MITCHELL | HAMLINE School of Law

Journal of Law and Practice

Volume 6 Article 2

2013

Electronically Stored Information: What Hath God Wrought?

Roger S. Haydock

Mitchell Hamline School of Law, roger.haydock@mitchellhamline.edu

Electronically Stored Information: What Hath God Wrought?

Keywords
Electronic discovery (Law), Electronic records--Law and legislation

ELECTRONICALLY STORED INFORMATION: WHAT HATH GOD WROUGHT?

By Roger S. Haydock *

6 Wm. Mitchell J.L. & Prac. 2

This article will appear in Fundamentals of Pretrial Litigation, 9th Ed. *by Roger Haydock, David Herr, and Jeffrey Stempel (West 2013).*

The Launch[1]

Who knew way back in 1844 that Morse Code and telegrams would someday be replaced by computers and digital messages? Who anticipated even ten years ago that electronically stored information (ESI) would come to dominate much of civil discovery? And who, pray tell, understands all of its ramifications and possibilities?

This article attempts to be an introductory primer into the world of ESI discovery. Electronically stored information comprises the myriad types of documents created by computers, smart phones, tablets, recorders, and similar devices. ESI is the moniker that federal and state rules and case law designate for the information created, communicated, or stored in digital form that requires the use of computer hardware and software. Basically, ESI is defined as the content directly or indirectly generated as a series of binary bits on an electronic medium. But you knew that already, even if Samuel Morse could not possibly foresee that happening.

What is less well known, perhaps, is the enormous impact ESI is having on discovery and litigation. Due to the abundance of electronically stored information and its illusive nature, electronic discovery introduces different variables into the traditional discovery process. The geometric increase of ESI in the business world and in ordinary life experiences is spawning new legal precedent and developing technological innovations. The discovery of ESI often requires specialized knowledge and tools to preserve it from destruction and to convert it into a readable, reviewable format.

Information created and stored on computer systems, laptops, smart phones, and similar devices is readily discoverable as long as it is relevant. E-mails, social network communications, video and audio recordings, blog postings, and website searches are an especially fertile ground for discovery. Litigators need to be well prepared to seek electronic data in all cases, from the simplest of actions to complex multi-district litigation.

---

* Professor of Law, William Mitchell College of Law and Charter member, Street Legal Road Lawyers. Ben Sexton and Harrison Misewicz assisted in the writing and editing of this article and helped make it make sense. West has graciously agreed to allow the pre-publication of this article before it appears in *Fundamentals of Pretrial Litigation*. Kudos to West.

[1] "What hath God wrought" was the first public American Morse Code message sent in 1844, from Baltimore to Washington D.C.

There are limits to the discoverability of ESI beyond relevance. It also has to be readily accessible and affordable. Courts usually draw a distinction between producing electronically stored information that is available and designing new computer programs to extract data: they will require the former and deny the latter unless there is no other way to obtain the information and the costs are affordable or borne by the requesting party. Parties can negotiate to share costs, and a party can seek judicial protection from excessive expenses.

The overall goals of e-discovery are the same as physical discovery. As with paper and printed documents, you will need to understand how to best preserve, disclose, request, and respond to ESI document production procedures. While a degree in computer science would help, you can learn to understand the existence and availability of ESI and how to direct and monitor ESI discovery. You can also learn to appreciate when it is necessary to consult with and retain an expert in intellectual technology or computer forensics. To be a proficient and professional litigator, you or your law firm will need to have available a litigation support person (or team) or access to a consultant for assistance.

The ESI Policies

Before embarking on the law relevant and peculiar to ESI discovery, understanding how ESI discovery is the *same* as paper, printed, and physical discovery (summarized for our purposes as paper) places this section in perspective. Often, the discovery rules that apply to both paper documents and ESI apply with equal force and effect to both types of mediums. Originally, the rule provisions were adopted only for paper documents as they were created at a time before the advent, or even conception, of ESI.

Overall, the policies underlying the discovery rules, case law, and relevant statutes are the same regardless of whether paper or ESI documents are involved. The discovery procedures to be used should be the ones that are (1) the most convenient, (2) the least burdensome, and (3) the least expensive. These three general guidelines help in interpreting and applying the law to ESI discovery.

Civil procedure rules have recently been amended to reflect differences. A number of federal and state rules now contain specific references to electronically stored information. These specialized ESI rules augment the traditional rules applicable to paper discovery. These rules will continue to be modified as ESI discovery issues evolve and as ESI technology changes.

Another overall policy relates to privacy and its scope and preservation. Modern technology and electronic devices make it relatively easy to convert traditional private and confidential information into public and easily accessible information. Further, the notion that "private" conversations, actions, and events will remain secret and unknown to other hearers and viewers is undone by the availability of ubiquitous video devices and social networks. These shifts significantly affect privacy expectations. What a person or business may have reasonably expected to be private information is now often made public. Privacy expectations have changed and so has the law regarding it.[2] Parties are no longer ensured of having their

[2] *In re* Cunnius, 770 F. Supp. 2d 1138, 1142–49 (D. Wash. 2011) (explaining the changes in privacy and ways to craft information demands without violating an individual's Fourth Amendment rights).

private information protected from discovery because it has likely entered the public domain.[3] And parties can no longer rely on the law to enforce their expectations of privacy because the expectations are no longer reasonable.[4]

In discovery, a protective agreement and order can still be used to retain confidential information, and the law can protect and preserve this information. But, it may well be that sources not governed by the discovery rules can and will disclose the private information to the public. Clients, lawyers, parties, and litigators should anticipate that seemingly private information and conduct will be made public or will be discoverable.[5] The more informed rubric is as follows: if you compose, say, or do it, expect it to be revealed and deal with the consequences.

