E-Discovery Operations

Tactical considerations for defensible eDiscovery

GIAC (GLEG) Gold Certification

GIAC ID# 00042

Author: Thomas Vines, GIAC.Thomas.Vines@gmail.com

Advisor: Barbara L. Filkins

Accepted: March 6, 2016

Abstract

Within the legal environment, Discovery is the process of identifying, locating, preserving, securing, collecting, preparing, reviewing, and producing facts, information, and materials for the purpose of producing/obtaining evidence for utilization in the legal process. Electronic Discovery (e-Discovery) is the application of these processes into the digital environment to collect Electronically Stored Information (ESI). Legal departments are ill prepared to deal with the digital environment of a business. Increasingly they are turning to the company's Information Technology (IT) department to identify, locate, preserve, and collect ESI. This is not break/fix work, typical in most IT operations, but a more complex set of processes. This paper explores the tactical processes necessary to comply with an increasingly demanding US Federal court system. This analysis includes the processes and controls necessary for a defensible e-Discovery program, including a review of identifying the record owner, methods for identifying, collecting, and preserving custodial data, and the management of custodian equipment.

1.0 Introduction

The tactical processes necessary to comply with an increasingly demanding US Federal court introduce a new level of complexity to the modern business. A defensible e-Discovery program must include a system of identifying record owners, methods for identifying, collecting, and preserving custodial data, and management of custodian datasets. It must include a well-documented and proven methodology concerning the creation of a data map per matter and per custodian (Schuler, 2009). Collection and preservation of data must include quality control measures and auditing, with the ability to document the chain of custody when needed (Scholtes, 2010). These processes must be repeatable and applied to each litigation event or matter, utilizing programmatic automation and auditing to improve efficiency and transparency.

Legal obligations surrounding a matter are complex. Custodians, either individuals or the company itself, share a “Duty to Preserve” (Jackson R. , 2012). The courts agree that there are no excuses for a Custodian to fail to preserve and protect electronically stored information when they have reason to believe it will be requested Electronically Stored Information (ESI). In the United States, ESI extends past the typical corporate email to forms of social media (DiBianca, 2014). Evidence in any form that a party to litigation has “possession, custody, or control” is subject to the Duty to Preserve.

The Duty to Preserve extends to the Counsel, who has the duty to understand the requirements of the Federal Rules and to explain this to the Company and the impacted workforce of the Company. There is a growing consensus that Counsel cannot adequately represent his/her client at the Federal Rules of Civil Procedure (FRCP) Rule 26(f) conference without a fundamental awareness of how the client stores and processes relevant ESI (Jackson R. , 2012). Failing to comply with the rules can lead to court-imposed sanctions, including assessment of attorney fees and costs, imposition of significant fines, issuance of adverse-inference jury instructions and even, in rare circumstances, outright loss of the case (Jackson R. , 2012).

Deciphering relevant ESI from non-relevant ESI is problematic, as is identifying where ESI is stored. Relevancy, therefore, becomes the focus of the discoverability analysis. The Attorneys work though these details in the required FRCP 26(f) Meet and Confer meetings. These meetings often set the rule of engagement for the eDiscovery collections team.

The courts have generally adhered to certain identified areas and categories of ESI considered irrelevant. Eliminating the files contained in the NRSL maintained by NIST is called "De-NISTing." This is not a perfect process. The hash values of the files change all the time due to patches, fixes, and updates by the vendor. Examples include program application files (e.g. *.exe, *.dll, *.ini, etc.), fragmented information on hard drives, RAM memory, temporary online information such as cookies or history files. The proper method for excluding these files is known as 'De-NISTing' (Practical Law, 2015). The National Institute for Standards and Technology ("NIST") publishes the National Software Reference Library ("NRSL"). The NRSL is a comprehensive listing of files distributed within software packages. This will help alleviate much of the effort involved in determining which files are important as evidence on computers or file systems (NIST.gov, 2015).

Companies are obligated to conduct an extensive search of their systems to ensure they collect all relevant data (The Sedona Conference, 2015). Determining where the relevant corporate ESI is stored can be an enormous undertaking. Custodian ESI is often stored within the company's technology environment, as well as a variety of smartphones, tablets, home PCs, and in the digital "cloud". Typical user-created information may include documents, email, databases, and other assets stored electronically. The self-evident problem of data volume and variety becomes clear at scale (Boudreau, 2010). In spite of a Company's potential lack of IT management, vendor oversight, or organizational governance, the obligation to produce relevant evidence persists (*Logtale, Ltd. v. IKOR, Inc.*, 2013).

Perfection is not required. What is required is the party's good faith and reasonableness (John L. Carroll, 2004). In fact, "courts cannot and do not expect that any party can meet a standard of perfection" *(Pension Comm of the Univ. of Montreal pension Plan v. Banc of Am. Sec, LLC, 2010*). Within that verdict, the Federal Southern District of New York decreed, "[a] party…does not have to go to 'extraordinary measures' to preserve all potential evidence." The court goes on to announce of companies that, "…litigants and their counsel will "act diligently" to "take the necessary steps to ensure that relevant records are preserved…". This places the burden of knowing the "what and where" of ESI within the company's technology environment management processes.

Figure 1 Electronic Discovery Best Practices

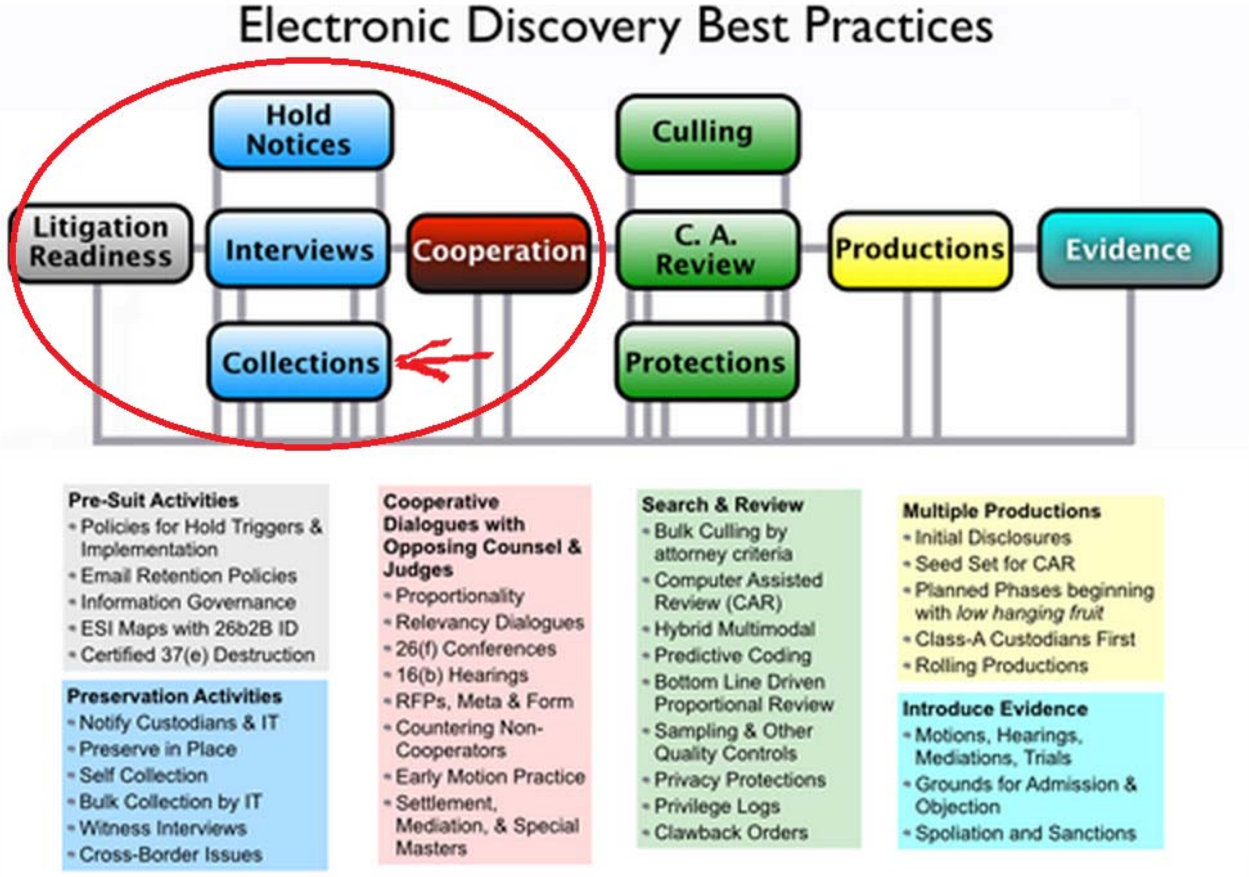


Figure 1 (Losey, 2012)

2.0 Data Mapping and What to Collect

Each of the Custodian's digital assets creates a reference point to map out where potentially relevant data may be located. This "Data Map" (Schuler, 2009) indicates location and identity of the data to be preserved as evidence. As the custodian's use of digital assets, both corporate-controlled and personally-owned, creates this map, the ability to find data (documents, email, text messages, and "any other tangible thing") relevant to the matter ceases to be a burden (Lisa M. Arent, 2002).

Interviews are necessary to find out where ESI may be stored. For defensibility, the most important thing is to ask custodians the same set of questions (Verga, 2014). Besides knowing whom the custodians are and what work they do, the interviews should identify where they store data, including: identifying equipment that houses ESI, understanding cloud storage, hosted applications, confirming how they communicate with the company, whom they communicate with, and other clarifying questions to help define the scope of the data map (Verga, 2014).

