types supporting contextual documentation may be relevant to interpret the produced data, like database schema and queries

#### F. Custodian

1. Who is the owner of IoT ESI for purposes of determining possession, custody, or control?
  - (a) Varies by IoT ESI categories
  - (b) The "owner" may often be a combination of the service provider and the user (individual or organization)
    - (1) Service terms and conditions
    - (2) Privacy considerations
2. Where is the relevant data generated?
  - (a) IoT Device, User Activation Device, WMP User – may or may not have a combination of actual (Sensor Device, User-Activated Device) and practical control over the IoT ESI.
  - (b) Controlling factors – 'where' and 'time' of data generation
  - (c) Must look to local law, decisional authority, or terms of service.

#### G. Collection and Formats

1. Initial questions that can be asked of any owner / provider / agent to assess accessibility
  - (a) Is the native format of IoT ESI reasonably usable or in a proprietary format?
  - (b) What collection or export tools are available?
  - (c) Does business intelligence (BI) reporting or similar aggregations of the IoT ESI exist that are more reasonably accessible and meaningful than raw data exports (e.g. logs, streams, sensor data)?
2. How to preserve or produce?
  - (a) What are the technical barriers that could contribute to this burden?



(b) If IoT ESI can only be read after processing by WMP or User Activation Device, which data set should be discoverable or should be produced?

3. Collection specific considerations for each category of IoT ESI

- (a) Standalone vs industrial applications vs ecosystems
- (b) Storage formats
- (c) Validation and accuracy
- (d) Static vs dynamic data elements
- (e) Data visualizations
- (f) AI/ML model data elements
- (g) Secondary sources and downstream storage

4. Collection general best practices

- (a) Methodology documentation
- (b) Data dictionaries and data flow maps

#### H. Search and Accessibility

1. Proportionality, burden, and cost generally of search, identification, collection and processing of IoT ESI
2. Search methodologies
3. Testing and sampling
4. Resources to support complex searching needs (e.g. internal IT resources, third party tools, or consultants to navigate search and retrieval of ESI)

#### I. Repositories

1. ESI may be stored in different “locations” that could be physical, local, or “cloud based.”
2. What are the terms of service associated with each IoT ESI location?
3. Which repositories need to be searched?
4. What is the difference between the data in each location?
5. What parameters can be used to define a “document” or a “record” within the IoT ESI data set?

#### J. Review

1. What criteria can be used to define a ‘document’ for purposes of capturing work product (e.g. priv, relevance) and labeling for production?
2. What are the available review technologies and/or methodologies for large-volume structured IoT ESI exports?
3. Format of data may limit or augment traditional ESI document review processes and production labeling (bates, redactions, endorsements)

### V. IoT ESI and Admissibility

With reference to and reliance on existing Sedona papers, this section of the paper will address concerns and best practices related to the admissibility IoT ESI evidence.

A. Authentication hurdles of IoT under Fed. R. Evid. R. 901.

1. Knowledgeable Fact Witnesses

- (a) May require third party subpoenas, obtaining witnesses who have to testify to atypical foundational facts

2. Distinctive Characteristics

- (a) Establishing admissible evidence generally vs. establishing that the evidence is of an “IoT nature,” may prove difficult

- (i) Typical metadata
- (ii) Security features/fingerprint
- (iii) Blockchain

3. Technology Experts

- (a) Particularly for certain IoT applications like Blockchain, the nature of the data itself may be of a sufficiently complex nature to require expert testimony, creating some hurdles.

B. Self-authentication of IoT ESI under Fed. R. Evid. R. 902(13)

1. Certification from a qualified person that complies with the certification requirements of Rule 902(11) or (12).
2. Self-authentication obviates a Rule 104(a) hearing.
3. Can there be a certification authority for certain IoT data?
4. "Trusted" sources of IoT data.
5. Use of Encryption, Hash Values, Metadata.
6. Blockchain evidence - Vermont, when accompanied by declaration of qualified person.
7. Hearsay and other objections to the *content* of IoT remain. Rule 902(13) advisory committee n. (2011) ("The opponent remains free to object to admissibility of the proffered item on other grounds—including hearsay, relevance, or in criminal cases the right to confrontation."). See below, too.

C. Rule 104(a) hearing topics

1. "Does the evidence have sufficient probative value to sustain a rational jury finding that the evidence is what the proponent claims it to be?"

(a) Possible Witnesses

- (i) Company IT personnel
- (ii) Company custodian of records
- (iii) Service providers (for IoT devices, such as SmartHome device, wearables, etc.)