The Sources of ESI Law

There are several legal sources controlling the discovery of ESI. Before beginning a review of the technological aspects of ESI and a summary of the law, an overview of these sources provides an introductory perspective.[6]

Rules of Civil Procedure: Federal Rules 26 (scope), 34 (document production), 37 (sanctions), and 16 (pretrial orders), as well as similar state court rules, have been amended to provide procedures that apply exclusively to ESI discovery. These rules add to or modify the existing procedures that govern all types of discoverable information.

Court Rules: Additional procedural rules appear in local court rules and in standing orders issued by judges.[7] These provisions apply to cases venued in these jurisdictions and before these judges.

Case Law: Numerous federal and state court decisions govern the application of the discovery rules. Every federal circuit and all state appellate courts have issued some or many opinions determining what and how ESI is discoverable. These cases fall into at least six ESI categories: (1) preservation, (2) cooperation, (3)

[3] *See* Wood v. Town of Warsaw, No. 7:10–CV–00219–D, 2011 WL 6748797, at *3 (E.D.N.C. Dec. 22, 2011) (granting motion to modify subpoena despite privacy concerns over private or confidential information on nonparty's computer because such concerns may be overcome by a protective order where counsel has an opportunity to review documents for privileged information prior to production).

[4] *See id.*

[5] Mezu v. Morgan State Univ., 269 F.R.D. 565, 577 (D. Md. 2010) (deeming confidential employee data under state law not protected by privilege and discoverable, effectively waiving any exception of privacy under an employer/employee understanding).

[6] See Mancia v. Mayflower Textile Servs. Co., 253 F.R.D. 354 (D. Md. 2008), for a discussion of attorney and client duties concerning ESI discovery.

[7] Thomas Y. Allman, The Sedona Conference Inst., E-Discovery in Federal and State Courts After the 2006 Amendments 3 (2012), *available at* http://www.ediscoverylaw.com/uploads/file/2012FedStateEDiscoveryRules%28May3%29.pdf.

accessibility, (4) proportionality, (5) cost shifting, and (6) spoliation sanctions. The footnotes in this article contain the seminal cases.

Professional Responsibility Rules: The ABA Model Rules of Professional Conduct and updated state rules list acceptable and unprofessional conduct regarding ESI discovery and evidence. Model Rule 3.4(a) states that a lawyer shall not "unlawfully obstruct" access to evidence or "unlawfully alter, destroy or conceal a document or other material having potential evidentiary value" or "counsel or assist another person" to do so.[8] While this rule applies to all types of discoverable evidence, it has become especially applicable to ESI cases.

Statutes: Federal and state statutes also govern the obligations of lawyers and parties regarding ESI. An example of such legislative regulation is the federal Sarbanes-Oxley Act, which prohibits the destruction, alteration, or fabrication of any evidence that is involved in a federal investigation.[9] Regulatory rules promulgated by the Securities and Exchange Commission further require that any documents sent, created, or received in connection with an audit or a review of financial information must be retained for a period of seven years.[10] And, again, while these provisions apply to all categories of documents, they were created with ESI in mind.

Sedona Principles: The need for guidance on handling the added responsibilities of federal and state rule amendments regarding ESI and instructions on how to handle resultant litigation activities gave rise to a group of interested individuals known as The Sedona Conference.[11] Sedona is a nonprofit legal policy research and education organization that has a working group comprised of judges, attorneys, and electronic discovery experts dedicated to resolving ESI issues. Sedona has published a number of documents concerning ESI, including the *Sedona Principles*.[12] Courts have found the *Sedona Principles* instructive with respect to electronic discovery issues.

Special Masters: To oversee and assist lawyers and their clients with ESI discovery issues, judges appoint masters with technological know-how and litigation experience.[13] Litigators may request the judge to do so or the court, on its own, may designate a special master. These experts can help the litigators reach agreements on ESI protocols, monitor ESI discovery, and provide recommendations regarding ESI procedures. They can save the parties, lawyers, and court substantial savings in costs and time.

---

[8] Model Rules of Prof'l Conduct R. 3.4(a).

[9] Sarbanes-Oxley Act of 2002, Pub. L. No. 107–204, 116 Stat. 745 (codified as amended in scattered sections of 15 U.S.C. and 18 U.S.C.).

[10] 17 C.F.R. § 210.2–06 (2012).

[11] The Sedona Conference®, http://www.thesedonaconference.org (last visited Apr. 7, 2013).

[12] *See* The Sedona Conference, The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production (Jonathan M. Redgrave et al. eds., 2d ed. 2007).