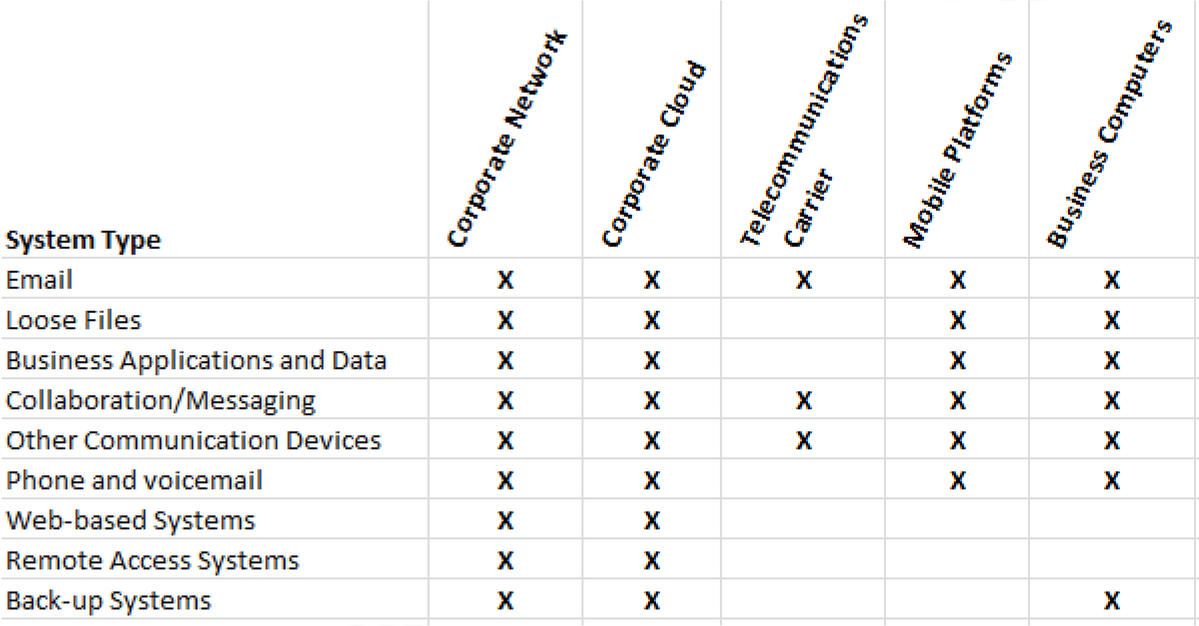
These questions and answers provide leads to other questions, all of which will help define the Company's protocol and procedures to practice eDiscovery in a defensible manner. In every step toward these protocols, it is critical to involve the Attorneys who lead the eDiscovery efforts. They must direct efforts concerning eDiscovery. Likewise, the Attorneys will manage a broad array of preservation activities and may need to understand the company's efforts to fulfill its "Duty to Preserve." This early case assessment knowledge of the data map sets the stage for Attorneys to have a cooperative dialogue with opposing counsel and judges involved with the matter. These efforts can inform proportionally agreements, define relevancy of ESI methodologies, early motions and even settlements and mediation.

ESI also resides within systems created by applications, infrastructure, platforms, and the like. For some company's corporate email, calendar and contacts may be located within the corporate network or cloud. Telecommunication carriers often retain call logs, Short Message Service (SMS), Multimedia Messaging Service (MMS), voicemails, and GPS data that go beyond data stored on the local device. Mobile platforms, like smartphones, may contain loose files of user-created music, pictures, movies, videos, user-synced documents, text notes, and other potentially relevant data. Lastly, the employees' corporate computer may have other loose files. This location may contain a rich source of locally saved user-created email, source documents, backup logs, as well as photos, music, mobile platform synchronized data and other information.

These five possible locations, Corporate Network and Cloud, Telecommunication Carrier, Mobile Platforms, and staff business computers each have their own data maps. (See Table 1, System Type and Location Matrix.) Each location may require its own tool sets, expert knowledge, and methodologies to collect data. Within these four locations, there may be as many as ten data types worth investigating. The ten include: Email, Loose Files, Business Applications and Data, Collaboration/Messaging, Other Communication Devices, Phone and voicemail, Web-based Systems & Cloud Computing, Remote Access Systems, and Back-up Systems.

Each system type requires pre-litigation analysis to determine accessibility. Accessibility determines whether data sources are in scope. Companies with multiple locations and multiple systems types may have as many as 34 different technical environments to investigate and data map. For each Location within the matrix in Table 1, there are specific laws to consider. While a complete review is beyond the scope of this paper, a substantial review of the capabilities and techniques on how to exhume data from these locations are subcomponents within the comprehensive pre-litigation audit with IT staff and vendors.

Table 1 System Type and Location Matrix



System Type	Corporate Network	Corporate Cloud	Telecommunications Carrier	Mobile Platforms	Business Computers
Email	X	X	X	X	X
Loose Files	X	X		X	X
Business Applications and Data	X	X		X	X
Collaboration/Messaging	X	X	X	X	X
Other Communication Devices	X	X	X	X	X
Phone and voicemail	X	X		X	X
Web-based Systems	X	X			
Remote Access Systems	X	X			
Back-up Systems	X	X			X

A review of the case law reveals that the courts have a very dim view of a company's inability to produce relevant data. If a company's information management system or the lack of one contributes to eDiscovery difficulty, it is very unlikely to persuade the courts for leniency (Lexis Nexis, 2008). A critical process for a successful information management system is pre-vetting these environments and pre-establishing procedures to identify, collect and preserve data from the appropriate system types and locations.

This is especially true with suspending or interrupting automatic retention features of electronic information systems or so-called auto-delete environments (Anne Kershaw, 2015). Many of these locations and systems may have auto-delete functionality enabled. For the custodians under legal hold, auto delete must be disabled. Within the legal community, it is well understood that the suspension of auto-delete functions must be configured to preserve potentially relevant ESI (Lisa M. Arent, 2002).

Some companies have learned this the hard way *(Mosaid v. Samsung, 2004*) (*Apple Inc. v. Samsung Electronics Co. Ltd et al, 2012*).

The suspension of auto-delete seems simple on the surface but complexities abound. Depending on the environment, location and system-type activities, the amount of coordination is directly proportional to the system complexity. A formal process may be required to assure education of vendors and staff and proper gathering of evidence. A cascade of actions needs to be aligned from inside counsel, to staff, to vendors and cloud providers to assure success. Performing these activities may not be possible before the auto-deletion claims potentially relevant data. A significant delay in disabling auto-delete may put companies in gross negligence territory (Griffin, 2006). *In Broccoli v. EchoStar Communications Corp* (229 F.R.D. 506, 512(D. Md August 4, 2005), the defendant drew the ire of the court by delaying 21 days the suspension of auto-delete in the equal employment opportunity case.

The Courts and their special eDiscovery experts' adjudicate different auto-delete mechanisms based on the merits and capability of the system(s). Auto-delete mechanisms differ by system type. Because Judges have long had to deal with email, some cases go back to the early 1990's; they are more familiar with the general capabilities of those systems. There is a vast amount of case law dealing with email as ESI. Email auto-delete is very easy to turn off and control, while auto-delete for loose files or applications in the cloud is more difficult. Safeguarding ESI located in complex systems from auto-delete takes longer and requires coordination. Where ESI is stored in distant locations and under the control of a vendor, the procedures and time necessary to stop auto-delete may take even longer.

Defensible eDiscovery requires significant pre-planning and analysis. Beyond that the company must have four additional well-functioning processes for each of the ten general system types. The processes should include; 1) establishing an accurate data map; 2) tracking and monitoring IT Infrastructure that may house ESI so that evidence collections can take place in a timely manner; 3) detecting the use of non-traditional data map locations, and; 4) ensuring auto-delete functions have been controlled to assure no loss of potentially relevant ESI.

2.1 Email Architecture

Email is the most requested eDiscovery data type with the longest record of accomplishment. Many cases have hinged on a single "smoking gun" email as GM, Microsoft, Samsung, and others have learned. The courts as early as 1995 set many rules concerning the proper collection and management of email data subject to legal hold (Lexis Nexis, 2008). Emails consist of attributes that must be maintained and preserved: addresses, header information, the message body, attachments, and metadata.

To track and monitor the relevant email evidence, it is important that a comprehensive evaluation of the entire email system(s) be performed. Understanding the email architecture is crucial to eDiscovery teams, especially as this knowledge can support a more timely response to demand. The eDicovery team must also understand the type of email service mix the company utilizes and its many dependencies to assist with the collection of potentially relevant email. .

The following questions can help to diagram and ultimately draw out the data map for the company's email architecture to support a data map in order for a collection to take place. Does the company own and control the mail or does the employee (Sullivan, Bob, 2013)? Does the email server have an auto-delete setting or a retention policy to delete mail older than a certain period? Does the email server have search capability? Can the email be exported so another system can search it? Can the email server archive the mailbox? Can that file be preserved in a safe location for further evaluation?

The user's mailbox brings other decisions to the forefront. Is the email only on the server? Is the email only on the client? Is it in both places? Can the mailbox be made 'read-only' to the user, to stop user deletes and enable preservation in place? How can a backup of the mailbox be made? What is the business impact of these decisions? Will the user be without mail until the collection is complete?

Most companies do not restrict the use of web-based email services from the workplace. Free email services abound from companies like Gmail, Outlook, Yahoo, GMX, AOL, and others. Custodian interviews can reveal the use of external email. E-mail searches within the company's email systems can reveal external messaging by examining sent items and performing network traffic analysis. Ultimately, the Custodian has the Duty to Preserve relevant data regardless of location.

Email auto-delete functions need to be well understood and documented. If the company's email services have automatic processes that purge email after a certain period, then processes must be set up to stop the auto-delete for Custodians. Likewise, a Custodian must have the ability to preserve future emails that may be relevant to the litigation.

Each of these questions and their answers are crucial to define for email eDiscovery. Management will need to address the cost of these capabilities, storage of this data, and the proper preservation of the data where only litigation support technicians can access it for processing. How management addresses these issues will directly influence the "reasonableness" test of the courts that may be needed later in appeal or to support objections from counsel.

