LITIGATION NEXT:

EDISCOVERY AND THE INDUSTRIAL INTERNET OF THINGS

LITIGATION NEXT:

EDISCOVERY AND THE INDUSTRIAL INTERNET OF THINGS

The term Industrial Internet of Things—also known as the Industrial Internet or IIoT—represents a distinct and powerful subset of the more commonly known Internet of Things or IoT. Most simply understood, the Industrial Internet brings IoT technologies to high-infrastructure investment industries like manufacturing, power, transportation and even water. In operation, however, the Industrial Internet will transform a wide variety of industries and ultimately drive the next Industrial Revolution. Specifically, the Industrial Internet leverages technologies like machine learning, big data/data analytics, and sensor-driven, machine-to-machine communication to extract data from virtually every kind of industrial machinery.

Combining the machines that fueled previous revolutions with technologies that collect, ingest, and analyze data from those machines offers the promise of heretofore unattainable industrial operational improvements and efficiencies. And that transformation has already begun. From the manufacturing factory floor to energy-harvesting windmills and oil and gas, businesses are embracing the Industrial Internet.[1] Ultimately, the Industrial Internet will redefine the business landscape and lead to entirely new categories of products and services. All told, the impact of the Industrial Internet will be measured in trillions of dollars.[2]

If past is prologue—just think about the smartphone wars—the Industrial Internet will bring numerous business and legal disputes. As old players and new entrants seek to define the ecosystem and protect current turf, litigation over issues like performance, proprietary knowledge, data use, and security seem certain to follow. Who owns the algorithm? How do data protection responsibilities

change when factories flood or someone gets hurt? What about when cyber-breaches or industrial espionage occur?

Disputes over the Industrial Internet will certainly give birth to new Ediscovery challenges as companies attempt to manage an environment that generates terabytes of data each day. How will those charged with preservation duties know what to look for and where to find what they need? How will they know how to isolate the relevant information out of a mountain of data? Will they know how to preserve it? How will vendors identify and isolate relevant information? How will attorneys collect, process, and make sense of the new data and unique data sources?

… the impact of the Industrial Internet will be measured in trillions of dollars.

The Electronic Discovery Reference Model[3] ("EDRM") provides a traditional framework of where to start. Many Ediscovery practitioners have adopted the EDRM to communicate a shared vision of the Ediscovery process flow and its relationship with Information Governance. The EDRM offers a conceptual rather than literal approach to Ediscovery.

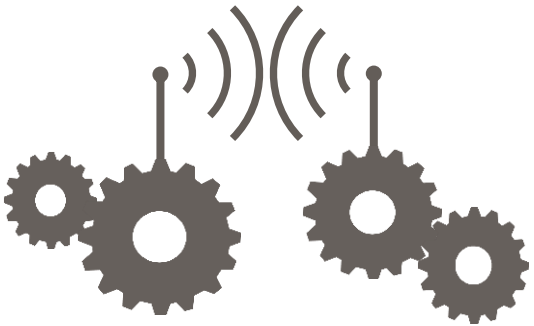
The model begins with the ongoing management, preservation, and collection of a company's electronically stored data, particularly in the context of a pending or actual legal dispute. The remainder of the model's flow outlines the structure for data processing, review, and production. Tackling practical Ediscovery obligations before, during, and after a dispute adds an additional layer to the EDRM framework. Along with established best practices, these analytical frameworks provide some guidance for how to approach Ediscovery challenges presented by the Industrial Internet.

EDISCOVERY AND THE INDUSTRIAL INTERNET:

A CHALLENGING SCENARIO

Using a specific hypothetical situation can help illustrate the unique considerations involved when data generated in the Industrial Internet becomes the subject of Ediscovery. As an example, the following scenario imagines a dispute involving Intellectual Property ("IP") issues related to the Industrial Internet and the challenges of preserving and producing data in that environment.

Meet Jen Daniels,[4] a double-major in physics and computer science. Jen's research positions in college lead to a primary research role in one of her university's patenting efforts around early machine-to-machine ("M2M") communication programming. A summer internship at a major Silicon Valley tech company then leads to graduate work in California. Together, she and Eric Bada, another grad student, launch a start-up focused on developing software for a telemetry-based water resource monitoring system. Jen and Eric patent their software, but run out of funding before they can monetize it. They both take jobs with a larger industry player who also agrees to pay off their debt in return for an assignment of all rights to their telemetry software.

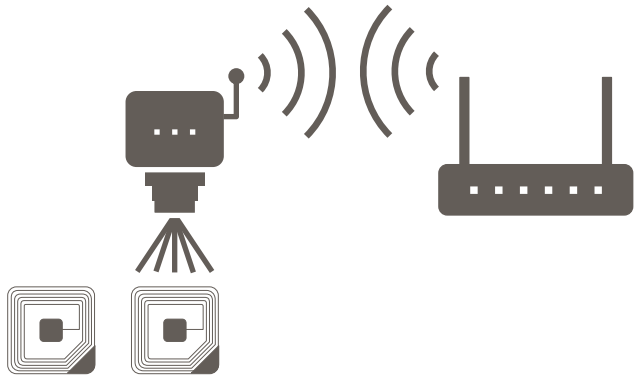


Jen receives her Ph.D. and continues her work around M2M communication, radio frequency ("RF") design, and wireless communication. She changes jobs several times in the ten years after earning her doctorate, finally landing at HubSmart, Inc. Along the way, she becomes a named inventor on several

patents in the same field. While working at HubSmart, Jen receives a patent related to the use of radio-frequency identification (“RFID”) to track and manage devices through a wireless network more efficiently. Jen assigns all rights to the patent to HubSmart. HubSmart’s extensive industry experience prompts the company to create a product that combines the patented technology with HubSmart’s own proprietary algorithm.

Jen misses the excitement and autonomy she experienced working at her start-up so she negotiates a buy-out with HubSmart. After waiting six months, Jen reaches out to her old partner Eric to discuss an idea she has been mulling involving a unique protocol to use RFID technology to harvest energy for a sensor network. Since their unsuccessful venture, Eric has founded a successful company in the early analytics space that was acquired for $10 million.

Together, Jen and Eric discover that they are still interested in monitoring and managing energy through M2M communication solutions. Combining their expertise, they form Jen/Eric Sensource, Inc. (“Jen/Eric”), a company that focuses on developing autonomous sensors for use as an innovative energy solution in industrial manufacturing. Their invention employs RFID and an algorithmic solution to a whole sensor network to harvest energy, thereby eliminating the need for a separate energy source to power the sensors. The invention has the added benefit of dramatically improving the system’s ability to monitor resources and optimize efficiencies. Their solution also employs a protocol stack specifically



used for the M2M communication within that sensor network. Through that algorithm and protocol stack, a gigantic amount of data is generated and transmitted from the sensor network.

Jen/Eric obtains an early investment, which allows Jen to build her dream team, including retaining one of her former teammates from HubSmart. Jen and Eric use a combination of strategies to protect their IP, including applying for patent protection on part of their energy harvesting solution. Eric's experience helps them quickly go from concept to market.