[13] PIC Grp., Inc. v. LandCoast Insulation, Inc., Civil Action No. 1:09–CV–662–KS–MTP, 2011 WL 2669144, at *1 (S.D. Miss. July 7, 2011) (applying Fed. R Civ. P. 53, the court appointed a special master to review allegations of the defendant failing to comply with ESI obligations, to ensure compliance with existing discovery holds, and to recommend a course of action for the remaining discovery issues).

The Lexicon of ESI

The following terms are used frequently in e-discovery and will be encountered in resolving ESI issues:

Source Media: The electronic device on which the ESI is stored. Source media includes computers, cell phones, portable hard drives, flash drives, websites, social mediums, tablets, and cloud storage. Individuals use these devices and sources to create billions of informational electronic documents, just as you are reading this section. Some of what is being created is likely relevant to potential and actual litigation.

ESI Production Protocol: An ESI production protocol is an agreed upon format for the delivery of responsive files between parties. It is necessary to ensure compatibility of these deliverables with each party's review methodology. A workable ESI protocol is crafted by lawyers and technological experts involved in the legal dispute. It is the way the parties agree to produce requested ESI and can be modified during the litigation to resolve ESI disclosure problems.

Native Format: Native format refers to the source or original state of an electronically stored file. Throughout the discovery process, files may be converted into a variety of formats compatible with each party's review platform, with TIFF or PDF being the most common. In general, retaining documents in their native format and files is highly recommended because this is the format ordinarily used to produce documents to opposing parties.[14]

Tagged Image File Format (TIFF Image; .TIF): The TIFF file is an image format that is widely supported by image viewing applications. It is a commonly used production format for ESI because it is compatible with most major review software. TIFF image files are more difficult to alter than a native file. However, they cannot always capture the full content of a native file (e.g., the markup layers on some electronic files).

Portable Document Format (PDF): PDF is a file type allowing documents to be viewed through Adobe Acrobat Reader on any computer without the need for additional software or hardware. It is often used as a native file format and is difficult to alter. And, it is a commonly requested ESI production format. The PDF format is generally able to preserve more of an electronic document's native characteristics than a TIFF image, but is usually larger in file size.

Metadata: For each action initiated on a computer, smart phone, tablet, or other device, a significant amount of information is captured and stored, including the user initiating the action, when it was performed, geographic location, and duration of use, among others. This information is called metadata, because it is "data about data."[15] There are several types of metadata, including (1) system metadata (author, date, time information), (2) embedded metadata (hidden or internally linked data), (3) substantive metadata (also

[14] Fed. R. Civ. P. 34(b) advisory committee note, 2006 Amendment ("[T]he option to produce in a reasonably usable form does not mean that a responding party is free to convert electronically stored information from the form in which it is ordinarily maintained to a different form that makes it more difficult or burdensome for the requesting party to use the information efficiently in the litigation."); *see also* Aguilar v. Immigration & Customs Enforcement Div. of U.S. Dep't of Homeland Sec., 255 F.R.D. 350, 355 (S.D.N.Y. 2008).

[15] *Aguilar*, 255 F.R.D. at 354.

known as application metadata), and (4) ephemeral metadata (data overridden by new data, such as web searches). The amount and type of metadata stored varies with the type of device used, but it can be humongous. Computer forensic tools can often recover lost metadata.

Forensic Imaging: To prevent the destruction of electronic data during the collection of files from a source device, a forensic expert can create an exact duplicate of all files, including deleted files and metadata. This copy is called the forensic image and is the source of documents for further analysis, review, and production.

Optical Character Recognition (OCR): There are several electronic file types that store potentially relevant information but cannot be readily searched. OCR is a technology that effectively "reads" documents that do not contain easily searchable text and writes the text to a searchable format. For example, a non-searchable PDF attached to an email may contain communication critical to a case, but, without OCR, that information would not appear discoverable in an ordinary full-text search result.

Load File: This is the single file or directory of files containing all of the data necessary to ingest the collection into a desired review platform, including native files, TIFF images, metadata, OCR, and other extracted text. A load file format is specified by the agreed upon ESI production protocol to ensure compatibility with each party's review platform. It contains the ESI that is disclosed and produced.

An ESI Scenario

A scenario will help bring these definitions to life:

An employee creates a document containing a list of all her clients on a company computer in a **PDF** format, which she names as Steal-Me.pdf. This electronic information appears on the hard drive of her computer and on the company server that serves as a backup source. She has just generated **ESI** and corresponding **metadata**, which captured the time the file was created, where it is stored, and when it was last accessed, among other data. She then transfers the PDF file to a flash drive, prints the PDF to paper, deletes the PDF, and quits her job. The flash drive is now the **source media**. The next day, all of her clients stop sending work to her former employer, who becomes suspicious and hires a forensic team to investigate ESI documents she has authored. The forensic team creates a **forensic image** of her hard drive and analyzes recently created or deleted files. They locate Steal-Me.pdf, among other responsive files, and notify the employer, who contacts legal counsel to initiate suit against the former employee.