2.2 Loose Files

"Unstructured data" often refers to loose files outside of applications, and this environment is a nightmare for eDiscovery (Wightman, 2013). ARMA International, formerly the Association of Records Managers and Administrators, defines unstructured data as a "generic label for describing any corporate information that is not in a database. It can be textual or non-textual. Textual unstructured data is generated in media like email messages, PowerPoint presentations, Word documents, collaboration software, and instant messages. Non-textual unstructured data is generated in media like JPEG images, MP3 audio files, and Flash video files" (Isaza, 2010). According to one eDiscovery vendor, Nuix, "approximately 80% of the data organizations store is unstructured." Some experts claim that the growth velocity of unstructured data may be as high as 50% year-over-year (Taylor, 2015). Loose files fall within at least four classifications, including text, documents, simple containers, and complex containers. Maintaining the location of these loose files is another difficult information governance task. Whether they are located in an on-premise file server, the custodian's private cloud, a corporate mobile platform, or somewhere else, the company and the custodian share the duty to preserve relevant ESI.

In some instances, the custodian may not be aware of where the ESI is stored. With newer Bring Your Own Cloud (BYOC) services, users are synchronizing files to locations without realizing it. This is great from a frictionless, ease-of-use case from the service provider. However, for eDiscovery purposes, dealing with the cloud can be very difficult. Many custodians, when they face an investigation or litigation, will scramble to remember where the ESI is and how to preserve it (Murphy, 2011). That will inevitably lead to higher costs and less timely legal decisions (Murphy, 2011). Luckily, the computers used to synchronize to the cloud leave hints to uncover what files went where (Harris, Dropbox Collections and Considerations, 2013)

Not every bit of ESI relates to the legal matter, however. Relevancy is a key concern for the courts. The *Zubulake IV* court first answered that question in 2003 when Judge Scheindlin ruled, "Must a corporation, upon recognizing the threat of litigation, preserve every shred of paper, every email or electronic document, and every tape backup? The answer is clearly 'no'." However, the files created by a custodian that may be meaningful to a case must be protected and should not be destroyed. Determining which files are relevant ultimately rests on the discretion of the attorneys reviewing the ESI before production. This review is very expensive and innovations in software may replace some of the drudgework at law firms, though its defensibility is still at question (William W. Belt, 2012).

Because of these concerns, some companies have bulk-collected custodian ESI because they have a lack of IT Management and Governance to determine, what files are relevant and which files are not. Companies bulk collect to avoid deleting data and suffering through a spoliation claim. Bulk collecting custodian loose files have been going on for years to avoid spoliation problems. It is up to the managing attorney to define the scope of the bulk collection based on case analysis, proportionality analysis, and Rule 26(b)(2) (B) accessibility analyses. Figure 3 summarizes the scope of a hold and the ESI subject to it (The Sedona Conference, 2010).

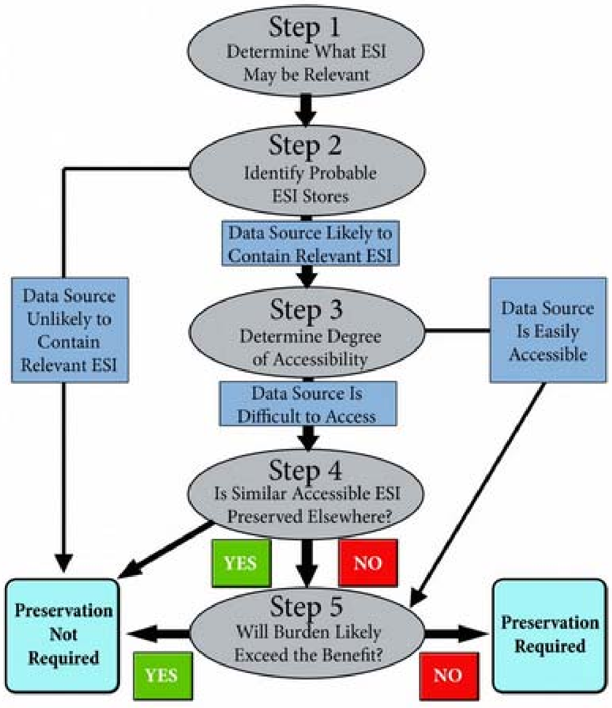

Step 1
Determine What ESI May be Relevant
Step 2
Identify Probable ESI Stores
Data Source Likely to Contain Relevant ESI
Data Source Unlikely to Contain Relevant ESI
Step 3
Determine Degree of Accessibility
Data Source Is Easily Accessible
Data Source Is Difficult to Access
Step 4
Is Similar Accessible ESI Preserved Elsewhere?
YES
NO
Step 5
Will Burden Likely Exceed the Benefit?
Preservation Not Required
YES
NO
Preservation Required

Figure 3 ESI Collections Decision Tree (Losey, 2012)

Based on witness interviews and legal analysis, bulk collection of local and network hard drives may be necessary (New York State Bar Association, 2013). The NYSBA goes on to outline, "In identifying custodians, it is important to consider former employees, independent contractors, any third parties that may store ESI on behalf of a party such as a cloud service providers and offsite storage facilities…”. For each relevant custodian, it is important to take reasonable steps to preserve relevant ESI. Preservation of ESI must take into account the platform from which the data is collected, whether locally, in the cloud, or on mobile devices, and such should be reflected in the identification, collection and preservation of that ESI.

2.2.1 Desktop and Laptop Computers

For every company-controlled digital asset, the consumerization of information technology has enabled workforce members to operate their own Data Center full of technology. An ever-increasing percentage of the knowledge workforce is inadvertently blurring the boundaries between the corporate information they work with every day to their own personal technology and information. The membrane between corporate technology and personal technology has become very permeable. In a digital world, storing information and documents on a USB drive, an SD card, or a smartphone or a tablet and moving data to and from corporate IT environments seems trivial. Employees, often with the motivation to increase their productivity, store data on personally owned and controlled technology assets. In many corporate environments, this data migration goes on undetected. The move to productivity can be a strategic economic approach for businesses to minimize costs while boosting efficiency. Allowing the workforce to use their digital assets often lessens the economic impact of outfitting a workforce with the latest and greatest technology (Györy, Cleven, Uebernickel, & Brenner, 2012). Instead, companies issue a stipend to the workforce member to acquire their own technology, thus reducing the administrative overhead of provisioning and procurement of technology. Regardless of the technology controls and administration controls, or lack thereof, Custodians and Corporations have a legal expectation to produce “any and all” relevant data during e-Discovery (Murphy, 2011).

Self-managed digital assists have given rise to Shadow IT (SIT) (Györy, Cleven, Uebernickel, & Brenner, 2012). SIT is often the unorthodox use of IT without the corporate direction, control, staffing, or planning of traditional Information Technology management (Gallagher, 2015). The phenomenon of personally owned self-sufficient digital knowledge workers has fueled the growth of SIT. The continued consumerism of IT has led to an ever-increasing capability of SIT. SIT is often a user-driven response to the rigid bureaucratic style of some IT organizations (Myers, 2015). This more organic and often unmanaged technology of bring your own device (BYOD) and bring your own cloud (BYOC) environments may help the immediate need of a company to minimize workforce provisioning, but fuels the negative business impacts (Győry, Cleven, Uebernickel, & Brenner, 2012) of vulnerability, non-compliance and litigation. SIT, where there is relevant ESI, continues to be the Company's obligation, as far as the courts are concerned. The Courts do not make any distinction between user-driven SIT and fully managed corporate IT. Overlooking unknown data in an unknown SIT system is easy. Missed data could lead to claims of bad faith and spoliation (Kroll OnTrack, 2013). Custodians and Corporations, along with the Attorneys representing them, have a duty to uncover SIT systems and produce relevant data. (Reginald W. Jackson, 2012).

There are many methods to discover digital assets connected to the Company network. Knowing what is on the network is the first control in the critical security controls framework (SANS CSC, 2015). This control helps inventory assets, which is just one piece of the loose files puzzle. The next piece of the puzzle is to link each custodian to a relevant digital asset that may store ESI. In a static company where one user only uses one computer, this may be a trivial task. However, with most employees using at least three devices to conduct business, most companies find this task difficult (Gillett, 2012).

Once the assets linked to the custodian are identified, then the effort of combing the computer for user-created data stored on its hard drive begins. Depending on the IT environment, this may mean performing a complete backup of the computer, or only a surgical search for files containing metadata associated with the custodian. Efforts are directly proportional to the IT management systems, its governance, and technology environment. In a smaller single-campus environment with a few custodians that have 100 megabyte or gigabyte files, Ethernet full backups may make sense. For any full backup, files in the collection need to be DeNISTed and non-user created files or data should be removed. Any remaining information not relevant to the matter should be removed, so you are left with the smallest, most defensible collection from that device. Throughout this identification process, legal and IT teams must work together to reinforce completeness of collection and relevance of collected data. The result of their collaboration will cull collected data down to the smallest legally defensible data set.

Cloud services are not immune to legal hold or collections, but they can be tricky (Murphy, 2011). For companies using cloud solutions, we assume their contract or agreement gives them control of the data and access to it. The corporate cloud storage of loose files is still subject to the same legal requirements and on-premise file storage, according to the courts. If the custodian controls data on cloud storage like iCloud, DropBox or Google drive, an entirely new set of challenges emerge. When the cloud stretches across international borders, the legal requirements are challenged a bit (Association of Certified eDiscovery Specialists, 2014). The European Union has very different privacy directives as well as a very different legal system. If the custodians are cross-border citizens or if the data is spread between a US jurisdiction and a foreign country, the laws of both countries must be followed and adhered too. Knowledge of the specific legal obligations in the country where the data is housed is necessary in these situations, requiring legal counsel with training in international law.