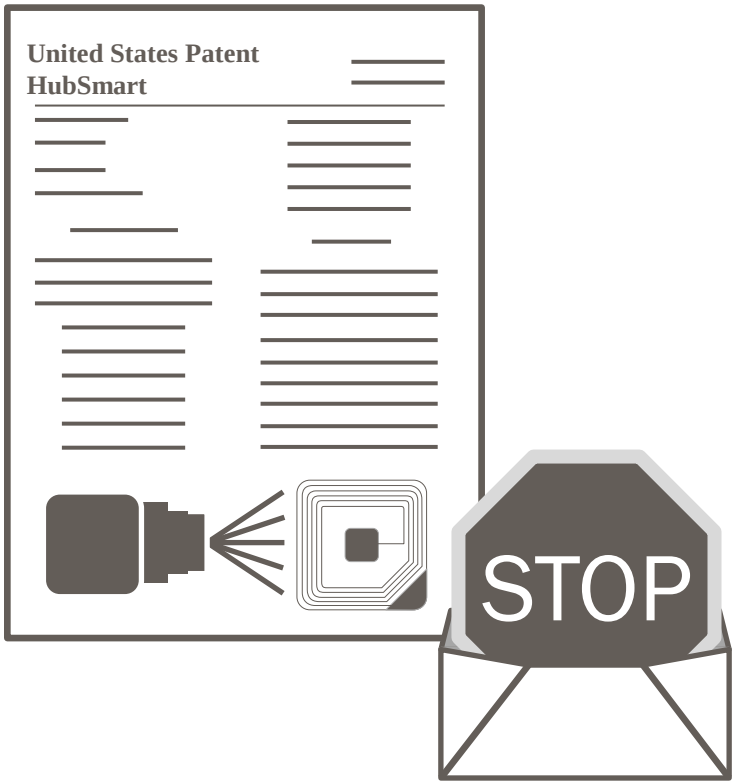
Eric's experience also leads him to make key partnerships with several companies working to define the Industrial Internet and its standards, including Big Fish, Big Ocean Manufacturing ("BiFBOM"). Jen and Eric begin to see numerous

platforms incorporate their algorithm and sensor network design, even including platforms outside of energy-harvesting, such as warehouse control, supply chain management, robotics, and others. Customers hail the efficiency of their design, both for its energy-harvesting solution and the efficiencies the underlying algorithm and protocol stack create when applied to M2M communication systems.

Within 36 months of starting the business, BiFBOM expresses an interest in acquiring Jen/Eric. BiFBOM offers Jen/Eric, and their initial investors a very compelling combination of cash and technical support to continue to develop their system. Six months after the offer, BiFBOM acquires Jen/Eric for $115 million and their ongoing commitment to technical research and development.

Trouble Brews

News of the acquisition prompts unwanted attention. HubSmart sends Jen and Eric a troubling letter claiming rights to technology within the Jen/Eric sensors. HubSmart alleges that the HubSmart team member Jen hired away participated in the wrongful IP use. Though that former HubSmart employee was part of the data science team, he tells Jen that HubSmart's claims are baloney because he materially changed the algorithmic solutions he previously used. BiFBOM also receives a letter from HubSmart claiming that the RFID technology the Jen/Eric sensors use infringes a HubSmart patent that lists Jen as one of the inventors. BiFBOM's General Counsel takes the demand letter very seriously, especially the language in the demand letter that claims that ***"BiFBOM's infringement of HubSmart's patented technology is ongoing and willful. HubSmart demands that BiFBOM immediately cease the use, promotion, and sale of RFID solutions incorporating HubSmart's patented invention."***



BEFORE LITIGATION:

FOUNDATIONAL CONCEPTS OF IDENTIFICATION AND PRESERVATION

Ideally, a large, multi-national company like BiFBOM would have an existing governance policy and established processes for data retention.[5] Organizations of this size most likely have the necessary people, policies, and procedures in place to identify and preserve relevant data. These companies know they need to meet the increased obligations that arise once a company gains knowledge of a dispute. Having that kind of process in place matters because failure to take adequate steps to preserve documents relevant to the dispute can expose a company to spoliation charges—which may materially prejudice the company's claims and defenses during litigation.[6]

Best practices require a thorough understanding of the people involved with the technology and the issues at the core of the dispute.

Whether the General Counsel's office has a litigation department or relies strictly on outside counsel, decisions need to be made quickly. Wherever the decision-making responsibilities reside, there must be an established chain of command for assessing and responding to the demand letter, as well as identifying and preserving information related to the alleged dispute.[7] In our scenario, BiFBOM's head of litigation would review the demand letters with an eye toward determining if the letters trigger a preservation duty. If they conclude that such a duty exists, the litigation head will then begin to coordinate an in-house legal team to conduct an investigation that identifies BiFBOM's preservation obligations and assesses the merits of HubSmart's claim.[8]

Responding to a demand letter involving the Industrial Internet involves many of the same steps and procedures required in any litigation. Upon receiving notice of a potential dispute, the individual inside the organization charged with preserving information must identify the relevant data sources and ensure the corresponding data custodians within the organization implement the appropriate litigation hold.

Best practices require a thorough understanding of the people involved with the technology and the issues at the core of the dispute. Those people may have additional information about the location of relevant documents and data. Established preservation methods can then be used to isolate and preserve that data, including ensuring that any automatic data overrides stop.

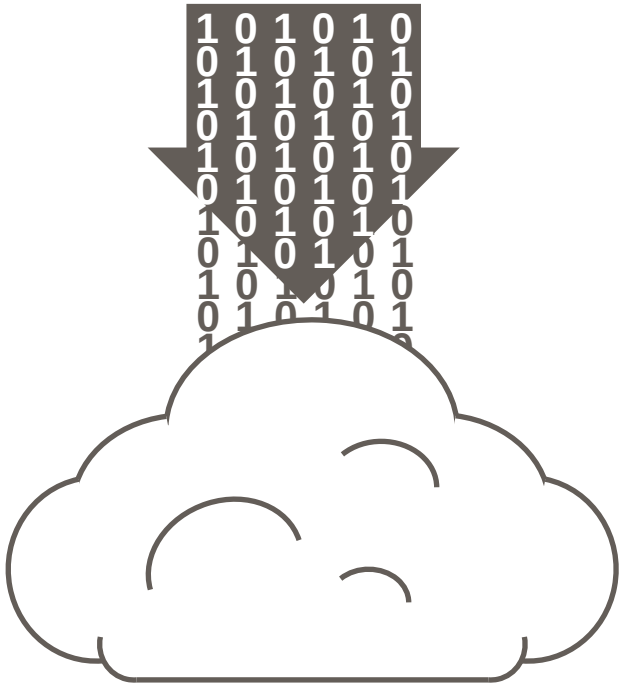
In BiFBOM's case, BiFBOM's head of litigation forwards the HubSmart demand letter to Alice Gomez, an attorney familiar with Ediscovery and BiFBOM's corporate structure and business organization. As part of her job, Alice also helps the General Counsel's office with its responsibilities regarding information governance and data retention.

Based on her experience handling IP disputes, Alice knows that the clock is ticking. Alice first interviews Jen and Eric. Knowing that the core dispute would be over IP, Alice wants to preserve any information acquired from Jen/Eric, including information related to the development of the technology such as lab notebooks, notes, and prior art used to support the patent filings. Alice also seeks out archived Electronically Stored Information ("ESI"), such as email, shared file server documents, and source code. Alice's interview with Jen and Eric (and subsequent conversations with BiFBOM's technical department) helps her determine how Jen/Eric materials are integrated into BiFBOM's IT

infrastructure. Alice knows this information is low hanging fruit and wants to act as soon as possible to preserve it. From the interview, Alice also learns the names of employees that Jen and Eric work with throughout the organization. Jen and Eric also provide an overview of how the technology works, but their explanation does not include granular details about the data flow in the sensor network.