Because the files have not been converted into another format, they are considered **native files**. The law firm then relies on its IT staff with expertise in computer forensics to prepare the discovery for review. The IT experts convert the native **PDF** file to a **TIFF** image and then perform **OCR** on the image to ensure all litigators are able to search and review the potential evidence in a format compatible with their review software, according to the agreed upon **ESI** production protocol drafted by the lawyers and technical advisers from both parties. The TIFF and **OCR** are then exported to an electronic load file, which is provided from the employer party to her lawyer. This process provides both litigating parties with **ESI** and allows them to search and produce relevant disclosable and discoverable information.

The Life Cycle of ESI

ESI discovery has a life cycle. There are ten key phases to a typical time chart that aid in understanding the entire process and identify variables unique to the e-discovery process:

1. *Legal Hold*

This preservation request or demand is triggered by actual litigation, the reasonable expectation of litigation, government inquiries, or other types of disputes. The hold correspondence entails a prompt notification to custodians of potentially relevant documents, including ESI, and advises them not to tamper with or delete such data. The custodians need to understand that nothing can be deleted and everything needs to be preserved. These files and the accompanying data can be placed by each custodian in a separate electronic file to be provided to the lawyer issuing the legal hold and, if discoverable, to opposing parties. The legal hold usually overrides an existing document retention/destruction policy.

2. *Identification*

Litigators, on their own or pursuant to Federal Rule of Civil Procedure 26(f) and similar state rules, will discuss and identify the types, locations, and sources of potential discovery. Parties typically agree to terms limiting the scope of the ESI collection to a reasonable breadth proportional to the damages sought in the suit. This is known as the doctrine of proportionality. As with paper documents, the scope of discoverable ESI also needs to comply with the governing legal relevancy standards.

3. *Preservation and Recovery*

Data preservation is obviously critical to its collection. At this point, responsive custodians and devices have been identified, but the data has not yet been sequestered from its native location. Like non-electronic information, preserving the original attributes of a piece of evidence is essential. Unlike paper information, ESI is highly volatile and requires specific technological processes to maintain its integrity. Spoliation may occur in the form of the deliberate or accidental deletion of potentially incriminating emails or files by a custodian or an automated computer system. Reasonable measures need to be taken to prevent these erasures and to maintain existing discoverable information.

A primary issue regarding data recovery is whether the deleted data can be recovered. The initial answer is that it depends. It depends on the type of data, how it was deleted or overridden, the resources and money available to attempt to recover it, and the ability of the computer forensic recovery tools. So, some data can easily be recovered, much can be recovered through reasonable efforts, and some will not be recoverable.

4. *Collection*

After potential evidence has been identified, it must be collected from its source media or device for review. The goal of forensic collection is to extract potentially relevant ESI from the identified source media and, without affecting its content or metadata, create a duplicative forensic image. Proper forensic collection can

involve cracking passwords, decrypting files, and recovering deleted or tampered files. Just like in the movies.

Due to the sensitivity of forensic data and the finality of a mistake, it is critical that collection is performed quite carefully and precisely. The product of the collection is usually a hard drive containing an exact duplication of the potentially relevant information on the source media. This mirror image of the data preserves the information in a protected medium and prevents the inadvertent destruction while the materials are being collected. The forensic image can subsequently be filtered to further identify relevant information for analysis.

5. *Analysis*

After a collection has been performed, the producing party usually performs an analysis of the files before providing them to opposing counsel. Irrelevant or privileged information and other non-discoverable data will need to be identified and withheld. The litigators can mutually agree on criteria to cull non-responsive documents from the responsive information. This process can involve keyword search hits (e.g., e-mails between a custodian and their counsel), irrelevant date ranges, and non-responsive system files. Effectively filtering a collection by such criteria requires collaboration by both sides of the case and an expert in data analytics to operate the filtration technology.

6. *Processing*

While the potentially relevant ESI has now been collected from the source media, each file is still vulnerable to spoliation. Simply accessing a file in its current state would modify its metadata to reflect the current user, date, and location, overwriting the original evidence. The first step in the processing phase is to extract each file's metadata and searchable text and store it in a static database linked to the corresponding source file. The second step of processing is to convert each file into a reviewable format as set forth by the production protocol agreed upon by the litigators. Common formatting protocols include:

Numbering: Assigning each document a unique identifying number by electronic stamp (known as bates stamp) or filename.

OCR: For documents that do not contain text (e.g., PDFs), OCR is necessary to make them searchable.

TIFF Conversion: If requested in the production protocol, native files are converted to TIFF images.

This work effectively "freezes" all electronic content and converts it into a format useful for review. After data is processed, it is exported to a load file and is then delivered to all responsive parties. The majority of the processing phase will be performed by a litigation support person or team or a retained vendor.

7. *Review*

After a load file is created for internal review or is received from the other side, it needs to be imported into a document review platform. At minimum, a review platform is software that allows litigators to view electronic documents and store pertinent information. Typically, the interface consists of a document viewer

pane, a list of the documents' original metadata, and a coding pane consisting of fields and designations used to record relevant information about each document. A pane is a region of the software's interface with a dedicated purpose. Most major review platforms may be accessed through highly secure websites, allowing multiple litigators to review a document set from any location with Internet access.