An accurate data map of custodial loose file environments can be challenging to construct. If the company has implemented the SANS Critical Security Controls, they can help define many aspects of the unstructured data environment (SANS CSC, 2015). A comprehensive review of the company endpoints is essential. This review should include the company's standard image that include the endpoint operating system and standard software as well as the endpoint controls used to manage the endpoints. If the company has an asset inventory system that tracks user interaction (e.g. login event), it may be viable to link the user to compute environment. Within the review, even the endpoints permission and privilege definition are important, as is the software installed on the endpoint.

To track and monitor IT Infrastructure that may house ESI so that evidence collections can take place in a timely manner, each of these factors needs to be gathered beforehand. If a Custodian uses a Laptop, Desktop, and Tablet each of these assets must be linked to the credentials that the Custodian is issued. If someone is subject to a legal hold, then each of those locations may need to be collected to preserve data. Linking endpoint destinations to the user source is critical. In large organizations with either high turnover or devices that are shared, this can be problematic. Generally, it is the people creating, using and storing ESI that are subject to legal holds. As such, much of the pre-analysis that must be performed concerns mapping the user to their devices. The user to asset tracking must be established, tracked for changes, and monitored before they are custodians. Without this pre-analysis effort, a post-litigation scramble takes place that is often ad-hoc. The user to the asset to the data linkage is a key feature of Records Information Management systems (RIMs) (International Organization for Standardization - ISO, 2001).

Essentially the same tracking and monitoring can be leveraged to detect the use of non-traditional data map locations. The use of first SANS Critical Security Control, Inventory of Authorized and Unauthorized Devices (SANS CSC, 2015) can be leveraged to identify SIT environments that may be hidden to the traditional IT department. By knowing, what IP Addresses are being used by each endpoint while simultaneously knowing what credentials are in use on the endpoint an environment of known-good equipment can be formulated. The identification of rogue devices can be calculated by eliminating the “known-good equipment” from the total environment. Software inventory tools that are mentioned in the second SANS Critical Control, Inventory of Authorized and Unauthorized Software (SANS CSC, 2015), can identify cloud applications like Dropbox, Google Drive and iTunes and the custodians can be queried about their use and if they contain relevant information.

In many endpoint environments, there is not an auto-delete function. However, data quotas on network drives, retention policies on network shares, and other data governance controls need to be well understood. This enables the litigation support team to address the complexity of the technical settings that may affect ESI. Typically, unstructured data is not considered the highest value ESI, but the company must make certain auto-delete functions have been controlled to assure no loss of potentially relevant ESI.

2.3 Business Applications & Databases

Business applications and databases are referred to as “structured data” (Carns, 2014). This information typically resides inside complex applications in the form of tables, forms, and reports (Carns, 2014). Representative systems could include both transactional (e.g. e-commerce, supply chain, financial, etc.) and reporting databases (e.g. labor, inventory, sales, etc.). Many times the database is front-ended by an application server or a web UI (user interface). Often the application server performs crucial processing itself to present or hide data based on permissions and privileges within the application itself. These segments of information, inside a larger system, provide structure to the data and give meaning as well as the definition to structured data.

Structured data systems that may be placed under legal hold vary as much as the ligation. Labor or Equal Employment Opportunity Commission (EEOC) matters may cover time punch systems, labor management tools, and staffing systems. Governmental regulatory cases may cover any regulated data sets. This may include financial systems to search for fraud covered by GLBA, or student information systems for FERPA investigations, and Electronic Medical Record (EMR) covered by HIPAA/HITECH.

Practically any enterprise resource planning (ERP) system may be subject to legal hold based on the merits of the matter. ERP systems can be a broad array of systems that may or may not be monolithic or completely integrated. Common ERP systems include the following: Accounting, Distribution, Production, Procurement, Sales, Customer Services, Corporate Governance, Human Resources, Business Intelligence, and others (Yeung, 2013).

The legal hold may cover each of these systems based on attorney lead analysis (The Sedona Conference, 2010). Bulk collections of these systems are impossible or impractical. The Data Owners of the system must work with IT to preserve the data until the attorneys determine what reports or datasets must be extracted from the systems for collection. This means that any auto-delete or data manipulation functions must be halted, at least temporarily, for potentially relevant data to be preserved. In some systems, like SAP, there are native capabilities to place certain data on hold (SAP, 2012).

The company must have an accurate data map of structured data. The identification of data type per system, per application, and per database is necessary. However, that data by itself may be inadequate. Identifying which credentials and the people issued those credentials that can access, update, modify and delete data with the application is necessary as well. Structured data and the IT Infrastructure must be tracked for configuration changes that may affect the structured data. This includes not just infrastructure changes, but application specific changes. If the company has custom code within the business applications that performs business specific calculations on structured data, then that code also may be subject to legal hold. Each of these factors needs to be pre-analyzed so that evidence collections can take place in a timely manner.

Within the company's structured data environment, it is unusual for a SIT environment to thrive. However, the company must be able to detect the use of non-traditional SIT structured data. This includes variations on BYOC as well. Also included are the cloud application solution providers, as well as departmental systems that may process or alter the structured data. This may be especially true in a reporting environment. Within a reporting environment, there may be several SIT type environments from a macro latent excel form to a custom Apache front-end used by ancillary staff.

Databases and their applications do not typically have auto-delete functions that need to be controlled to assure no loss of potentially relevant ESI. However, it is a standard IT practice to dispense with data that is no longer relevant to the business. Processes that delete or archive structured data need to be well understood, so that relevant ESI is not inadvertently destroyed.

2.4 Collaboration/Messaging

Among the collaboration and messaging system, there are vast differences. Two ubiquitous forms are email and Instant Messaging (IM). E-mails are akin to letters, as they are longer, more formal, and for the most part have more structured in logic. IM is much more conversational and similar to conversations (Carroll, 2007). In the early 2000s, many industry pundits believed that IM would replace email as the communication method of business including Gartner (Gartner, 2007). The prevailing eDiscovery factor is that email has a higher degree of expectation to be archived and saved.

The 2011 Sedona Conference gave issued guidance that there is no duty to preserve instant or text messages if a party does not routinely save those messages and litigation is not anticipated (Gareth Evans, 2014). Courts have generally found that, because of the presumed "volume of instant messages” and its “many platforms,” it would be very difficult, if not impossible, to “compile messaging" for review or production. Another factor is the inferred non-value of the IM communications due to their perceived conversational tone and informality.

However, some industries do not get a pass on archiving and managing IM. These industries produce high-value IMs and collaboration communications. These include heavily regulated industries like banking, brokerage, and stock market traders. In these industries, IM is considered a form of communication that must be recorded, so the transactions that are executed within the business are reputable. Traders in today’s markets are relying almost exclusively on instant messenger and social media to discuss real-time marketplace conditions, take orders, and in general conduct business (William Kane, 2014).

Enterprise collaboration is not dead, but most companies are not leading the effort. The drivers are individual employees using a mix of mobile, social, cloud and data platforms. IMs value is in being the "connecting tissue" between employees, customers, and business results (Kapko, 2013). In this situation, pre-analysis can save a tremendous amount of effort. If it is determined, that IM’s are out of scope then companies can prioritize efforts around system types that are in scope of discovery. If IM’s are in scope the same controls, logging, and archiving that support operations can support ediscovery.

2.5 Other Communication Devices

In the classic sense of the meaning “Communication Devices” have irrevocably changed both Corporate and SIT environments. Since the iPhone’s introduction on January 9, 2007, mobile computing has revolutionized the workplace (Apple, 2007). Generation 1 iPhone had as much raw computing power as either the Apollo crew spacecraft or the IBM System/360 model 75 in 1969 at Houston Ground control and the Goddard Space Flight Center (ComputerWeekly, 2009). Today, a mobile platform and its accessories can create a walking data center connected to the cloud with Infrastructure as a Service (IaaS), Software as a Service (SaaS) and Platforms as a Service (PaaS) within most major markets in the US (RackSpace, 2013). Mobile platforms are digital assets that can store, process and transmit both structured and unstructured data types in more personal ways than a PC, which makes them better in many respects (Pash, 2010). In many ways, mobile platforms like iOS and Android and their many form factors of phone, phablet, and tablet have made traditional desktop or laptop a secondary device (McLean, 2015).

Mobile platforms are critical to the eDiscovery community. There is no duty to preserve instant or text messages if a party does not routinely save those messages and litigation is not anticipated (Gareth Evans, 2014). However, the likelihood that such devices would contain non-duplicative information increases as the capabilities increase. When workers and custodians use them as portals into the cloud, there is an ever-increasing probability that relevant original content may indeed reside on communication devices.

The value of pictures in litigations cannot be overstated. Some cases hinge on the metadata contained within a picture stored on a communication device (Bennion, 2014). A picture is worth a 100-metadata tags that include GPS data, data time, and a host of other data if uploaded to the social media cloud. The data on phones and a company’s duty to preserve is evolving. Many courts still believe that picture, text message, and other device-only ESI are ancillary at best, due to the several factors including who controls the phone (e.g. company or personal) the routine nature of device backups on a PC, and other issues subject to environmental factors. However, criminal courts have long used cell phone data to prosecute and convict (Nelson, 2014). This has become so pervasive that courts have started to consider the cell phone as an extension to a person’s “personal papers” and gave them constitutional protection from search and seizure (Liptak, 2014).

The company must have an accurate data map and know what communication devices are used and how they are managed. Whether or not the company uses a Mobile Device Management system (MDM), it needs to know if smartphones and wearable computers are leveraged within its environment. Along the continuum of endpoints, the mobile device, for the moment at least, is too constrained to be a full-fledged content creation device. However, within the realm of business applications, email, and IM, they may be most used creation device deployed. These apex systems hold the authoritative copy of the transaction, with at least two exceptions: pictures and text messages.

Each of these content types and the associated metadata may need to be preserved. Both company and custodian have a Duty to Preserve. Determining or establishing a transfer path from device to preservation location is a necessity. One common method of moving data from a smartphone is email, where the smartphone user forwards the ESI to a Company controlled preservation vault for safekeeping. Other methods that will need in-depth pre-analysis are smartphone backups to PCs, as well as, forensic imaging requiring the smartphone to be connected and its access code procured.