Alice also knows that she has to contact the IT people on the ground currently using the Jen/Eric sensors. After briefly speaking with the project sponsor and the IT people supporting BiFBOM's industrial sites, Alice concludes that the sensor data she may need is stored in the cloud. Alice also reaches out to the Marketing Department and BiFBOM's Mergers and Acquisitions ("M&A") team responsible for finalizing the Jen/Eric deal.[9]

Following BiFBOM's traditional preservation protocols, Alice documents all of her conversations and preservation efforts. Within 30 days after receiving the demand letter, Alice completes her investigation into additional data sources and issues a litigation hold in line with her understanding. But Alice's litigation hold includes only sensor and related data stored within the cloud.



To meet preservation obligations, disputes involving the Industrial Internet may require more than the traditional approach of merely identifying data custodians and data sources. Those charged with managing Ediscovery and data preservation can consider formal or informal sensor-centric data mapping—identifying the litigation-involved sensors first and mapping the path of data sent from the sensor to any human interfaces, which reverses the normal people-to-data investigation used in litigation. By focusing on the sensor, the data it generates, where that data goes, and how that data is transformed into something a person can then look at and digest, sensor-centric data mapping can accurately determine the universe of data that needs to be preserved. Thus, organizations can more readily see what data exists and where potentially unexpected preservation duties may arise.[10]

In this scenario, the Jen/Eric sensors generate a significant amount of data each day because they are tasked with monitoring multiple functions, including environmental factors related to warehouse

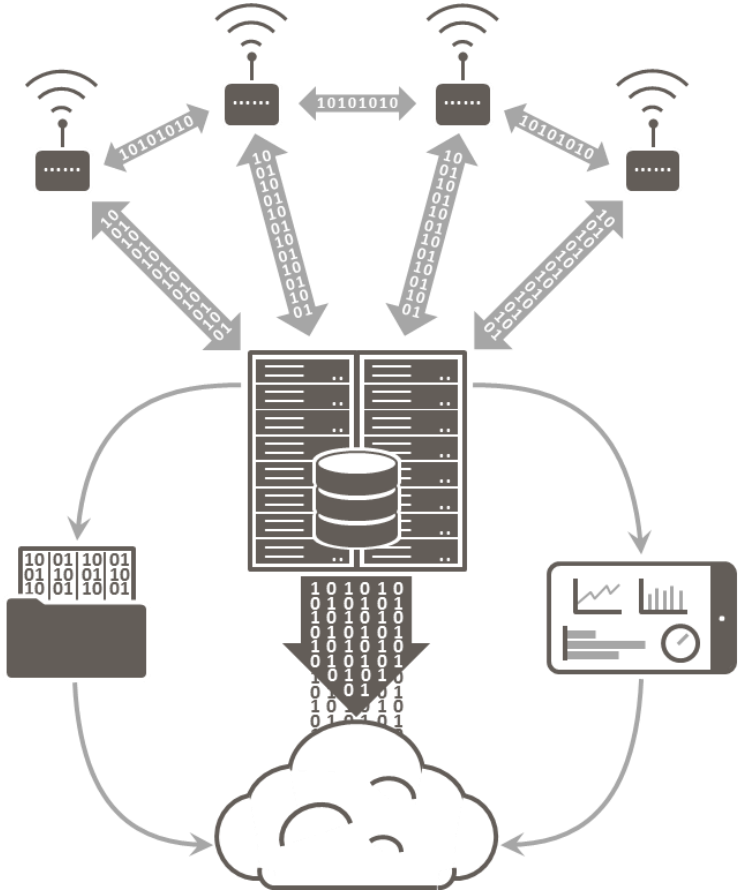
Third Party Cloud & Ediscovery

The cloud offers corporate users an inexpensive way to create, store, and access vast volumes of data. The cloud also provides an efficient and cost-effective way to scale the company's data stores to meet changing demands. However, when business disputes arise, cloud usage can create an additional layer of complexity for Ediscovery.

In litigation, cloud data is likely to be considered within a corporate owner's possession, custody, or control even though the data itself is not located on site at the corporation. As a result, courts may consider cloud data to be accessible and subject to preservation obligation. Parties should therefore prepare early in the case to identify relevant cloud data and plan to preserve that data. Early preparation may present opportunities at the Rule 26(f) conference to explain why certain segments of cloud data are inconsequential to the case and do not require preservation, thereby limiting discovery costs. As corporate cloud usage increases, expect rules and best practices for handling cloud-stored data to develop.

control, supply chain management, and robotics. Each sensor creates its own stream of operational and energy-harvesting data (“primary data”). The sensors also communicate with each other by sending data back and forth within the sensor network (“cross-sensor data”). The algorithmic protocol then prompts the sensors to send both forms of data to a central server at regular intervals throughout the day. The sensors immediately overwrite primary and cross-sensor data once communication to the central server occurs.

From there, the central server analyzes the data packets received from the sensors and communicates its analysis to both a real-time human-interface dashboard as well as to the cloud. As part of the analytic process in the central server, raw data from the sensors is stripped from the packets and then also uploaded as a log file to the cloud to support cloud-based secondary analytics. The central server is programmed to maintain a continuously executing, 30-day retention of raw data, where Day 1 data is overwritten when Day 31 data is



collected. Central server back-ups do not include retention of the raw data from the sensors.

Once the data is sent to the cloud, additional analytic processing occurs. The cloud server compares and analyzes data streams from numerous factories and the results are sent to a human-interface dashboard. Performance adjustments for the central server or the sensors are transmitted back from the cloud to the central server, and the central server sends corresponding commands back to specific sensors that result in performance changes at the sensor level.

In BiFBOM's case, Alice's decision to preserve only sensor data stored within the cloud fails to consider the entire universe of sensor data being generated. As executed, her preliminary litigation hold fails to account for data being generated by the sensors, the central server, and the data output to the human-interface. Although complex, this level of understanding and detail may be necessary in cases involving data generated in an Industrial Internet setting.[11]

When a dispute involves the Industrial Internet, don't settle for the traditional approach of focusing only on potential custodians for a litigation hold. In addition to fulfilling your obligations relative to the identification of key players and data sources, utilize a "Day in the Life of the Data" workflow mindset to uncover where relevant data may be generated, sent, or processed, and whether that information must also be preserved.

Be prepared to develop innovative approaches for storing Industrial Internet data identified for preservation. Possibilities include the cloud, a secondary server, and/or a network-attached storage ("NAS") device.

DURING LITIGATION:

USING CASE LAW AND COMMENTARY AS A GUIDE FOR PRESERVING EVIDENCE

Ediscovery efforts in the period following a demand letter usually focus on maintaining the *status quo.* A litigation hold interrupts regularly scheduled corporate data overwriting and retention protocols and keeps potentially relevant data intact. Maintaining that data in response to the possibility of litigation can be an effort that continues for weeks, months, and in some instances, years. The length of this period depends on the parties and, sometimes, what they chose to do in the interim. The most customary practice involves the receiving party issuing a denial of the alleged infringement while also beginning to formulate a defensive position to be ready should the dispute progress. Once a Complaint is filed, however, the Ediscovery landscape shifts.

Big Data in Ediscovery

Today, data-driven tools like Analytics, Early Case Assessments, and Technology Assisted Review already help practitioners meet Ediscovery challenges. Ongoing developments in the industry seek to address litigation's ever-growing data volumes while improving process efficiency and quality. Advancements from technologies like automation, machine learning, and artificial intelligence will likely provide those gains —and define the future of Ediscovery. Courts will continue to welcome Ediscovery improvements, so litigators and Ediscovery practitioners must be prepared to evolve their current practices in time with the changing technologies. Still, for these new tools to work best, someone will need to understand the data at issue, its source, and purpose in the dispute. Thus, Ediscovery practitioners will continue to play a crucial role in understanding clients' businesses and data.