Review workflows vary for each case but usually involve an administrator assigning batches of documents to reviewers, who analyze documents and records information relevant to the case. A reviewing litigator may also be looking for privileged documents to exclude from the review or to redact privileged content from relevant documents. The review phase is typically a linear process and may take a few weeks to many months—yes, you read that correctly—depending on the volume of discovery.

8. *TAR or Manual Review*

Technologically assisted reviews (TAR) may be an efficient and effective way to identify relevant discoverable information in very large document sets. Properly designed search terms and a responsive computerized system may be the best or only way to review the reams of available ESI information. Using such a system, attorneys initially review a sample of the document universe, assigning designations for relevance and other key attributes. Based on these decisions, the computer performs an algorithmic analysis of the entire document universe and assigns each document a designation (e.g., hot, background, junk). After the computer codes the documents, a sample is generated to verify its accuracy. The system can then be "trained" to produce a desirable accuracy level and error threshold. At that point, the lawyers can then prioritize the document review or accept the produced results as final.

Manual review—individuals looking on their own for relevant information—is a common option, but the enormity of the task often requires some technological assistance. There may not be a need for a sophisticated TAR system, but some computerized based process which augments manual reviews may be needed. Another option is sampling, with a TAR-like system reviewing selective ESI. If that review produces relevant information, then expanded sampling or more extensive reviews would be warranted.

9. *Production*

After the review phase is complete, documents deemed responsive to the dispute are assigned unique identifying production numbers, transferred or exported from the review platform to a separate new file, and delivered to opposing counsel and the court according to the predefined ESI production protocol. Based on the type of data being produced and each party's review methodology, the protocol may include production of native files, TIFF images, PDFs, and load files.

A well-designed ESI production protocol can make this process relatively easy and affordable. Often, a production protocol may require unnecessary steps that can be burdensome and costly to both sides. For example, a protocol requiring only bates- stamped TIFF images may seem to simplify the process at the time of the agreement, but it could add a significant amount of unnecessary time and cost to the production. On the other hand, if redactions were made in the review platform, TIFF images or PDFs must be produced to prevent privilege exposure. The best way to minimize costs and risk to both sides is to identify variables preemptively and tailor the protocol to your case.

10. *Presentation*

There are several commercial software platforms designed for the presentation of electronic evidence. After the evidentiary set has been identified, a litigation support specialist can provide the technical support necessary to prepare the evidence for the court or deposition. Litigators need to work closely with their technical support staff to ensure that the presentation follows their arguments and meets their standards for presentability.

And now you know, almost for sure, that you will need a technology adviser to help you through all this to get it right, unless you are one yourself.

The Discoverability of ESI

The scope of ESI discovery is the same as other information under the federal or applicable state rules. Federal and state courts have interpreted and applied these rules and developed various approaches to ESI discovery.[16]

Procedural ESI Rules

Federal Rule 26(a)(1) specifically makes electronically stored information subject to the same initial disclosure requirements for paper documents.[17] Federal Rule 26(b)(2)(B) explicitly extends discovery to electronically stored information.[18] This rule specifies: "A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost," unless there exists good cause for such production.[19]

This latter rule introduces two specific factors when considering ESI discovery: its reasonable "accessibility" and any "undue burden or cost" incurred in its production.[20] Types of ESI that may not be discoverable include data from obsolete computer devices (have you heard of Wang?), deleted information (not spoliation), and other data that is not electronically searchable (where's Hal?). Good cause may be established in an effort to recover this data because the benefit of the disclosed information outweighs the burden and expense of producing it or because the relevant data is not available from any other

[16] Point Blank Solutions, Inc. v. Toyobo Am., Inc., No. 09–61166–CIV, 2011 WL 1456029, at *4 n.3 (S.D. Fla. Apr. 5, 2011) ("Judge Scheindlin is in the Second Circuit, which has some rules which are different than those in our Eleventh Circuit.").

[17] Fed. R. Civ. P. 26(a)(1).

[18] Fed. R. Civ. P. 26(b)(2)(B).

[19] *Id.*; *see also* Star Direct Telecom, Inc. v. Global Crossing Bandwidth, Inc., No. 05–CV–6734T, 2012 WL 1067664, at *8 (W.D.N.Y. Mar. 22, 2012) (issuing sanctions for failing to preserve other sources of requested ESI after discovery backup tapes would not be a viable source).