Reviewing the company's architecture and infrastructure surrounding communications devices will identify is system characteristics. Depending on the matter and the details in the litigation, these devices, their data map, and the custodial ownership are key issues that need pre-analysis and definition before the legal hold arrives. Unfortunately, there is no way short of a forensic inspection to determine if a smart phone user deleted data. Most systems also lack ways to disable auto-delete functions, like deleting old text messages as the messages exceed storage system settings. On mobile devices, there are few comprehensive control systems, like a MDM, that can ensure no loss of potentially relevant ESI.

2.6 Phone and Voicemail

Custodians generally understand that corporate email is subject to hold, but other potential evidence like voice mail may be just as important (Aversano, 2015). There has to be a strong reason to establish voicemail evidence as central to the case. The courts typically focus on how readily accessible voicemail messages are when establishing whether it should be considered as evidence (Vincent Syracuse, 2013). If voicemail is unduly burdensome to identify, preserve, and produce, it is often considered inaccessible.

There are several types of voicemail systems. The type of system will determine what steps that company should take to preserve voicemail messages. There are two major types, analog, and digital. If the system needs to be preserved, the company's routine deletion schedules, at least regarding the custodians, must be suspended. In an analog system, this means tape archives. In a digital system, often the system has voice mail boxes that can be exported into MP3 files. Often these systems are linked to email, whereby the voicemail system forwards messages to the email system. In these integrated systems, collection and preservation of the email mailbox automatically preserves the voicemail files.

Voicemail has also moved to the cloud, for example, Google Voice, Grasshopper, and Office365 voice services. Each of these cloud systems is digital in nature and has multiple configurations that allow for archiving, forwarding, and managing environments with technical policies. If your company uses cloud-based service for voicemail, then a strong architectural and capability review with the vendor must occur before eDiscovery demands are placed upon the company.

Understanding the voicemail architecture is necessary for eDiscovery teams. Identifying the type of Voicemail service mix the company utilizes, and its many dependencies can be overwhelming. Rare is the infrastructure where a large company has a single monolithic voicemail server. Regardless of platform, the system type and capabilities must be well understood by the Litigation Support team to assist with the uncommon collection of potentially relevant voicemail. The pre-analysis of the voicemail architecture will create a more timely response to eDiscovery demands. In order to anticipate how to collect and preserve voicemail evidence, it is important that a comprehensive evaluation of the entire voicemail system be performed.

Voicemail auto-delete functions need to be well understood and documented. If the company's voicemail services have automatic processes that purge email after a certain period, then processes must be set up to stop the auto-delete for Custodians. Likewise, a Custodian must have the ability to preserve future voicemails that may be relevant to the litigation. In many enterprises, moving to IP-based phone systems, the preservation and control of messages is becoming easier. In many companies, the voicemail and email systems are integrated. Therefore, if you stop the auto-delete in email, you can also stop the auto-delete in the phone system.

2.7 Web-based Systems

Most users, including sales staff, business leaders, and IT personnel use the terms "Web-Based systems" and "The Cloud" interchangeably. The courts and the court's experts find great distinction between the differing types of Cloud services, such as IaaS, SaaS (e.g. The Cloud), and Web-based systems. Web storage of "loose files" and structured data in support of applications blur the lines of the controlling party and their requirement to preserve (Murphy, 2011). In some environments, the custodians themselves must gather data and produce it as evidence. In other systems, the company is responsible for working with the vendors and extracting the relevant data.

Vendors in the space include, but are certainly not limited to, Microsoft, Google, Apple, Dropbox, and Box.net (Harris, Google Drive Collections and Considerations, 2013). These services provide a varied amount of cloud storage space free as part of their base offerings for consumers and companies. Each of these services is linked to a client install. The client install can be on a PC, Tablet, or Smartphone. These programs synchronize a set of files to the cloud, allowing all devices associated with the cloud account (computers, phones, tablets) to have access and constant syncronization of the shared files.

Litigation teams need to be well acquainted with the official and unofficial web-based systems in use by the company's employees. This may take the aggregation of several parts of the business including Networking, Security, Architectural Engineering, Endpoint Compute, and other teams that operate both endpoint and egress controls. Together these systems stitch a broad array of intelligence to develop an accurate data map. This is particularly difficult without specific custodian interview questions that help determine if BYOC or SIT is in use within the affected business organization.

The tracking and monitoring of IT Infrastructure that may house ESI could be less of a concern depending on the web-based system design and communication methods. Local copies could be maintained, but not every BYOC vendor has enabled designs similar to Google, iTunes, and Dropbox. This situation stresses the need for endpoint software inventories and a high degree of pre-analysis and control to limit software installation.

Each legal matter is different, but if web-based systems are in scope, then many items must be in place for timely collection or preservation. The sheer number and disparities of these types of systems make them difficult to govern. The Courts have been unclear on how it views their inaccessibility. Continuous evaluation and monitoring are necessary for the on-going identification and pre-analysis necessary for defensible collections. Detecting the use of non-traditional data map locations like BYOC is nearly impossible with manual methods. To monitor network communications that connect to BYOC locations, the eDiscovery team may need instrumentation that detects outbound content. It is important to remember that off-site non-company controlled data storage locations may require either the custodian themselves or the vendor to cooperate with the lawsuit. The detection of the possibility may increase the comprehensiveness of the collections system, but data outside the companies control is unreasonable for the company to be responsible for collecting. The Duty to Preserve is still upon the custodian, and they should go to any BYOC data locations they have and turn over the relevant ESI. Interviews are crucial to identifying SIT and BYOC web-based or cloud environments.

For company controlled web-based systems the auto-delete functions need to be suspended. Like the email auto-delete functions, the web-based systems need to be well understood and documented. If the company's web-based applications or services have automatic processes that purge data after a certain period, then processes must be set up to stop the auto-delete for Custodians. Likewise, a Custodian must have the ability to preserve future data that may be entered into the systems or services.

2.8 Remote Access Systems

Since before Frances Cairncross's book, "The Death of Distance" published in 1997, employees have been using Virtual Private Networks (VPN) and Remote Access Servers (RAS) to gain access to company data from remote locations. In today's workplace, most employees still use similar systems to telework. With the adoption of Citrix and VMware view and a whole marketplace of product remote access is widespread. This is a unique challenge for eDiscovery Operations and the attorney's they support.

The pre-planning and analysis for remote access systems is different from either structured or unstructured data systems. This will mean understanding and monitoring the data that passes through a company's data center to a remote VPN'ed endpoint. The custodian that uses an endpoint from home, depending on the circumstances of the legal matter, may be in scope. This may be the case even if the home PC is a personally owned device. The data residing on that home PC is still under the control of the company. The company did allow remote access to the ESI by the custodian and the Duty to Preserve has not been suspended. This is another situation where custodian interviews may help identify what ESI is in scope as well as its location within or outside the company's technology environment.

Each remote access session requires credentials and privilege in order to attach to the corporate data repositories. The company has made a determination who should enjoy remote access. Access provisioning is job role or job function based, and has technical policy and access rules that define what a remote worker can perform from their endpoint. Behind each endpoint, there is a client device, sometimes a laptop, PC, tablet or smartphone, which reaches through the Internet to attach to the corporate environment.

Variability in endpoints have driven companies to adopt Virtual Desktop Integration (VDI). Some view this move away from the PC and Laptop as the return of the mainframe (Knorr, 2010). As a result, many companies are restricting data movement. They no longer allow workers to save data to local drives, print, and use USBs from within VDI and other virtual environments. Collections within virtual environments are similar to corporate endpoint collections. VDI environments store all their data on company assets that are within easy reach of eDiscovery Operations for identification, collection, and preservation.

2.9 Back-up System

Backup systems are highly specialized in today's business environment. Rare is the venerable tape drive with full backups on the weekend and incremental backups during the week. No matter what system a company uses, it is imperative that the company examine its backup strategy. The scope of the legal hold has for years extended to backups regardless of the medium used for backup. Courts generally accept that old-fashion tape backup systems are unreasonable and place an unfair burden in producing electronic documents in litigation (The Sedona Conference, 2010). The key legal concern is the costs to restore all the tape data in contrasted to the value of the case. The proportionality tests have established a process to value the likely outcome of the case as compared to the costs to the restoration costs. If the restoration costs are greater than the potential value of the case, then no tape restores are required. In many jurisdictions, tape-held information is considered "inaccessible" and does not need to be restored at all. However, as more and more companies move to disk-to-disk architectures and online backups, the cost reduction and accessibility make them more often subject to preservation notices.

The burden of knowing where the backups are and how to retrieve them fall squarely on the companies' shoulders. The company must understand how backups are created, where data is stored, and how to retrieve that data Major backup-in-the-cloud vendors are Office365, Google's Vault, and Amazon Glacier just to name a few. However, a very profitable market segment from eDiscovery vendors is the ability to access and search "The Cloud" for you. Backup copies once meant for disaster recovery have become the de facto archive that plaintiffs desire. Some plaintiff lawyers use the threat of tape restore as a key legal strategy to force defendants to settle (Schuler, 2009). Even in Zubulake IV in 2003, Judge Scheindlin did not establish a rule that exempts all backup tapes from the duty to preserve. Instead, it focused on how the backup systems operate to determine whether a specific tape must be preserved in certain circumstances. The NYSBA recommends," ensuring that all ESI sources are properly identified and addressed, including online, near-line, and offline servers and storage devices and home computers, when applicable." They go on to include preserving tapes by, "removing backup tapes from the routine recycling, overwriting, or destruction process" (New York State Bar Association, 2013).

Understanding the backup architecture, and what actions need to be performed to preserve ESI in a timely manner, is crucial for IT and Legal in developing a strategy to prepare for litigation and eDiscovery response. Backups contain loose files as well as application and database information. In many environments, these data streams are conjoined in a multi-stream backup methodology that simultaneously writes many systems of different data types onto massive sized tape drives. The same due diligence required in the prior systems is also required for their backups.