The landscape changes in our scenario when HubSmart files a Complaint accusing BiFBOM of patent infringement. Then, in BiFBOM's case, the individual charged with overseeing the litigation should review the Complaint and immediately make several decisions, including who will serve as outside counsel. Counsel will usually review the scope of the original litigation hold considering the newly filed Complaint and make the necessary changes, such as adding additional data custodians implicated by the allegations in the Complaint.

At the same time, outside counsel will begin to formulate a defense. That counsel should work with BiFBOM to find the individuals and documents needed to support any affirmative defenses, counterclaims, and counter-actions, which may expand the scope of the litigation hold. Ideally, counsel would then bring in experienced Ediscovery consultants to craft a strategy for document collection and production, *in advance* of any document requests, and seek their guidance on how the discovery process can be made more efficient and cost effective.

In the BiFBOM case, after reviewing the Complaint with outside counsel, Alice concludes that she needs to expand the original litigation hold to include additional members of the Jen/Eric team. Following this activity, BiFBOM files its Answer, along with a Motion to Dismiss. Here, the BiFBOM legal team decides not to challenge the HubSmart patent in an *Inter Partes* Review with the Patent Trial and Appeals Board, because such a proceeding would put Jen in the position of trying to invalidate her own patent.

If the district court decides that the case will proceed, Ediscovery efforts will heat up. The parties will make their initial disclosures regarding custodians and key sources of information in the case. What happens next depends upon the specific venue of the case and the individual practices of the judge, because different courts impose different obligations with varying timelines.

Accordingly, when the parties finally have their first Meet and Confer depends on each court's established practices, though per Rule 26(f)(1), the Meet and Confer must happen no later than 21 days before the Rule 16 scheduling conference.[12] Once scheduled, the court brings the parties together to create an initial schedule for discovery, define ESI protocols, and consider the scope of Protective Orders, if needed. Specific Ediscovery problems may arise at this juncture, but this initial meeting more frequently covers process and procedures. Because of the discovery complexities inherent in today's data sources, especially in an Industrial Internet environment, early cooperation between the parties is key. The Federal Rules and guiding commentary were rewritten in 2015 to emphasize and codify the parties' responsibilities with respect to cooperation and proportionality.[13]

These changes should prompt the parties to come to the table with substantive information to move discovery forward. In this hypothetical, HubSmart's counsel should make clear that they will be seeking raw data from the sensors, and not just from the cloud—and this correspondence can occur even before the initial Meet and Confer.[14] This would alert Alice and the BiFBOM team to preserve additional data, such as the data generated by the sensors and the central server. HubSmart's failure to ask for raw sensor data at the Meet and Confer may prejudice their ability to later demand that BiFBOM produce such data, especially during a discovery dispute.[15] More importantly, relevant data may ultimately be overwritten by normal business processes if such notice does not occur.

Discussing discovery demands for sensor data

would also give BiFBOM an earlier opportunity to determine whether its efforts to preserve, collect, and examine the raw sensor data are proportional to the case.[16] Proportionality of requests has been a primary focus of the recent Amendments to the Federal Rules and best practices.[17] As courts look to shape Ediscovery parameters for the Industrial Internet, they will look to those revisions for guidance on how to handle issues regarding proportionality, such as the obligation to preserve back-ups when there is reasonable anticipation of litigation, or whether such preservation creates a significant and/or expensive burden.[18] In addition, courts will also certainly seek guidance from earlier decisions involving complex, large-scale discovery situations.[19]

In one representative case, *Pippins v. KPMG LLP*, plaintiffs in a putative class action requested that defendant KPMG preserve the hard drives from all 2,500 potential plaintiffs in the class.[20] Because preservation of each hard drive would cost $600, KPMG argued the total $1.5 million preservation bill would "swallow the amount at stake."[21] KPMG complicated the situation by using a previously issued discovery stay as a shield to prevent the plaintiffs from looking at even *one* of the involved hard drives. Thus, when the parties could not reach an agreement for a protective order regarding KPMG's preservation duties, a frustrated magistrate and affirming district judge required KPMG to preserve all 2,500 hard drives.

The *Pippins* court explained that proportionality does not "create a safe harbor for a party that is obligated to preserve evidence but is not operating under a court-imposed preservation order."[22] Rather, proportionality "may prove too amorphous to provide much comfort to a party deciding what files it may delete or backup tapes it may recycle" before that party files a motion for protective order "seeking to have a court define its preservation obligations."[23] As a result, the court advised that "prudence favors [either] retaining all relevant materials . . . or swiftly moving for a protective order."[24] With BiFBOM facing damage exposure north of $100 million, extensive and/or expensive discovery burdens are more likely to be seen as appropriate.

Requests for Production – Plaintiff's First Request for Production

Requests for Production help shed light on whether the original litigation hold properly identified the scope of relevant material. Ediscovery has matured out of its initial days of uncertain obligations and cautionary tales of spoliation. Now, particularly under the new proportionality standards enunciated in Rules 26(b)(1) and 37(e), parties have an obligation to approach discovery with an eye towards reasonableness.[25] Thus, the contours of discovery of standard ESI depend on the nature of the dispute, the issues involved, and developed Ediscovery practice.

Inevitably, it seems the parties will end up before the judge or presiding magistrate to contest and define discovery obligations involving Industrial Internet data.

So, what about requests that implicate the terabytes of data generated by Industrial Internet enabled factories? For example, HubSmart's First Request for Production could broadly seek "all data generated by the Jen/Eric sensors." Remember that Alice did not issue a hold at the sensor level—or even the central server level—based on her understanding that all relevant data exists in the cloud. Nor did she preserve data that goes to the human-interface dashboard. Absent any early disclosure by HubSmart's counsel about the necessity of such sensor data, HubSmart's Request for Production places BiFBOM on notice for the first time that HubSmart intends to take the dispute to the sensor level. As a result, BiFBOM must now craft a strategy to respond to HubSmart's request, meet discovery obligations, and sufficiently preserve data in the event the court orders them to comply with HubSmart's request.

BiFBOM's counsel should recognize that, though unintentional, the failure to preserve data from the sensor and central server creates risk for BiFBOM. In *Brown v. Tellermate Holdings Ltd.*, the defendant's failure to preserve data it controlled but stored in a third-party provider's cloud-based application ended in preclusion of a critical

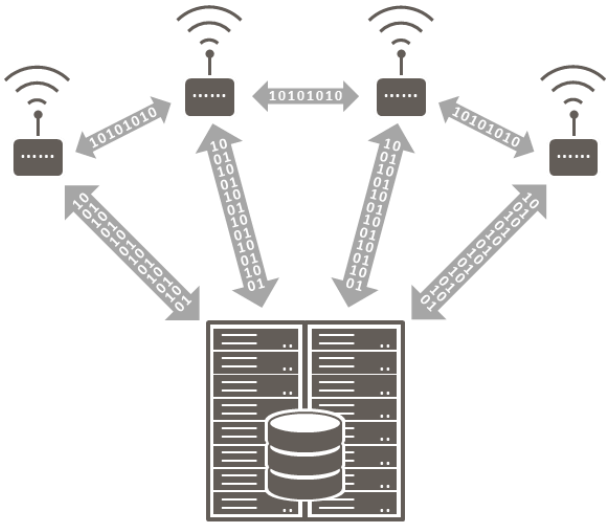
defense.[26] The sanction came about in large part because of significant and repeated bad conduct by both the defendant and its counsel. Nonetheless, the *Tellermate* court said "[t]he integrity of the [cloud-based data] is just a different side of the same coin as the failure to produce it. Both shortcomings were premised on the basic inability to appreciate whose information it was and who controlled it." Though the egregious factual circumstance in play in *Tellermate* makes it distinguishable from the situation facing BiFBOM, it offers aggrieved plaintiffs arguing inadequate preservation certain language that can bolster claims regarding data preservation responsibilities despite new data storage—and potentially data creation—environments.

