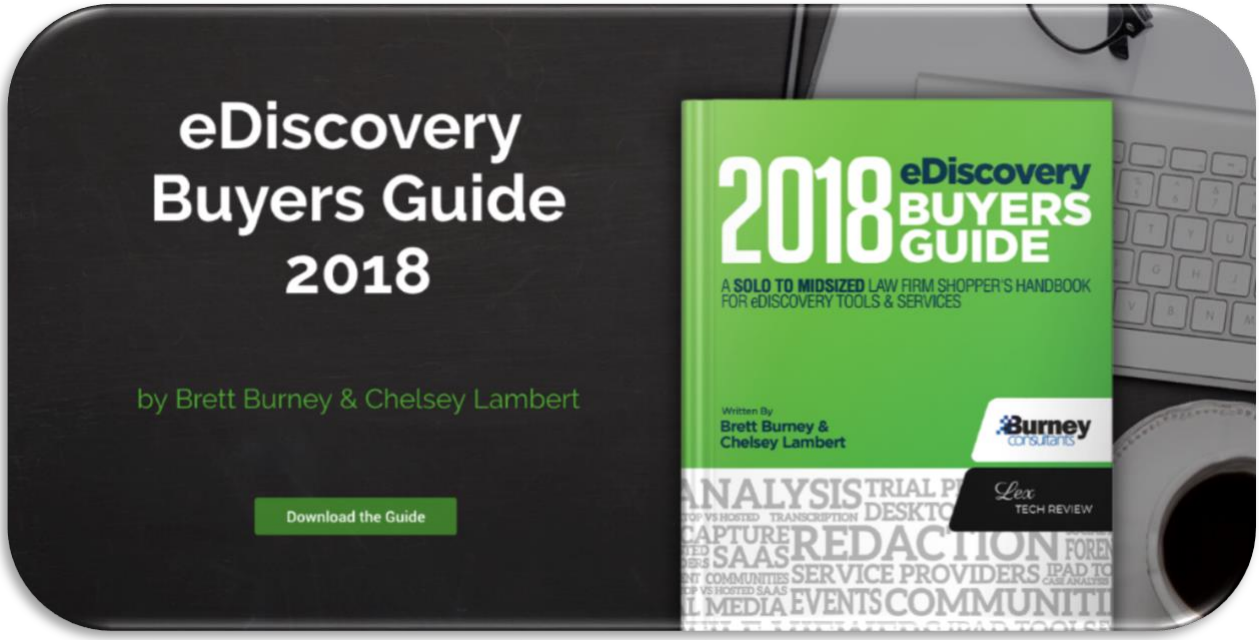
eDiscovery for the Small Firm

Colorado Bar Association Webinar
August 21, 2018

Brett Burney
Burney Consultants LLC
burney@burneyconsultants.com

www.ediscoverybuyersguide.com

How Did We Get Into This E-Mess? I'm Supposed To Be Practicing Law!.....3
The Federal Rules Were Amended To Address The Problems (Twice!)..... 8
States Love E-Discovery Too! (even Colorado!) 11
The E-Discovery Ethical Obligations You Can't Escape 12
How To Convince Your Client To Preserve ESI When All They Want To Do Is Delete It 17
How To Avoid Being Cyber-Bullied By The Other Side In E-Discovery..... 22
Data Collections Without Data Disasters..... 29
E-Discovery Tools For Mere Mortal Lawyers 34



Download the **FREE** eDiscovery Buyers Guide

A Solo to Midsized Law Firm Shopper's Handbook for eDiscovery Tools & Services

www.ediscoverybuyersguide.com

Authored by
Brett Burney and **Chelsey Lambert**

Wouldn't it be nice if there was a handbook to explain when and how to use eDiscovery solutions without spending hundreds of thousands of dollars?

For solo, small and mid-sized law firms finding answers to eDiscovery tech questions hasn't been an easy task.

Brett Burney (Burney Consultants LLC) and Chelsey Lambert (Lex Tech Review) have teamed up to publish the 2018 eDiscovery Buyers Guide to solve exactly this problem.

How Did We Get Into This E-Mess? I'm Supposed To Be Practicing Law!

Our world is digital.

While we still cherish paper in the legal profession, the vast majority of all "printed" documents today are initially created electronically (e.g. email, Microsoft Word, Excel, WordPerfect, etc.). If you're holding a paper document in your hand, it's because someone printed a digital document.

The Federal Rules of Civil Procedure were amended December 1, 2006 to officially recognize that "electronically stored information" (ESI) is equivalent to information stored in paper form.

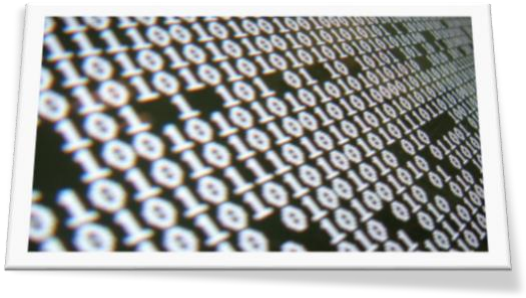
In their 2005 Notes, the FRCP Advisory Committee stated unequivocally:

> **"Rule 34(a) is amended to confirm that discovery of electronically stored information stands on equal footing with discovery of paper documents."**

The 2006 FRCP amendments dictated changes in how discovery is conducted in civil litigation regarding discussion about how ESI is to be collected, preserved, and produced.