Each legal matter is different, and generally, backup systems are considered out of scope due to their inaccessibility. However, if the court believes that the backups are the only location of relevant data, then the parties may have to split the costs and restore the data. The backup architecture and its policies need to be well understood and documented. As part of the Information Management tasks, a Company already tracks and monitors the status of backups and tests them for integrity. These management tasks may fully support the legal need to recover ESI. As a key IT Infrastructure that may house ESI, backup systems on a server and endpoint bases must be evaluated in case a legal matter does cover the company's backup system. Just like in other systems in our analysis, the auto-delete functions need to be suspended so that evidence collections can take place in a timely manner without data loss.

It is important to remember that off-site non-company controlled backup locations may require either the custodian themselves or the vendor to cooperate with the lawsuit. The detection of the possibility may increase the comprehensiveness of the collections system, but backup/archive data outside the companies control is unreasonable for the company to be responsible for collecting. The Duty to Preserve is still upon the custodian, and they should go to any BYOC data locations they have and turn over the relevant ESI. The courts may expect the company to know that third party backup software was installed on the custodian's computer. The courts may reason that IT management practices would detect large amounts of data leaving the companies technology environment. The courts have a very dim view of a company's inability to identify or produce relevant data. If a company's information management system or the lack of one contributes to eDiscovery difficulty; it is very unlikely to persuade the courts for leniency (Lexis Nexis, 2008).

3.0 Constructing Defensible Operations

Best practice governing bodies and the courts have recognized standardized processes ever since the FRCP extended into eDiscovery in 2006. The continued use of manual identification, collection and preservation methods are unfeasible and even indefensible in discovery involving significant amounts of ESI (The Sedona Conference, 2013). A company adopting sophisticated automated tools, alone, will not necessarily lead to successful results. Lawyers and their teams must recognize that the process by which legal support staff operates the tools is just as important as the tools themselves (The Sedona Conference, 2013). It is important to establish an iterative process that incorporates feedback and learning that allows for measurement and validation of results. The time and effort spent up-front to design a defensible eDiscovery process that targets the real needs of the company is a requirement before deploying any system-driven methods of search and retrieval.

In order to craft written processes and procedures for the unique mix of system types and locations a company has deployed, a comprehensive audit of how the company's workforce use and store data (Schuler, 2009). The fundamental data gathered will provide the basis for the pre-analysis of potential custodian data stores. The comprehensive audit also helps establish the IT monitoring controls necessary to stay abreast of the dynamic nature of workforce data creation, transmission, and processing. Lastly, the audit and pre-analysis assists in defining the auto-delete suspend functions.

The establishment of written processes and procedures for collecting evidence are the next series of steps in developing defensible operations (Association of Certified eDiscovery Specialists, 2014). Well defined and designed operations from Legal Hold to Custodian Identification to Collection and finally, Preservation ensures success. This will assist not only in the overlapping IT management areas, but also in the day-to-day operations of the eDiscovery department.

Each litigation event needs an activity log that describes steps taken, conversations had, and how decisions were made during the phases of discovery helps with defensibility as well (Association of Certified eDiscovery Specialists, 2014). This assists with the recall of certain details that help demonstrate a good faith in court. Furthermore, both logs and notes help to construct defensibility in actions taken to identify data sources, the steps taken to collect them, and ultimately how the evidence was preserved. Notes and logs also assist in the creation of report findings to the managing Attorney that is directing the eDiscovery efforts.

Each of the ten system types discussed earlier has nuances based on location type, vendor, implementation, and staff expertise. Each needs a plan and process to gather the relevant data. The details of each system, including the technical configurations, are important. Even the software tools used and the eDiscovery staff's training on the tools may be crucial in a high-visibility litigation event. Litigation support staff must develop methods to do the following: 1) manage the company's unique mix of systems, 2) stay informed about technology changes within the environments, and 3) staff to appropriate levels to operate the collections systems. Having the proper mix of staff to handle litigation requests is another organization factor that can show good faith. Good faith itself is the bedrock of defensibility.

Each of the process systems assists in creating a specific litigation event data map (Schuler, 2009). Each supporting technology system should have a set of procedures describing the data sources, steps taken to collect them, and how they were preserved. This is crucial work if the matter ever goes to trial, or if there is a motion to discover the companies' eDiscovery practices.

4.0 Conclusions

Companies are not constructed with litigation defense in mind (Murphy, 2011). Neither are they constructed for information security (Barker, 2015). They are organized to perform revenue-generating activities. Companies of size would be wise to plan for litigation and prevent the mad scramble to adjudicate an overwhelming discovery of system types and possible locations of ESI. Benjamin Franklin's axiom that "an ounce of prevention is worth a pound of cure" is as true today as it was when Franklin made the quote on February 4, 1735 issue of The Pennsylvania Gazette.

Companies must prepare for litigation, just as they should for cyber-defense. Executive management must lead the Planning, Organizing, Staffing, Directing, and Controlling of the enterprise (Koontz, 1955). Executive management must understand the value of records management, as well as how the businesses revenue generating machinery creates, uses, and stores data. This knowledge is the fulcrum used to move the company from an exposed position of danger to a prepared position of safety. Before litigation occurs, executive management at medium and large firms must plan and organize for litigation. Organizing an information governance program to manage the data, measure its value, and enforce retention periods is a fundamental enabler. Establishing control mechanisms to identify where data is stored, by whom, and for what purpose is another basic enabler. Executive management must make the decision to enable an economic response to e-Discovery, or deal with the aftermath of being ill-prepared.

A showing of good faith has always been necessary when responding to discovery. Ediscovery respondents bear this burden. Whether plaintiff or defendant, counsel for either side cannot claim that they did not know ESI system types or locations. Attorneys have a duty to the court to uncover relevant data, no matter in what form and wherever they may be stored, and make time to collaborate with proper IT personnel. Proactive conversations with ESI stakeholders that include custodians, IT stewards, and data owners are a key responsibility of counsel. The attorneys leading eDiscovery need this information to create and maintain documentation regarding what preservation actions were taken when the obligation arose and how both custodians and relevant ESI repositories were systematically identified (Christina Angell, 2014).

For some smaller companies, it may be impossible to fund and adequately staff a litigation support function to decipher the locations and systems potentially subject to legal holds. These small businesses can be destroyed by litigation (Bort, 2015). The rigor required in establishing data classification taxonomies and ownership of user-created content presents many challenges. Managing the digital identities and privileges to create and store user-created content must be addressed. User-driven innovation and SIT can be uncovered through interviews and knowledge of what is connected to the enterprise and what software has been installed (SANS CSC, 2015). Lastly, to operate a defensible eDiscovery program the organization must recognize a return on its investment (ROI). The ROI must be an integral part of the methodology. Savings emerge as irrelevant data is stripped away and the amount of data remaining for legal review shrinks. The effectiveness of the eDiscovery process must be managed closely and reporting made available to executive management.

In business, litigation may be inevitable. A defensible e-Discovery program can do a great deal to defend the enterprise. Establishing an organizational culture that values business records, treats each document as a record to be used and treated in a reasonable manner through its lifecycle mitigates the effects of litigation though Records Information Management. Data Governance and Records Information Management along with the e-Discovery Reference Model (EDRM) and its integration with Information Governance Reference Model (IGRM) can deliver a path to minimize litigation response while maximizing effectiveness.

The challenge in addressing the overly litigious business environment is not just juggling one more management task alongside people, products, and profits (W.J. Sanders III, 2000). It is determining the proper organizational response for creating a practice of both reasonableness and good faith before litigation occurs.

References

AdvantaCare Health Partners, LP v. AccessIV, No. 03-04496, 2004 WL 1837997 (N.D. Cal Aug 17, 2004).

American Bar Association. (2015, 05 27). *Step in a Trial*. Retrieved from How Courts Work: http://www.americanbar.org/groups/public_education/resources/law_related_education_network/how_courts_work/pleadings.html

Apple. (2007, January 9). *Apple Reinvents the Phone with iPhone*. Retrieved from www.Apple.com: https://www.apple.com/pr/library/2007/01/09Apple-Reinvents-the-Phone-with-iPhone.html

Apple Inc. v. Samsung Electronics Co. Ltd et al, No. 5:2011cv01846 (N.D. Cal 2012).

Association of Certified eDiscovery Specialists. (2014). *CEDS Examination preparation manual third edition.* Miami, Florida: ACEDS.

Aversano, K. (2015). Avoiding the hammer: defensible strategies for FRCP proposed Rule 37(e). *Information Management Journal*, 30-34.

Bennett, B. (2015, June 8). *With Islamic State Using Instant Messaging Apps, FBI Seeks Access to Data*. Retrieved from Emergency Management: http://www.emergencymgmt.com/safety/Islamic-State-Instant-Messaging-Apps-FBI-Seeks-Access-Data.html

Bennion, J. (2014, May 20). *What Morgan Freeman's Face Teaches Us About Metadata And E-Discovery.* Retrieved from Above The Law: http://abovethelaw.com/2014/05/what-morgan-freemans-faces-teaches-us-about-metadata-and-e-discovery/

Blue Sky Travel & Tours, LLC v. Al Tayyar, 2014 WL 1451636 (4th Circuit March 31, 2015).

Bort, J. (2015, May 29). *CEO of bankrupt Linux company says employee lawsuits put it out of business.* Retrieved from Business Insider: http://www.businessinsider.com/ceo-employee-lawsuits-killed-mandriva-2015-5?op=1

Boudreau, K. (2010). Open platform strategies and innovation: granting access vs. devolving control. *Management Science 56(10)*, 1849-1872.

Brady, N. C. (2011, October 29). *Configuring Discovery Methods*. Retrieved from SCCM 2012 in a LAB - Part 3. Configuring Discovery and Boundaries: http://www.windows-noob.com/forums/topic/4428-using-sccm-2012-in-a-lab-part-3-configuring-discovery-and-boundaries/

Carrillo v. Schneider Logistics, Inc., No. CV11-8557-CAS (C.D.Ca 12 31, 2012).