Considering the risk presented by *Tellermate* and similar decisions, BiFBOM has an interest in "playing nice" when responding to HubSmart's demand for sensor data. First, Alice should work with BiFBOM's IT department to preserve data from the sensors and the central server and determine what, if any, preservation efforts should be directed at the human-user dashboard.[27] Then, BiFBOM should approach HubSmart during a Meet and Confer to address how to get HubSmart enough information to satisfy BiFBOM's discovery obligations. For example, BiFBOM could propose producing the ongoing log files. If that doesn't work, BiFBOM could offer to produce 30 days of raw data along with the log file with the agreement that, if HubSmart concludes the log is insufficient, it will bear the burden of showing why the log is inadequate.

If the parties cannot agree, the dispute will likely be presented to the court and BiFBOM's actions above provide ammunition for it to argue it has satisfied its obligation to act reasonably under the new rules.[28] Inevitably, it seems the parties will end up before the judge or presiding magistrate to contest and define discovery obligations involving Industrial Internet data. Unfortunately, regardless of its efforts at this stage, BiFBOM will have to come clean about its inability to produce sensor data for the period that predates HubSmart's Request for Production.

HubSmart and BiFBOM spend months fighting about preserving, collecting, and analyzing the sensor data. HubSmart rejects BiFBOM's proposal that HubSmart pay for the analysis of a month's worth of sensor data. HubSmart argues that it is entitled to more data. The parties appear before the court on motions. The court ultimately decides that BiFBOM's plan is reasonable and that HubSmart must pay for the analysis. But HubSmart uses the argument as a chance to inform the court of BiFBOM's failure to preserve data from the sensors and central servers—and the possibility that the harm caused by that failure may warrant spoliation sanctions.

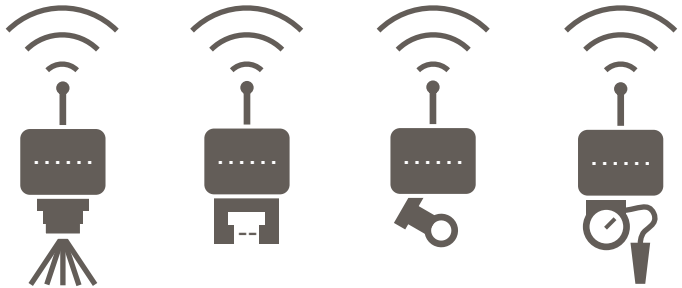
Along the way, HubSmart and BiFBOM agree on how sensor data is to be produced. However, reviewing the data will present problems for both sides. Unlike traditional ESI such as emails and patent applications, which can be rendered into a form easy to understand and review, sensor data requires a different, more experienced, and likely significantly more expensive approach for review and production. Disputes involving Industrial Internet sensor data will require the help of data scientists, much like current source code reviews. This will require identifying experts earlier and serve to make the cost of Industrial Internet Ediscovery more expensive.



In BiFBOM's case, HubSmart's expert alleges that the data logs are insufficient because the logs do not reveal a key feature of the algorithm—the self-corrections the sensors made during the periods between reporting to the central server.

HubSmart takes the position that, coupled with the failure to maintain the data, these changes hinder its ability to prove a key claim element and that it is therefore entitled to sanctions for spoliation. HubSmart also asks the court to make an adverse inference with respect to that claim element as a sanction. BiFBOM and Jen/Eric have other defenses, but an adverse inference would deeply damage their main defense and the possibility of a quick exit. In their responsive pleading, BiFBOM contends that the 2015 amendment to Rule 37(e) makes clear that spoliation sanctions should not occur unless the court determines either that a party was prejudiced by the "loss of information" or upon a showing of an "intent to deprive another party of the information's use."[29] They submit an affidavit from Alice regarding her efforts to preserve the data upon receiving the demand letter and other efforts taken to improve and increase the scope of the litigation hold. Both sides use case law decided after the recent amendments to the discovery rules to support their positions.[30]

Disputes involving Industrial Internet sensor data will require the help of data scientists, much like current source code reviews.



Court's Order on Spoliation

Almost two years after the dispute begins, the judge denies the motion for sanctions. Unfortunately for BiFBOM, however, the court's order explicitly noted key concessions the BiFBOM data scientist made during the discovery hearing regarding the actual operation of the sensors and data storage within the sensor system. These concessions make it much easier for HubSmart to prove infringement. Considering the costs of litigation and the easily ascertainable value of Jen/Eric reflected by its acquisition cost, BiFBOM ultimately makes the painful but practical decision to settle the litigation with HubSmart. The ability to get the deal done by year-end also offers some appealing tax benefits. As a result, BiFBOM agrees to pay both a lump sum and quarterly royalty payments under an ongoing licensing arrangement. Moving forward, BiFBOM recognizes it needs to adjust its protocols and procedures to be ready to respond to Ediscovery in the new Industrial Internet environment.

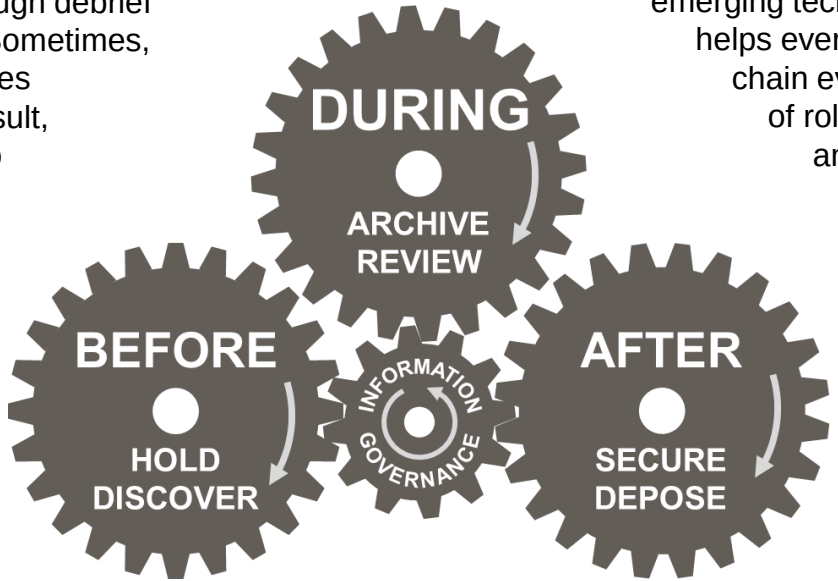
Given the updated *Sedona Principles'* recognition of how new data sources will impact proportionality, consider moving for a Protective Order that seeks to set data retention responsibilities and define production methodologies as soon as possible in Industrial Internet litigation. Doing so protects the inherent value of the data and may limit the burdens associated with ongoing preservation and production of terabytes of data.

AFTER LITIGATION:

ASKING THE RIGHT QUESTIONS

No matter the size of the company or the ultimate result, it makes good sense to take the time to do a thorough debrief after litigation concludes. Sometimes, when internal process issues contribute to a negative result, those involved may wish to move on to avoid finger-pointing or outright blame. But analyzing what Information Governance and retention practices worked—and what needs adjustment and revision—offers multiple benefits.

First, it highlights any gaps in the current governance and retention policies regarding existing and emerging technologies. Second, it helps everyone in the preservation chain evolve their understanding of roles and responsibilities and engenders more critical thinking for future conflicts. Finally, and perhaps most importantly, this analysis provides the basis for organization-wide good data hygiene and offers a clear path forward for the company's Information Governance.