(b) Possible Topics

- (i) IoT Data Collection Policies
- (ii) IoT Data Retention Policies
- (iii) IoT Data Structure and Use
- (iv) IoT Data Privacy Policies and Impact on Admissibility

D. Potential IoT hearsay Issues

1. Difference between “point of control” of IoT data and the “point of use” of the IoT data, particularly when trying to link IoT data to a particular person
  - (a) There are multiple levels of complexity from the IoT sensor to the database on a server where the sensor’s data is stored
  - (b) In other words, the chain of custody creates some hearsay problems
  - (c) Risk of manipulation of IoT data
  - (d) Is the IoT data a “statement” under Fed. R. Evid. 801(a)?
2. Hearsay of “overheard” communications on an IoT device

E. Daubert/Frye applicability and experts

1. Experts on proper methodologies of IoT data analysis and authentication
2. Experts on proper retention and deletion policies for IoT data
3. Experts on particular IoT technologies
  - (a) Blockchain
  - (b) Network infrastructure and architecture
  - (c) Sensors
4. Experts on particular IoT industries
  - (a) Supply chain
  - (b) Cryptocurrency
  - (c) Autonomous vehicles

F. Forensic acquisitions

1. Companies that specialize in IoT data
2. On-site acquisition and collection of IoT data
3. Complexities of reviewing and securing IoT data for collection
  - (a) *Compare* source code review protocols. Will something similar be needed here?

G. Expert reports

## VI. Appendix Topics

Potential topics for appendices include the following.

- A. Additional details relating to IoT ESI, including the IoT Reference Model. The IoT Reference Model describes four layers in the IoT ecosystem:
  - 1. Device layer: These are the physical components that directly capture information via sensors or via input from people. Some devices can communicate directly to the Internet (e.g., a wi-fi enabled air-conditioner) while others require the use of a gateway that can aggregate data from multiple devices and potentially pre-process the data before transmitting it to a cloud platform (e.g., an office building with networked motion-sensing lighting and climate controls).
  - 2. Networking layer: Provides network connectivity and communication capabilities for IoT devices. May include Bluetooth, wi-fi, cellular, or other networking technologies.
  - 3. Service support and application support layer: an intermediary layer in the IoT ecosystem that provides technology support such as storage or computing to the IoT ecosystem.
  - 4. Application layer: the software system used to control IoT devices, leverage the data gathered by the devices, or otherwise derive value from the IoT system.
- B. Generation of sensor data / where does it come from
  - 1. Examples of raw data export vs aggregate report.
    - (a) A raw data export from an IoT device can include logs from sensors, file system information from on-board storage, and a variety of other data points regarding the functionality of the device. Given the immense diversity of IoT devices in the marketplace and the often-proprietary nature of their software and hardware, it can be exceedingly difficult to extract, collect, and use raw data exports.

- (b) Because IoT devices by their very nature include the ability to communicate with other devices, networks, and platforms, it is generally simpler to gather and review aggregate data sent from the device. For example, trying to extract information from a smart device can be quite difficult. But reviewing the device's history on an accompanying home, business, industrial automation application is typically much simpler.

DRAFT



C. Collection and delivery mechanisms of IoT ESI devices

1. There may be limited documentation for the device.
2. The connection port may be proprietary.
3. The data may be encrypted or in a format that needs to be converted.
4. What will be necessary to allow the data to be reviewed or produced.
5. Physical possession of the device doesn't mean you have adequately preserved or collected all the data.
6. Is the owner of the device / account identified and available?
7. Should the device remain powered on or can it be powered off?
8. Should the device be disconnected from Wifi?
9. Limited data may be available if offline.
10. If device is online it is likely that account credentials are required to access account content.

D. Transformation of IoT ESI into smaller data sets

Immense Data Sets - IoT generates a large amount of high-speed, varying and unstructured big data. The large amount of data that IoT generates needs to be processed before the information can be used. Because the data often comes from numerous devices or in different formats, there are several things you must do before processing or applying any type of analytics to the data.

1. Standardize or transform the data to a uniform format, ensuring that that format is compatible with your application.
2. Store or create a backup of the newly transformed format.
3. Filter any repetitive, outdated, or unwanted data to help improve accuracy.
4. Integrate additional structured (or unstructured) data from other sources to help enrich your current data set

E. Where does the data go? Explanation of connectivity considerations like third party applications, integrations, or other 'downstream' locations.

1. IoT devices create data that is sent to the main application to be sent on, consumed and used. This data can be sent in real time or in batches at specified times or amounts. Time sensitive data has to be accurate and timely, by its nature, to fulfil the purpose of the application.
2. After the initial creation of data, which takes place on the device, it is transferred over the Internet, typically using protocols described above, to a central system which collects and organizes this data.
3. IoT data is mostly unstructured and is typically stored in databases in the cloud.
4. Other storage locations include local databases, but typically big data analytics platforms are utilized through IoT cloud services to process and store IoT data.