Carroll, T. (2007, August 1). *IMs As ESI: When To Save Instant Messages And How To Properly Authenticate Retained IMs*. Retrieved from Metropolitan Corporate Counsel: http://www.metrocorpcounsel.com/articles/8659/ims-esi-when-save-instant-messages-and-how-properly-authenticate-retained-ims

Christina Angell, M. B. (2014). Legal Ethics of Social Media. *Section of Family Law* (pp. 5-6). Stowe, Vermont: American Bar Association. Retrieved from http://www.americanbar.org/content/dam/aba/events/family_law/2014/10/legal.authcheckdam.pdf

Chutich v. Papa John's International, Inc., No. C10-1139-JCC (W.D. Wa. 11 9, 2012).

Computer Research Association. (2012, Nov 30). *Challenges and Opportunities with Big Data.* Retrieved from www.cra.org: http://www.cra.org/ccc/files/docs/init/bigdatawhitepaper.pdf

ComputerWeekly. (2009, July 17). *Apollo 11: The computers that put man on the moon*. Retrieved from ComputerWeekly.com: http://www.computerweekly.com/feature/Apollo-11-The-computers-that-put-man-on-the-moon

Cornell University Law School. (2005). *Legal Information Institute*. Retrieved from Rule 26. Duty to Disclose; General Provisions Governing Discovery: https://www.law.cornell.edu/rules/frcp/rule_26 retrieved 6-1-2015

DiBianca, M. (2014, 01 02). *Discovery and Preservation of Social Media Evidence*. Retrieved from www.americanbar.org: http://www.americanbar.org/publications/blt/2014/01/02_dibianca.html

e-Discovery HQ. (2012, June 25). *e-Discovery Requirements*. Retrieved from http://ediscoveryhq.com: http://ediscoveryhq.com/ediscovery/ediscovery-requirements/ retrieved 7-6-15

eDiscovery101. (2013, November 18). *Cloudy, with a chance of eDiscovery*. Retrieved from eDiscovery101: http://ediscovery101.com/tag/google-drive/

EDRM.NET. (2012, Oct 11). *Information Governance Reference Model (IGRM)*. Retrieved from www.edrm.net: www.edrm.net/projects/igrm retrieved 5-15-15

EDRM.NET. (2014, May 14). *EDRM Framework Guides Version 3*. Retrieved from EDRM Framework: http://www.edrm.net/resources/guides/edrm-frameworks-guides retrieved 5-30-2015

Gallagher, S. (2015, March 8). *The Ambassador who worked from a Nairobi bathroom to avoid State Dept. IT.* Retrieved from Ars Technica: http://arstechnica.com/information-technology/2015/03/the-ambassador-who-worked-from-nairobi-bathroom-to-avoid-state-dept-it/

Gareth Evans, J. R. (2014, January 15). *2013 Year-End Electronic Discovery and Information Law Update*. Retrieved from Publications: http://www.gibsondunn.com/publications/pages/2013-Year-End-Electronic-Discovery-InformationLaw-Update.aspx

Garrie, D. (2013, February 9). *E-Discovery on Smart Phones and Tablets — (Part 2 of 4)*. Retrieved from Law and Forensics: http://www.lawandforensics.com/e-discovery-on-smart-phones-and-tables-part-2-of-4/

Gartner. (2007, June 21). *Gartner Predicts Instant Messaging Will Be De Facto Tool for Voice, Video and Text Chat by The End of 2011.* Retrieved from Gartner: http://www.gartner.com/newsroom/id/507731

Gartner Group. (2011, July 31). *Pattern-Based Strategy: Getting Value from Big Data July 2011. .* Retrieved from www.gartner.com: http://www.gartner.com/it/page.jsp?id=1731916 retrieved 6-7-2015

Gillett, F. (2012, February 22). *Employees Use Multiple Gadgets For Work — And Choose Much Of The Tech Themselves*. Retrieved from Forrester Research: http://blogs.forrester.com/frank_gillett/12-02-22-employees_use_multiple_gadgets_for_work_and_choose_much_of_the_tech_themselves

Goetz, M. (2013, August 1). *Trial Evidence.* Retrieved from American Bar Association: http://www.ropesgray.com/~/media/Files/articles/2013/08/TrialEvidence_ArticleReprint_SocialMediaEvidenceInCivilLitigation.ashx

Gokare, P.C. v. Federal Express Corp., No. 11-cv-02131 (Western District of Tennessee 8 1, 2012).

Grayson v. Cathcart, No. 2:07-00593-DCN (2013 U.S. Dist Apr. 8, 2013).

Greenberg, B. J. (2015, September 15). *Seven questions every CIO should be able to answer about eDiscovery and legal holds.* Retrieved from General System Dynamics: http://gsysd.com/articles/what-every-cio-needs-to-know-about-legal-holds.html

Griffin, G. (2006, May 6). *Disorder in the court*. Retrieved from Denver Post: http://www.denverpost.com/business/ci_3791466

Györy, A., Cleven, A., Uebernickel, F., & Brenner, W. (2012). Exploring the shadows: IT governance approaches to user-driven innovation. *ECIS 2012 Proceedings* (pp. paper 222 (1-13)). ECIS.

Harris, N. (2013, June 4). *Dropbox Collections and Considerations*. Retrieved from Digital Strata: http://www.digital-strata.com/blog/2013/6/4/dropbox-what-it-is-where-to-find-it-and-why-it-matters.html

Harris, N. (2013, June 26). *Google Drive Collections and Considerations*. Retrieved from Data Strata: http://www.digital-strata.com/blog/2013/06/26/google-drive.html

Healthcare Information and Management Systems. (2014). *Title 45 - Public Welfare. Subtitle A, SUBCHAPTER C PART 160, GENERAL ADMINISTRATIVE REQUIREMENTS.* Retrieved from Subpart A - General Provisions. 45 CFR 160.103: http://www.himss.org/files/HIMSSorg/Content/files/CPRIToolkit/version6/v7/D88_Special_Issues_and_Concerns(2).pdf

International Organization for Standardization - ISO. (2001). *ISO 15489-1:2001 - Information and Documentation - Records Management - Part 1: General.* Retrieved from www.iso.org: http://www.iso.org/iso/catalogue_detail?csnumber=31908

International Standardization Organization (ISO). (2001). *ISO 15489-1:2001 - Information and Documentation-Records Management Part 1: General.* International Standardization Organization (ISO).

ISC². (1992). *History of (ISC)²*. Retrieved from www.isc2.org: https://www.isc2.org/isc2-history.aspx

ITIL. (2011). *ITIL Incident Management*. Retrieved from itlibrary.org: http://www.itlibrary.org/index.php?page=Incident_Management

Jackson, R. (2012, Jackson, Reginald). *THE BURDENS OF TECHNOLOGY: ATTORNEY DUTIES IN THE ELECTRONIC AGE.* Retrieved from Southeastern Bankruptcy Law Institute: http://www.sbli-inc.org/archive/2012/documents/T.pdf retrieved 5-20-2015

Jackson, S. (2011). Rule 30(b)(6) Deposition Mystery Revealed: What Records Professionals need to know. *ARMA International, www.arma.org November/December*, 27-30.

John L. Carroll, K. J. (2004). Observations on "The Sedona Principles". *The Sedona Principles* (pp. 4-5). The Sedona Conference.

Kaupp, C. (2013, July 9). *eDiscovery on the Cheap*. Retrieved from Digital-Strata.com: http://www.digital-strata.com/blog/2013/07/09/ediscovery-on-the-cheap.html

Koontz, H. &. (1955). *Principles of management. an analysis of managerial functions. .* New York: McGraw-Hill.

Kroll OnTrack. (2013, 09 26). *Sekisui Am. Corp. v. Hart: Judge Scheindlin's Latest Footprint in Spoliation Case Law – Part 2*. Retrieved from TheeDiscoveryBlog.com: http://www.theediscoveryblog.com/2013/09/26/sekisui-am-corp-v-hart-judge-scheindlins-latest-footprint-in-spoliation-case-law-part-2/ retrieved 6-5-15

Law.com. (2015, 07 07). *Basic Principles of Case Law*. Retrieved from Law: http://common.laws.com/case-law

Legal Hold Pro. (2014). *Legal Hold & Data Preservation Benchmark Survey 2014.* Legal Hold Pro and the Steinburg Group.

Lexis Nexis. (2008). *Discovery.* Retrieved from LexisNexis: www.lexisnexis.com/discovery

Liptak, A. (2014, June 16). *Major Ruling Shields Privacy of Cellphones*. Retrieved from NY Times: http://www.nytimes.com/2014/06/26/us/supreme-court-cellphones-search-privacy.html?_r=0

Lisa M. Arent, R. D. (2002). E-discovery: Preserving, Requesting & Producing Electronic Information. *Santa Clara High Technology Law Journal*, 131-180.

Logtale, Ltd. v. IKOR, Inc., 2013 WL 3967750 (N.D. Call July 31, 2013).

Losey, R. (2012, October 8). *Electronic Discovery Best Practices*. Retrieved from www.EDBP.com: http://www.edbp.com/preservation/

Marshall Brain, T. C. (2003). *How E-mail Works*. Retrieved from How Stuff works Computers: http://computer.howstuffworks.com/e-mail-messaging/email3.htm

McLean, M. (2015, March 11). *ARE MOBILE DEVICES REPLACING DESKTOPS AND LAPTOPS?* Retrieved from Barcoding Connected: http://blog.barcoding.com/2015/03/are-mobile-devices-replacing-desktops-and-laptops/

Mosaid v. Samsung, 348 F. Supp.2d 332,333, and 339 (D.N.J. 2004).