Communicate the Resolution

Though seemingly evident, communicating the resolution often gets overlooked. Especially in large organizations with many moving parts, those who ultimately craft a negotiated resolution or win (or lose) a court-ordered one, may forego or forget to share the ultimate result with those involved in the case.

But communicating outcomes can serve as the best first step to identifying needed changes to data protocols and litigation hold procedures and reinforcing those governance practices and processes that worked. Because no operating manual or resource yet exists for making Industrial Internet Ediscovery work, documenting early successes and failures will help companies accelerate their learning curves in this domain.

Proper communication should highlight any compliance efforts or retention strategies that worked well so that others in the organization can implement them moving forward.

In the BiFBOM scenario, the General Counsel leads the efforts, but still empowers Alice to keep asking the questions. The General Counsel should understand that Ediscovery issues that arise in litigation reflect a systemic issue rather than any specific failing on Alice's part. The miscommunication that arose in Alice's initial interviews with Jen and Eric should result in an immediate change. Alice should document her misunderstanding regarding the operation of the sensor system and its data universe. In response, Alice should add questions regarding new data sources and custodians to her process checklist for Ediscovery efforts involving acquired technology companies, especially in the Industrial Internet space.

Review Roles

When it comes to the Industrial Internet, a review of relevant roles should be conducted and should include both traditional data custodians as well as those individuals who were identified during the sensor-centric analysis. Taken together, these custodial techniques provide a solid foundation for meeting litigation hold preservation obligations.

Identifying the job function performed by those involved in any kind of litigation provides a roadmap of where to start and who needs to be contacted when similar issues arise. The BiFBOM analysis revealed an individual in each factory where the sensors are deployed with oversight analysis for the human-user dashboard. Putting that role on a map of Industrial Internet key players will help create a partnership between the General Counsel's office and the factory floor to identify relevant data as well as possible strategies for preservation.

Similarly, a role-based analysis will help both employees and outside Ediscovery service providers charged with data collection in Industrial Internet settings understand the many new jobs and responsibilities being created by the Industrial Internet. As IT merges with the operational technologies on the factory floor and in other Industrial Internet settings, traditional IT department inquiries need to expand to the Industrial Internet's universe of app developers, site-based hardware, and cloud-based analytics capabilities. Understanding those responsible for the data at each node ensures the effectiveness of a litigation hold involving technologies within the Industrial Internet's emerging ecosystem.

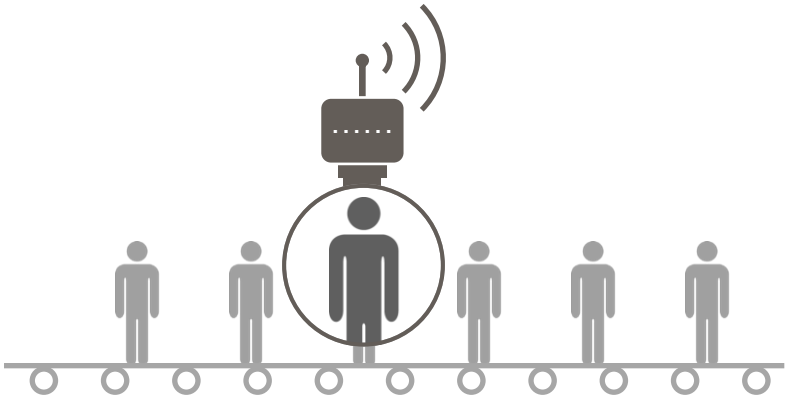
Understanding those responsible for the data at each node ensures the effectiveness of a litigation hold involving technologies within the Industrial Internet's emerging ecosystem.

After the time and expense associated with a large data collection effort, it is not surprising when companies are hesitant to take the steps necessary to release a litigation hold. But making strategic, defensible decisions to clean up any data no longer subject to the hold makes financial sense and further minimizes risk that it will need to be collected and produced in future litigation.

While companies need to anticipate any future litigation implicated by the current action, they should be careful not to let it cast too large a shadow. Beyond the significant costs associated with maintaining Ediscovery databases, doing so makes it easier for future opponents to "stumble upon" potentially helpful information that might otherwise not have been collected because it would have been dispersed per normal retention practices. It also allows those opponents to gain insight from the company's litigation history, because the way documents are stored for litigation efforts can reveal a counsel's thought processes—an outcome that should be avoided whenever possible.

…companies should actively release a litigation hold by only maintaining data within the repository that must be preserved, even if that means undoing a costly or originally burdensome effort.

Instead, companies should overcome the desire to maintain a repository, especially as mountains of Industrial Internet data are created in the future. Rather, companies should actively release a litigation hold by only maintaining data within the repository that must be preserved, even if that means undoing a costly or originally burdensome effort.



At BiFBOM, Alice should meet with the General Counsel, outside attorneys, and Ediscovery experts who handled the HubSmart litigation. This team can craft a plan that identifies the location of all preserved data and the timing of its release into normal data retention processes. Alice should also contact everyone affected by the litigation hold and identify anyone still retaining data because of the dispute. It is important to ensure that custodians are informed when it is appropriate to release their data.

Internet of Things Litigation Update

Internet of Things (IoT) litigation involving connected devices has emerged to offer a preview of the kinds of cases and claims that will follow sensor-enabled devices. Data from sensor-enabled objects—like personal activity trackers, home automation/security systems, and "smart" cars—has also taken center stage in many disputes. Some disputes involve product defects. Others were filed against product manufacturers who either failed to disclose cybersecurity risks or sold products with cybersecurity risks built into their source code or operating system. While those cybersecurity claims have all been dismissed to date for lack of standing, we can expect courts to weigh in soon about how litigants should handle the vast data streams generated by consumer IoT devices, especially as cybercrimes and hacking continue to proliferate. Those decisions, in turn, will influence what happens with Ediscovery in the IIoT.

Also as part of case closing efforts, outside counsel should draft a letter confirming the return and destruction pursuant to the Protective Order of all BiFBOM data in HubSmart's possession.

In addition, as part of their post-litigation analysis, BiFBOM will want to assess how it can proactively handle data from newly acquired companies, whether any cross-matter management issues exist, and whether any training protocols need to be changed. For now, known best practices for all data can serve as good guidance for how to address each of those areas with respect to the Industrial Internet.

As acquisitions and innovative joint ventures fund ongoing advancements in the Industrial Internet, consider using "lessons learned" from litigation to assess M&A deals as part of the standard information governance practice. For example, document where and how any acquired company keeps its data, especially data preserved for any ongoing litigation. That way, if that acquired company (or its product) ends up being the subject of litigation, you know where to find relevant data. Doing so helps head off some of the potential issues that may appear in the future.

Conclusion

The exact parameters of future Ediscovery battles involving data from the Industrial Internet depend, of course, on the nature of the dispute involved. While sensor data may prove essential to establishing whether a proprietary invention has been infringed, it could also play a critical role in many other kinds of litigation. Think about a case involving a contested insurance coverage claim for business interruption losses in a sensor-enabled factory. Or consider a breach of contract dispute over performance of the sensors themselves—scenarios we intend to explore in the future. Whatever the underlying nature of the claim, the early days of general Ediscovery litigation offer a cautionary tale to those first up to bat on Industrial Internet Ediscovery issues. As courts struggle to adapt old rules to recent technologies, those first litigants are sure to face increased costs and expenses as responsibilities for preservation, collection, and production get defined for new data realities.