[20] *See, e.g.*, Clean Harbors Envtl. Servs. v. ESIS, Inc., No. 09 C 3789, 2011 U.S. Dist. LEXIS 53212, at *19–21 (N.D. Ill. May 17, 2011) (requiring the requesting party to share the cost of production if they insisted on conversion of files from obsolete off-site backups).

source.[21] Federal Rule 34(a)(1)(A) provides that ESI must be produced as "stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form."[22] And, Rule 34(b)(2)(E) states that "a party must produce [ESI] in a [format] in which it is ordinarily maintained or in a reasonably usable [format]"[23] and only in one format.[24]

Further, Rule 34(b)(1)(C) allows the requesting party to specify the form in which ESI is to be produced.[25] Rule 34(b)(2)(D) permits the responding party to object to the proposed format.[26] If no format is specified or if there is an objection, the responding party must identify the intended format to be used for disclosure.[27]

Additional rules govern privilege and work product data that may have been inadvertently or mistakenly produced. ESI may well contain privileged or confidential information that is obvious or is encrypted and that is mingled with or attached to discoverable information and documents. Federal Rule 26(b)(5)(B) details the procedure for asserting claims of privilege and other work product and the requirements on the receiving party to return, sequester, or destroy the non-discoverable or protected information.[28] Issues relating to the waiver of privilege and work product claims may be resolved by the parties or by a court.

These rules require the responding party to furnish ESI in a manner understandable to the requesting party and to bear the cost and expense of compiling the data and translating them into a readable printout or some other machine-readable format.[29] The rules also allow the responding party to refuse to provide ESI if it is not readily accessible either because it is too burdensome to produce or because it costs too much to produce. The parties may confer and mutually agree on a limited scope of ESI discovery or split the costs of production. If unable to agree, the court may decide the issues based on a Rule 37 motion for production enforcement[30]or a Rule 26(c) protective order.[31]

---

[21] Camesi v. Univ. of Pittsburgh Med. Ctr., Civil Action No. 09–85J, 2010 WL 2104639, at * 7 (W.D. Pa. May 24, 2010) (providing that the burden is on the requesting party to show that the need for the ESI outweighs the burden or cost of producing it).

[22] Fed. R. Civ. P. 34(a)(1)(A).

[23] Fed. R. Civ. P. 34(b)(2)(E)(ii)

[24] Fed. R. Civ. P. 34(b)(2)(E)(iii); *see also* Covad Commc'ns Co. v. Revonet, Inc., 267 F.R.D. 14, 20 (D.D.C. 2010) (stating that the parties had "bigger fish to fry" than reproducing documents that are already in a usable format into a format that includes metadata).

[25] Fed. R. Civ. P. 34(b)(1)(C); *see also* Romero v. Allstate Ins. Co., 271 F.R.D. 96, 106 (E.D. Pa. 2010).

[26] Fed. R. Civ. P. 34(b)(2)(D).

[27] *Id.*

[28] Fed. R. Civ. P. 26(b)(5)(B).

[29] Adams v. Dan River Mills, Inc., 54 F.R.D. 220, 222 (W.D. Va. 1972).

[30] Fed. R. Civ. P. 37; *see also* Susquehanna Commercial Fin., Inc. v. Vascular Res., Inc., No. 1:09–CV–2012, 2010 WL 4973317, at *1, *12–15 (M.D. Pa. Dec. 1, 2010).

[31] Fed. R. Civ. P. 26(c).

Federal Rule 26(f) encourages parties to discuss and resolve these ESI matters at the early stages of the case during discovery planning discussions as well as during ongoing litigation.[32] Rule 16(b)(3)(B) references electronically stored information as part of the overall disclosure and discovery process.[33] Similar state court rules provide parties with the same or similar duties, rights, and procedures.

Judicially Imposed ESI Factors

Courts have crafted factors especially applicable to electronically stored information which augment the above civil procedure rules. Judges take into consideration these factors in determining whether ESI needs to be disclosed or discovered. The following list synthesizes and summarizes these numerous factors. Courts vary in relying on or ranking these inclusive factors.[34] The applicable precedent and the facts and circumstances of each case determines which of these factors apply and control the outcome:

- The breadth of the request and the extent to which the request is specifically tailored to discover helpful information.

- The availability of the information from other available sources.

- The cost of production in total expenses and as compared to the amount in controversy.

- The resources of each party as compared to the total cost of discovery.[35]

- The relative ability of each party to control costs and incentives to do so.

[32] Fed. R. Civ. P. 26(f); *see also In re* Facebook PPC Adver. Litig., No. C09-03043 JF (HRL), 2011 U.S. Dist. LEXIS 39830, at *3–11 (N.D. Cal. Apr. 6, 2011) (ordering court production of privileged source code and continued cooperation between litigants with handling protected information).

[33] Fed. R. Civ. P. 16(b)(3)(B).

[34] Point Blank Solutions v. Toyobo Am., Inc., No. 09-61166-CIV, 2011 WL 1456029, at *4 n.3 (S.D. Fla. Apr. 5, 2011).

[35] Boeynaems v. LA Fitness Int'l, LLC, Civil Action Nos. 10-2326 and 11-2644, 2012 U.S. Dist. LEXIS 115272 (E.D. Pa. Aug. 16, 2012) (class action plaintiffs were expected to pay costs for discovery given the asymmetrical balance of discoverable information).

- The materiality of the data and the benefits to the party seeking the information.

- The importance of the issues.

- The complexity of the case.

- The need to protect privileged information, work product, trade secrets, or other confidential information.

- The ease of accessing the data. [36]

- The extent to which the production would disrupt normal operations of the responding party.

- Whether the ESI is in a readily accessible format or needs to be translated into another format.

- Whether the information or software needed to produce the data is proprietary or invades confidential business information.