Murphy, B. (2011, 11 29). *e-Discovery in the cloud not as simple as you think.* Retrieved from http://www.forbes.com: http://www.forbes.com/sites/jasonvelasco/2011/11/29/e-discovery-in-the-cloud-not-as-simple-as-you-think/

Myers, N. S. (2015, March 9). *The Impact of Shadow IT Systems on Perceived Data Credibility and Managerial Decision Making.* Retrieved from Available at SSRN: http://ssrn.com/abstract=2334463 or http://dx.doi.org/10.2139/ssrn.2334463 retrieved 6-21-2015

Nelson, S. (2014, June 12). *Police Need Warrant for Cellphone Location Data, Appeals Court Rules*. Retrieved from U.S. News: http://www.usnews.com/news/articles/2014/06/12/police-need-warrant-for-cellphone-location-data-appeals-court-rules

New York State Bar Association. (2013, April 5). *BEST PRACTICES IN E-DISCOVERY IN NEW YORK STATE AND FEDERAL COURTS.* Retrieved from NYSBA.org: http://www.nysba.org/workarea/DownloadAsset.aspx?id=51833

NIST. (2012, August 31). *Computer Security Incident Handling Guide*. Retrieved from NIST.SP.800-61r2: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf retrieved 6-5-15

NIST.gov. (2015, 09 10). *(NSRL) Project Web Site*. Retrieved from National Software Reference Library: http://www.nsrl.nist.gov/

Ohio Northern District Federal Courts. (2011). *Ohio Northern District Federal Courts Rules and Orders Local Civil Rules Appendix K.* Cleveland OH: Ohio Northern District Federal Courts.

Pash, A. (2010, 11 04). *Your Smartphone Is a Better PC than Your PC Ever Was or Will Be*. Retrieved from LifeHacker: http://lifehacker.com/5681573/your-smartphone-is-a-better-pc-than-your-pc-ever-was-or-will-be

Pelline, D. G. (1998, May 18). *Smoking gun in Microsoft memos?* Retrieved from CNET News: http://news.cnet.com/2100-1001-211315.htm

Pension Comm of the Univ. of Montreal pension Plan v. Banc of Am. Sec, LLC, 685 F. Supp. 2d 456,497 (Southern District of New York January 15, 2010).

RackSpace. (2013, October 22). *Understanding the Cloud Computing Stack: SaaS, PaaS, IaaS*. Retrieved from Rackspace.com: http://www.rackspace.com/knowledge_center/whitepaper/understanding-the-cloud-computing-stack-saas-paas-iaas

Reginald W. Jackson, E. (2012). *THE BURDENS OF TECHNOLOGY: ATTORNEY DUTIES IN THE ELECTRONIC AGE.* Retrieved from Southeastern Bankruptcy Law Institute: http://www.sbli-inc.org/archive/2012/documents/T.pdf retrieved 5-20-2015

Resolution Trust Corporation Fa v. Southern Union Company Inc., 985 F.2d 196, 25 Fed.R.Serv.3D 253 (United States Court of Appeals, Fifth Circuit Mar 5, 1993).

Sableman, M. (2013, July 12). *Instant message conversation forms instant contract*. Retrieved from Thompson Colburn LLP: http://www.thompsoncoburn.com/news-and-information/internet-law-twists-and-turns/blog/13-07-12/instant-message-conversation-forms-instant-contract.aspx

SANS CSC. (2015). *Critical Security Controls - Version 5*. Retrieved from www.sans.org: https://www.sans.org/critical-security-controls/ on 05-21-2015

SAP. (2012, January). *Setting Legal Holds*. Retrieved from http://help.sap.com: http://help.sap.com/erp_hcm_ias_2012_01/helpdata/en/be/bbb6a71e934b5080c0209bc8160938/content.htm

Sara Radicati, J. L. (2013, March). *Microsoft Exchange Server and Outlook Market*. Retrieved from Microsoft-Exchange-Office-365-and-Outlook-Market-Analysis-2013-2017: http://www.radicati.com/wp/wp-content/uploads/2013/03/Microsoft-Exchange-Office-365-and-Outlook-Market-Analysis-2013-2017-Executive-Summary.pdf

Scholtes, J. (2010, 11 23). *How to become litigation ready*. Retrieved from www.aiim.org: http://community.aiim.org/blogs/johannes-scholtes/2010/11/23/how-to-become-litigation-ready

Schuler, K. C. (2009). *E-Discovery creating and managing an enterprise program: a technical guide to digital investigation and litigation support.* Syngress Pub.

Security Space. (2015, September 1). *Mail (MX) Server Survey - September 1st, 2015*. Retrieved from http://www.securityspace.com: http://www.securityspace.com/s_survey/data/man.201508/mxsurvey.html

Silvestri v. General Motors, 271 F.3d 583, 591 (4th Cir. 2001).

Small Business Administration. (2015, 07 14). *SUMMARY OF SIZE STANDARDS BY INDUSTRY SECTOR*. Retrieved from Small Business Size Standards: https://www.sba.gov/content/guide-size-standards-0

Sullivan, B. (2013, April 23). *Use your personal smartphone for work email? Your company might take it*. Retrieved from NBC News: http://www.nbcnews.com/technology/use-your-personal-smartphone-work-email-your-company-might-take-6C9558082

Sullivan, M. (2015, 07 17). *These 12 startups died in Q2. Here's why and how.* Retrieved from VentureBeat: http://venturebeat.com/2015/07/17/these-12-startups-died-in-q2-heres-why-and-how/

Taylor, C. (2015, April 30). *Trends in Information Governance: eDiscovery and Big Data*. Retrieved from www.datamation.com: http://www.datamation.com/applications/trends-in-information-governance-ediscovery-and-big-data.html

The Sedona Conference. (2010, September). *Commentary on Legal Holds: The Trigger and the Process*. Retrieved from The Sedona Conference: https://thesedonaconference.org/download-pub/3992

The Sedona Conference. (2013, December). *Best Practices Commentary on Search and Retrieval Methods.* Retrieved from THE SEDONA CONFERENCE: https://thesedonaconference.org/download-pub/3999

The Sedona Conference. (2013, December 31). *Commentary on Information Governance*. Retrieved from https://thesedonaconference.org: https://thesedonaconference.org/publication/The%20Sedona%20Conference%C2%AE%20Commentary%20on%20Information%20Governance retrieved 6-5-2015 page 130

The Sedona Conference. (2015, April 30). *The Sedona Conference Commentary on Possession, Custody, or Control*. Retrieved from https://thesedonaconference.org: https://thesedonaconference.org/publication/The%20Sedona%20Conference%20Commentary%20on%20Rule%2034%20and%20Rule%2045%20%E2%80%9CPossession%2C%20Custody%2C%20or%20Control%E2%80

The Sedona Conference Glossary. (2014, April 30). *E-Discovery and Digital Information management (Fourth Edition)*. Retrieved from https://thesedonaconference.org: https://thesedonaconference.org/download-pub/3757 retrieved 6-5-2015

Toshniwal, R. D. (2015). . Big Data Security Issues and Challenges. , 2(2). *Complexity Vol. 2*, 2.

Totenberg, N. (2014, 07 28). *When Did Companies Become People? Excavating The Legal Evolution.* Retrieved from National Public Radio: http://www.npr.org/2014/07/28/335288388/when-did-companies-become-people-excavating-the-legal-evolution retrieved 6-21-2015

U.S. Army. (1936). *George Washington University. "ATTACHMENT 2 AR 320-5, CLASSIFICATION OFC. Army Regulations (1936)"*. Retrieved from gwu.edu.: http://nsarchive.gwu.edu/radiation/dir/mstreet/commeet/meet14/brief14/tab_d/br14d1b.txt retrieved 07-07-2015

Vincent Syracuse, P. S. (2013, January 29). *E-discovery: Managing the duty to preserve voicemail*. Retrieved from Inside counsel: http://www.insidecounsel.com/2013/01/29/e-discovery-managing-the-duty-to-preserve-voicemai

W.J. Sanders III, A. C. (2000, April 27). *2000 Annual Shareholders Meeting*. Retrieved from Jerry Sanders Speech at the Annual AMD Shareholders event: http://www.pcstats.com/releaseview.cfm?releaseID=198

West v. Goodyear Tire & Rubber Co., 167 F.3d 776,779 (2d Cir 1999).

Wightman, J. (2013, October 30). *Unstructured Data: The Black Hole of Ediscovery*. Retrieved from www.jdsupra.com: http://www.jdsupra.com/legalnews/unstructured-data-the-black-hole-of-edi-20236/

Wikipedia. (n.d.). *Incident_Management*. Retrieved from https://en.wikipedia.org: https://en.wikipedia.org/wiki/incident_management retrieved 6-5-15

William Kane, G. W. (2014, November 17). *An Instant Message from the CFTC: Preserve Communications – Enforcement Is Up!* Retrieved from Baker Hostetler: http://www.bakerlaw.com/alerts/an-instant-message-from-the-cftc-preserve-communications-enforcement-is-up

William W. Belt, D. R. (2012). Technology-Assisted Document Review: Is It Defensible? *Richmond Journal of Law & Technology Volume XVIII, Issue 3*, 1-6.

Withers, K. J. (2006, Spring). Electronically Stored Information: The December 2006 Amendments to the Federal Rules of Civil Procedure. *Northwestern Journal of Technology and Intellectual Property Vol.4*, p. 171.

Wyatt, K. (2015, July 14). *Lawsuits are friends of pot opponents.* Retrieved from Durango Herald: http://www.durangoherald.com/article/20150714/NEWS04/150719823/0/News03/Pot-opponents-using-lawsuits-to-kill-industry-

Yeung, S. H. ERP II Modules. *Enterprise systems modules.* Sidney Australia.

Young, D. L. (2011). *A Primer on 30(b)(6) Depositions; A defense Perspective.* Retrieved from http://www.americanbar.org: http://www.americanbar.org/content/dam/aba/administrative/labor_law/meetings/2011/ac2011/134.authcheckdam.pdf