Managing that expense means adapting current Ediscovery best practices to that reality. In addition to identifying the people who control relevant information, it will become increasingly important to look also to the devices that create the data. Doing so will ensure a clear understanding of the data stream and outputs that can prove crucial to a dispute—and provide assurance that discovery obligations have been met. In the end, success may depend on finding a legal team that understands both the technology at the heart of the Industrial Internet as well as the goals, principles, and practicalities of Ediscovery in today's complex and constantly evolving litigation environment.

This article is authored by Marla Butler, Li Zhu, Michael Dirksen, and Vivian Enck. Their full biographies can be found on page 32. The opinions expressed herein are those of the author(s) and do not necessarily reflect the views of the firm or its clients. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] A 2015 study of 350 manufacturing companies asked about plans to use the Internet of Things to improve business performance. Two-thirds of the companies had either a plan to leverage the technology or were in various stages of implementation, but only 10% of those companies were already in full utilization mode. The MPI Group, *The Internet of Things Has Finally Arrived (Unfortunately, Most Manufacturers Aren't Ready)*, Rockwell Automation, (2015), http://www.rockwellautomation.com/resources/downloads/rockwellautomation/pdf/capabilities/connected-enterprise/mpi-iot-study.pdf; *The MPI Internet of Things Study*, BDO, (2016), https://www.bdo.com/getattachment/7ec3c316-1df2-4b02-88f7-6b4770cc81f8/attachment.aspx?2016-Internet-of-Things-Study-WEB.pdf.

[2] *See* Industrial Internet Consortium Infographic, *Industrial Internet: The $33 Trillion Opportunity That is Happening Now*, http://www.iiconsortium.org/images/case-study-posters/Industrial-Internet-Infographic.jpg. Maybe it goes without saying that manufacturing companies that have begun to implement components of the Industrial Internet in their business are the ones that have realized the potential impact that such technology can have. GENPACT Research Institute, Industrial Internet of Things (IIoT) Research Executive Summary, (2016), http://www.genpact.com/downloadable-content/insight/industrial-internet-of-things-iiot-research-executive-summary.pdf.

[3] *EDRM Model*, (2014), http://www.edrm.net/frameworks-and-standards/edrm-model/.

[4] The people, companies, and litigation used for illustrative purposes here are entirely fictional. Any resemblance to any actual litigants or disputes is purely coincidental.

[5] As an ongoing part of the Ediscovery process, governance issues for the Industrial Internet will be discussed here as part of lessons learned in the "After" section—particularly consideration of how governance policies may need to be updated to address the specific preservation challenges involved in the Industrial Internet.

[6] *See Cat3, LLC v. Black Lineage, Inc*., 164 F. Supp. 3d 488, 500 (S.D.N.Y. Jan. 12, 2016) (costs and evidentiary sanctions awarded under revised rule standards where plaintiffs both intentionally manipulated the email produced with the intent of "gain[ing] an advantage in the litigation" and engaged in conduct "not consistent with taking 'reasonable steps' to preserve the evidence.").

[7] *Victor Stanley, Inc. v. Creative Pipe, Inc.*, 269 F.R.D. 497, 521 (D. Md. Sept. 9, 2010).

[8] *Zubulake v. UBS Warburg LLC,* 220 F.R.D. 212, 217-218 (S.D.N.Y. Oct. 22, 2003).

[9] *Pension Committee of the University of Montreal Pension Plan, et al. v. Banc of America Securities, LLC, et al.*, 685 F. Supp. 2d 456 (S.D.N.Y. Jan. 15, 2010 as amended May 28, 2010).

[10] *Below v. Yokohama Tire Corp*., 2017 U.S. Dist. LEXIS 27280 (W.D. Wis. Feb 27, 2017). This products liability case alleging defective tire manufacturing as the cause for an automobile accident highlights that ESI can even be found in a 2005 pickup truck. Here, plaintiffs failed to preserve, *inter alia*, an electronic data recorder that defendants allege would have contained information valuable to their defense of the case. The Court noted plaintiffs' counsel "should have taken additional steps to ensure that the truck (or at least potentially key evidence) was preserved."

[11] Fed. R. Civ. P. 37(e) advisory committee's note to 2015 amendment. (The "rule recognizes that 'reasonable steps' to preserve suffice; it does not call for perfection.").

[12] Fed. R. Civ. P. 26(f)(1).

[13] Fed. R. Civ. P. 1 advisory committee note 2015 amendment. “Parties jointly share with the court the responsibilities of securing ’a just, speedy, and inexpensive determination of every action.’”

[14] Fed. R. Civ. P. 26(d)(2). The recent changes made to Rule 26(d)(2) now even allow Fed. R. Civ. P 34 requests to be propounded in advance of the Meet and Confer.

[15] *See ChriMar Systems v. Cisco Systems*, 312 F.R.D. 560, 2016 WL 126556 (N.D. Cal. Jan. 12, 2016). In *ChriMar*, the plaintiff issued an overbroad Fed. R. Civ. P. 30(b)(6) deposition notice and then failed to Meet and Confer regarding the same. Acknowledging the amendment to Fed. R. Civ. P. 26(b)(1), the court said that a test exists that “balances the proportional needs of the case…considering the importance of the issues at stake in the action[,] . . . the importance of the discovery in resolving the issues, and why the burden or the expense of the proposed discovery outweighs its likely benefit.” The Court also noted that, had the plaintiff timely responded to defendant’s request for a Meet and Confer, “the parties might have been able to agree to a narrowed version of the topic in advance of the depositions.”

[16] *See Solo v. United Parcel Serv. (UPS). Co.*, 2017 U.S. Dist. LEXIS 3275 (E.D. Mich. Jan. 10, 2017). The Court found plaintiffs’ request for data on backup tapes to be “extraordinarily burdensome” where defendants offered detail into the costs associated with responding to the request and where defendants also offered an alternative approach to comply.

[17] *See* Fed. R. Civ. P. 26(b)(1) (“Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and *proportional to the needs of the case,* considering the importance of the issues at stake in the action, the amount in controversy, the parties’ relative access to relevant information, the parties’ resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit.” (emphasis added)); *see also The Sedona Conference, Cooperation Proclamation*, 10 Sedona Conf. J. 331 (2009 Supp.) *and Mancia v. Mayflower Textile Servs. Co*., 253 F.R.D. 354, 363 (D. Md. Oct. 15, 2008) (citing Sedona Proclamation). *See also,The Sedona Conference, The Sedona Principles, Third Edition*: *Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, (March 2017 Public Comment Version), https://thesedonaconference.org/publication/The%20Sedona%20Principles.

[18] *See In re Takata Airbag Prods. Liab. Litig.,* No. 15-02599, MDL No. 2599 (S.D. Fla. Mar. 1, 2016) (Discovery dispute over redaction cites Chief Justice Roberts’ commentary in the *2015 Year End Report*, wherein Justice Roberts noted that the amendments to Rule 26 “crystalizes the concept of reasonable limits in discovery through increased reliance on the common-sense concept of proportionality.”); *see also The Sedona Principles, supra* note 17 at Cmt. 2.c. (“The parties and the court should be aware that discussions held early in the action are limited by the information available to the parties, and that proportionality may be revisited as the action evolves. The parties should summarize their discussions of proportionality and, where different, their respective analyses of the proportionality considerations in the parties’ report to the court, and be prepared to discuss any significant proportionality issues at the Rule 16(b) conference with the court.”).

[19] The Sedona Conference, in response to the December 2015 amended Federal Rules about advances in technology and ever-changing data realities, has issued updated Principles (currently in public comment form) for handling complex discovery situations. *See generally, The Sedona Principles, supra* note 17.

[20] *Pippins v. KPMG LLP*, 279 F.R.D. 245 (S.D.N.Y. Feb. 3, 2012).

[21] *Id.* at 249.