- Whether the translation, if necessary, is too burdensome or costly.

- Whether the requesting party has offered to pay some or all of the production costs. [37]

[36] Adair v. EQT Prod. Co., No. 1:10cv00037, 2012 WL 1965880, at *5 (W.D. Va. May 31, 2012) (denying a protective order after the movant had asserted that ESI was inaccessible but failed to demonstrate that filtering by a custodian would be a burdensome expense).

[37] *In re* Ricoh Co., Patent Litig., 661 F.3d 1361, 1366 (Fed. Cir. 2011).

- Whether the data is stored in a way that is not reasonably warranted by legitimate personal, business, or non-litigation reasons.

- Whether the data was stored in a manner designed to defeat discovery.

- Whether the responding party was properly aware of potential or actual litigation in storing or discarding data.[38]

- Whether the responding party has violated any protocols or rules regarding preservation or spoliation.[39]

Preserving ESI

Parties to potential or pending lawsuits, official government proceedings, and reasonably foreseeable litigation have an obligation to preserve documents, paper, and electronically stored information.[40] This obligation usually extends to arbitration and administrative procedures as well. Representative lawyers will issue litigation holds to their clients advising them in no uncertain terms to retain and not destroy or delete information. This obligation extends to all parties and their employees and agents and to lawyers as well, in house or retained. Generally, the litigation hold applies to backup mediums that are accessible, but not to systems that are inaccessible, which includes backups maintained solely for the purpose of disaster recovery. These preservation obligations override document retention/destruction policies that become suspended.

Because of the nature of ESI, these obligations are especially vital to preserving relevant and potentially discoverable information. Courts are imposing severe sanctions for failures to comply with these responsibilities. Because of these developments, the wisest practice is to err on the side of preserving and not deleting or destroying documents, even if there is a reasonable document destruction policy in place.[41] Even if not required by law to be preserved, fact finders and decision makers are likely to conclude that the

[38] Goodman v. Praxair Servs., Inc., 632 F. Supp. 2d 494 (D. Md. 2009).

[39] Victor Stanley, Inc. v. Creative Pipe, Inc., 269 F.R.D. 497 (D. Md. 2010).

[40] *See* Micron Tech., Inc. v. Rambus Inc., 645 F.3d 1311, 1324 (Fed. Cir. 2011) (providing that litigation is foreseeable if "overcoming [potential] contingencies was reasonably foreseeable").

[41] *Victor Stanley, Inc.*, 269 F.R.D. at 524.

deleted or destroyed data must have contained information harmful to the discarding party. These adverse inferences may be imposed by law or by common sense.

A party may be able to have a third person or business, not a party to the case, retain and not discard ESI.[42] Federal Rule 45 and similar state rules allow a party to subpoena documents, including electronically stored information, from a non-party.[43] A lawyer for a party can send a preservation request to a non-party asking that certain documents be preserved before the subpoena is issued and served. The non-party may or may not have a duty to do so or the adverse consequences for not complying may be insignificant. But, often the non-parties will comply to be fair and to avoid becoming embroiled in litigation efforts to retrieve that data from them.

The ESI Doctrines

There are four primary doctrines that govern or assist in controlling the scope and cost of ESI discovery: cooperation, accessibility, affordability, and proportionality.[44]

Cooperation: Discovery rules, judicial opinions, and best practices have developed protocols for lawyers and their clients to seek mutual cooperation and reach reasonable agreements regarding the production of ESI. Meet and confer rules, pretrial orders, discovery plans developed by lawyers, and special master appointments are effective ways to reach cooperative solutions to the myriad of problems inherent in ESI discovery. Participants include experts in technology and computer forensics to develop ways and means of producing accessible and affordable ESI.[45]

Accessibility: As explained previously, the key to usable ESI discovery is its accessibility. A responding party has an obligation to provide ESI in a readily accessible format. This may be the native format of the ESI or another format that is cost effective. Because of the various formats that compose ESI, the specific disclosure format is based on what the requesting party has reasonably suggested, any objections by the responding party, what format the data is in, what format may be able to translate the data, and the costs associated with these processes.

---

[42] *See* Columbia Pictures, Inc. v. Bunnell, 245 F.R.D. 443, 447 (C.D. Cal. 2007) (quoting Fed. R. Civ. P. 34 advisory committee note, 2006 Amendment) (affirming discoverability of ESI in RAM because "Rule 34 requires no greater degree of permanency from a medium than that which makes obtaining the data possible"). Courts have required third parties to produce information from quickly erasing RAM, which a party to the case had a legal right to access.

[43] Fed. R. Civ. P. 45.

[44] Merriman v. Minn. Life Ins. Co., No. 12-C-621, 2012 U.S. Dist LEXIS 124854, at *9–11 (E.D. Wis. Aug. 31, 2012) (explaining that the Seventh Circuit has started a pilot program for ESI discovery issues wholly based on the *Sedona Principles* with mandatory adherence from all parties appearing before the court).

[45] Fed. R. Civ. P. 34 advisory committee note, 2006 Amendment; *see also* S2 Automation LLC v. Micron Tech., Inc., No. CIV 11–0884 JB/WDS, 2012 WL 3656454, at *18–19 (D.N.M. Aug. 9, 2012) (stating that prior to any court involvement in ESI disputes, parties should seek and resolve disputes before the expense and work occurs, and additional time may be required to allow a responding party to assess appropriate forms of production).

Affordability: Also, as discussed previously, the expense involved with ESI discovery is often a factor in its discoverability. Ordinary document production can be quite a costly endeavor, and ESI discovery can easily add extensive or mind-boggling costs to this process. The federal and state rules that provide parties with protections against unduly expensive procedures can be used to control these costs. If the parties and their lawyers cannot mutually agree on ways to reduce expenses, a court can intervene to determine what is fair, affordable, and appropriate given the issues at stake.

Proportionality: This concept has always been a factor in document production, including paper documents. The scope of discoverable information ought to be based on the significance of the information sought and the costs involved in producing it relative to merits of the claims and defenses. If the process and expense outweigh the benefits of the sought-after information, the doctrine of proportionality provides that such information, which may be relevant, is not discoverable. Factors courts rely on in determining proportionality include:

- The total cost of production compared to the amount in controversy or the significance of the legal issues.

- The total cost of production compared to the resources available to each party.

- The financial ability of a party to afford the expenses compared to the value of the information to the other party. [46]

The outcome of these balancing tests rests on the specific needs and interests of each case.[47]

ESI Cost Shifting

One way to alleviate affordability and proportionality issues is to share expenses depending upon the financial wherewithal of the parties or shift production costs to the requesting party. Federal and state rules explicitly empower the parties, their lawyers, and the court to determine what is the fairest way of distributing costs.[48] Factors that have been developed to provide a fair and balanced approach include:

[46] *In re* Aspartame Antitrust Litig., 817 F. Supp. 2d 608 (E.D. Pa. 2011) (detailing different standards for accessibility across several jurisdictions and determining whether the request is proportionate to the amount in dispute).

[47] Chenault v. Dorel Indus., Inc., No. A–08–CA–354–SS, 2010 WL 3064007 (W.D. Tex. Aug. 2, 2010).

[48] *See* Plantronics, Inc. v. Aliph, Inc., No. C 09–01714 WHA (LB), 2012 WL 5269667, at *12 (N.D. Cal. Oct. 23, 2012) (providing how and when it is appropriate for a court to tax ESI discovery costs).

- How much can a party afford to pay for discovery?

- Is it fair to impose extensive ESI discovery costs on the responding party or the requesting party?

- Which party, if any, is more responsible for the problems involved with ESI production?

- What is the fairest way to share, split, or impose discovery expenses?

ESI Spoliation

Parties and their lawyers have always been under a duty to preserve and not destroy relevant documents. It is possible, but more difficult, to get rid of paper evidence; usually it requires shredding, burning, and other forms of physical destruction. These processes are more difficult to do privately or without the assistance of others. Electronically stored information can much more easily be deleted in private and through seemingly non-discoverable ways. The temptation to do so may be too tempting, resulting in the spoliation of otherwise discoverable information.

Courts have been made aware of these realities and have responded with sanctions imposed against such improper conduct.[49] The sanctions are authorized by the inherent power of the court and pursuant to Federal Rule 37 and similar state rules.[50] Usually, spoliation sanctions will be considered if there was a clear duty to preserve, if there exists a culpable failure to do so, and if there is a reasonable probability that the loss of evidence will materially prejudice the adverse party. Courts typically design a sanction to deter parties from engaging in spoliation, place the risk of losing on the party who wrongfully created the risk, and restore the prejudiced party to the position the party would have been in but for the wrongful destruction.

These sanctions, in some jurisdictions, have been severe and imposed not only on parties but also on their lawyers. There are a variety of sanctions at the court's disposal, and the various federal circuit courts and state appellate courts continue to develop their own applicable precedents.[51]

[49] Qualcomm Inc. v. Broadcom Corp., No. 05cv1958–B (BLM), 2010 WL 1336937, at *1–2 (S.D. Cal. Apr. 2, 2010) (dismissing sanctions against outside attorneys after showing that improper conduct was the client's fault).

[50] Fed. R. Civ. P. 37.

[51] *See, e.g.*, Victor Stanely, Inc. v. Creative Pipe, Inc., 269 F.R.D. 497 (D. Md. 2010).

The applicable rules and case law may exonerate a party if ESI has been deleted or discarded. Federal Rule 37(e) states that a court may not impose sanctions if the electronically stored information was destroyed or lost because of the "routine, good faith operation of an electronic information system."[52] It is proper to periodically modify, overwrite, or delete ESI in the normal course of events. Businesses and individuals may do so in the ordinary course of their work or life. The rules do not intend to punish them for routine, good faith practices.[53] A litigation hold or preservation request can override these practices and place a potential party on notice that litigation is foreseeable. It may come down to two questions: what do they know and when did they know it?

Who knew, indeed.

[52] Fed. R. Civ. P. 37(e).

[53] Ferron v. EchoStar Satellite, LLC, 410 F. App'x 903, 911–12 (6th Cir. 2010).