[22] *Id.* at 255 (internal citations omitted).

[23] *Id.* (internal citations omitted).

[24] *Id.* (internal citations omitted).

[25] *See* Fed. R. Civ. P. 26(b)(1); *see also* Fed. R. Civ. P. 37(e) advisory committee note 2015 amendment, (“Another factor in evaluating the reasonableness of preservation efforts is proportionality. The court should be

sensitive to party resources; aggressive preservation efforts can be extremely costly, and parties (including governmental parties) may have limited staff and resources to devote to those efforts. A party may act reasonably by choosing a less costly form of information preservation, if it is substantially as effective as more costly forms. It is important that counsel become familiar with their clients' information systems and digital data — including social media — to address these issues. A party urging that preservation requests are disproportionate may need to provide specifics about these matters in order to enable meaningful discussion of the appropriate preservation regime.").

[26] *Brown v. Tellermate Holdings Ltd.,* 2014 U.S. Dist. LEXIS 90123 (S.D. Ohio July 1, 2014).

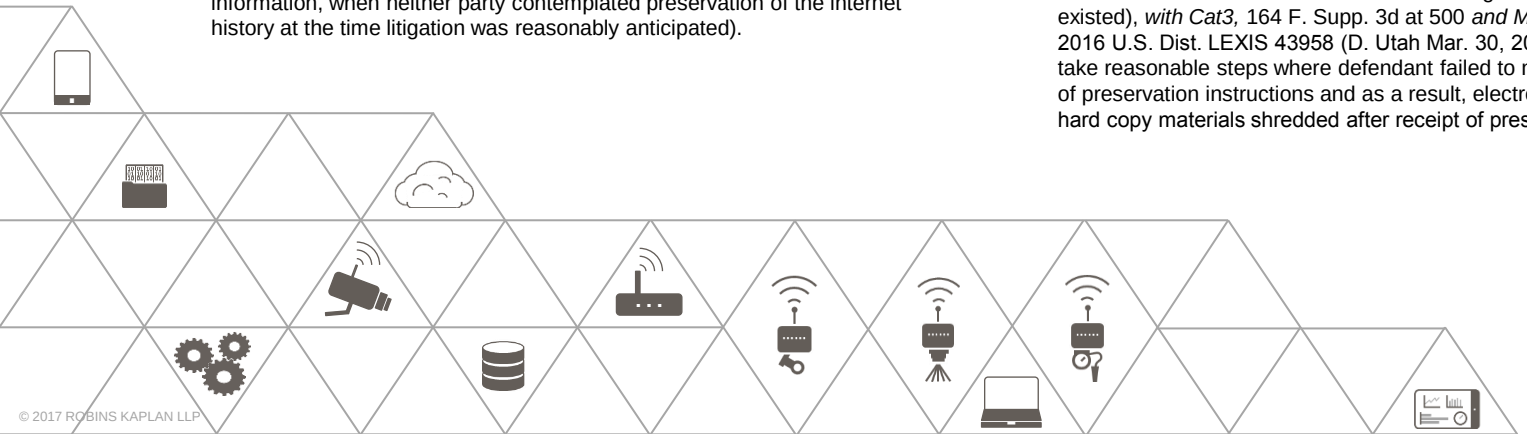
[27] Several technical approaches could be leveraged as viable solutions to the storage problem created by the massive quantities of raw data from the sensors. Possibilities include the configuration of a Network Attached Storage ("NAS") device as a component of the greater network or the use of a mirroring drive setup.

[28] *Marten Transp., Ltd. v. Plattform Adver., Inc*., 2016 U.S. Dist. LEXIS 15098 (D. Kan. Feb. 8, 2016) (Failure to preserve internet history does not warrant sanctions against a party who properly preserved all other relevant information, when neither party contemplated preservation of the internet history at the time litigation was reasonably anticipated).

[29] Fed R. Civ. P. 37(e) provides: (e) FAILURE TO PRESERVE ELECTRONICALLY STORED INFORMATION. If electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery, the court:

> (1) upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or
>
> (2) only upon finding that the party acted with the intent to deprive another party of the information's use in the litigation may:
>
> > (A) presume that the lost information was unfavorable to the party;
> >
> > (B) instruct the jury that it may or must presume the information was unfavorable to the party; or
> >
> > (C) dismiss the action or enter a default judgment.

[30] *Compare Best Payphones, Inc. v. City of New York,* 2016 U.S. Dist. LEXIS 25655 (E.D.N.Y. Feb. 26, 2016) (No sanctions against party who failed to preserve relevant information when failure occurred because of negligence rather than ill intent and curative measure to gather information elsewhere existed), *with Cat3,* 164 F. Supp. 3d at 500 *and McQueen v. Aramark Corp.,* 2016 U.S. Dist. LEXIS 43958 (D. Utah Mar. 30, 2016) (Court finds "failure to take reasonable steps where defendant failed to notify necessary individuals of preservation instructions and as a result, electronic data was deleted and hard copy materials shredded after receipt of preservation letter.").



Industrial Internet Ediscovery Team

Marla Butler - Partner
MButler@RobinsKaplan.com

A trial attorney with two decades of experience litigating complex patent and commercial cases, Marla has an in-depth understanding of the technologies and manufacturing environments at the heart of the Industrial Internet. Marla recognizes the crucial role Ediscovery will play in Industrial Internet litigation and is working now to help clients find ways to control costs, manage scale, and achieve litigation goals within the Industrial Internet's new data paradigms.

Li Zhu - Associate
LZhu@RobinsKaplan.com

Li focuses on complex patent and commercial litigation, representing both plaintiffs and defendants in a variety of markets and technical fields. Based in Silicon Valley, Li's experience includes crafting strategic solutions to the Ediscovery issues that often arise in complex data environments. This experience helped him recognize and anticipate the coming Ediscovery challenges that the Industrial Internet creates.

Michael Dirksen - Ediscovery Attorney
MDirksen@RobinsKaplan.com

Part of the Robins Kaplan Ediscovery Group, Mike helps clients align data and business realities with litigation objectives throughout the entire life-cycle of litigation. Mike's own early experience as an inventor for a corporate employer helped spur his interest in the Industrial Internet and determine how to address Ediscovery issues across the full range of disputes involving the Industrial Internet.

Vivian Enck - Ediscovery Consultant
VEnck@RobinsKaplan.com

Vivian has more than 30 years of experience in complex litigation support. Along with document management and records retention consulting, she provides the actionable strategies clients need to meet real-world Ediscovery demands. This guidance help clients fulfill Ediscovery obligations, while managing risk and costs. Vivian's best practices emphasis informs how she sees Ediscovery related to the Industrial Internet.

BISMARCK
1207 West Divide Avenue
Suite 200
Bismarck, ND 58503
701 255 3000 TEL

BOSTON
800 Boylston Street
Suite 2500
Boston, MA 02199
617 267 2300 TEL

LOS ANGELES
2049 Century Park East
Suite 3400
Los Angeles, CA 90067
310 552 0130 TEL

MINNEAPOLIS
800 Lasalle Avenue
Suite 2800
Minneapolis, MN 55402
612 349 8500 TEL

NAPLES
711 Fifth Avenue South
Suite 201
Naples, FL 34102
239 430 7070 TEL

NEW YORK
399 Park Avenue
Suite 3600
New York, NY 10022
212 980 7400 TEL

SILICON VALLEY
2440 West El Camino Real
Suite 100
Mountain View, CA 94040
650 784 4040 TEL

SIOUX FALLS
101 South Main Avenue
Suite 100
Sioux Falls, SD 57104
605 335 1300 TEL

ROBINS KAPLAN LLP
REWRITING THE ODDS