The FRCP Advisory Committee also noted:

> **"Electronically stored information (ESI) has important differences from information recorded on paper:**
>
> **First, ESI is stored in exponentially greater volume than hard-copy documents;**
>
> **ESI is dynamic, rather than static;**
>
> **and ESI may be incomprehensible when separate from the system that created it."**



What Does The Little "e" Mean?

While the term "e-discovery" or “eDiscovery” sounds intimidating, it is simply the application of traditional discovery practices applied to the contemporary digital world.

Black's Law Dictionary defines discovery as:

> *"...a pre-trial device that can be used by one party to obtain facts and information about the case from the other party in order to assist the party's preparation for trial."*

E-discovery does nothing to change this definition, but the explosion of digital data does require the legal world to employ new and inventive strategies to achieve the same goal as traditional discovery.

Rule 1 of the Federal Rules of Civil Procedure (FRCP) states that all of the rules are to be *"construed and administered to secure the just, speedy, and inexpensive determination of every action and proceeding."* In order to secure the just, speedy, and inexpensive determination of law, it is imperative to understand the intricacies of e-discovery so that we can logically apply cost containment where appropriate. In other words, we don’t want any expensive surprises or cost runaways.

Even the bench has recognized the importance of raising FRCP 1 to rein in the runaway costs involved with e-discovery. Magistrate Judge Andrew Peck of the Southern District of New York wrote in an October 2011 article for Law.com that *"in my opinion, computer assisted coding should be used in those cases where it will help 'secure the just, speedy, and inexpensive' (Fed. R. Civ. 1) determination of cases in our e-discovery world*[1]*."*

It's obvious that e-discovery is not that different from the traditional practices of discovery that have evolved in this country's adversarial system of law for decades. The little "e" however, causes us to re-consider some of the outdated approaches to discovery that existed before technology consumed our lives.

[1] Search, Forward, Law.com, October 1, 2011 (http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202516530534)

Burney consultants
www.burneyconsultants.com
(216) 245-1414
burney@burneyconsultants.com

What is ESI?

It's important to understand that our definition of a "document" is changing and evolving.

For decades, FRCP 34 was titled **"Producing Documents, and Tangible Things..."** because we all had a solid, conceptual understanding of a "document" - usually defined by the four corners of an 8½" x 11" sheet of paper.

That was fine as long as we created documents by handwriting, or used a typewriter to create documents on physical paper. But then the world started using electronic word processors, and sending email, and texting on our mobile devices. All of these new-fangled electronic forms of communication challenged our concept of a "document" and "tangible things."

Of course you can print out a document created in Microsoft Word, or print out an email message, or even print out web page. But the problem then is that a printout of a digital file is not the original document - it's a printed representation, and now is separated from the metadata and other information that accompanies a digital file.

In many cases, digital files are never meant to be printed - have you ever gone through the nightmare of printing a Microsoft Excel spreadsheet?

*Does this look familiar? Why is printing out an Excel spreadsheet such a nightmare? Because a spreadsheet is **NOT** meant to be printed!*

In 2006, the title of FRCP 34 was amended to recognize digital files with the phrase "electronically stored information" and now states:

> **"Producing Documents, Electronically Stored Information and Tangible Things..."**

The phrase ***electronically stored information*** (ESI) is now used to encompass the vast variety of digital and electronic files that are discoverable today.

We are comfortable that ESI includes more document-like files such as:

- Microsoft Word documents
- Email messages
- PDF files
- Text files

But we are less agreeable about how to collect, preserve, review, and produce ESI when we discuss information such as:

- Microsoft PowerPoint presentations
- Websites
- Text messages
- Instant messages
- Audio files (.MP3, .WAV)
- YouTube videos
- Skype conversations
- Digital pictures (.JPG, .GIF)
- Facebook feeds
- Twitter feeds
- GPS coordinates
- The Internet of Things data

But the fact is that all of these items (and much more!) fall under the definition of ***"electronically stored information"*** and are required to be collected, preserved, reviewed, and produced in a litigation matter.

In 2006, the drafters of the FRCP amendments could not even envision new forms of ESI such as Twitter, SnapChat, Whatsapp, and the variety of other forms of ESI that have popped up in the last 8-10 years ... and that will continue to appear in the future.

How Does E-Discovery Differ From Traditional Methods Of Discovery?

One of the biggest differences between electronic discovery and traditional paper discovery is the immense volume we see with electronically stored information. While it takes several store rooms, many boxes, and loads of money to store millions of documents in paper form, those same documents can easily fit on a computer hard drive the size of a paperback novel.

And because it's so easy (and inexpensive) to store information in digital form, people tend to keep so much more than ever before. This means there will be that much more information to cull through during the discovery phase of litigation.

On the other hand, electronic discovery is really just discovery with an "e" in front of it. The addition of the letter "e" does not significantly change the traditional rules of discovery (although it has AMENDED the federal and state rules), it just requires a different strategy to play the game.

The biggest difference that many people point out is that dealing with ESI requires a level of collaboration between litigating parties that is unprecedented. Lawyers are taught from the first day of law school to be adversarial in nature. The thought of collaborating and cooperating with an opposing party is very unsettling to many lawyers, even distasteful to some.

It is becoming apparent, however, that collaborating on logistical issues such as the production of electronically stored information is the only way that the legal profession is going to successfully embrace electronic discovery.

For more information on the need to seek cooperation on e-discovery issues, please see the The Sedona Conference Cooperation Proclamation (http://bit.ly/75xVPA).

The Federal Rules Were Amended To Address The Problems (Twice!)

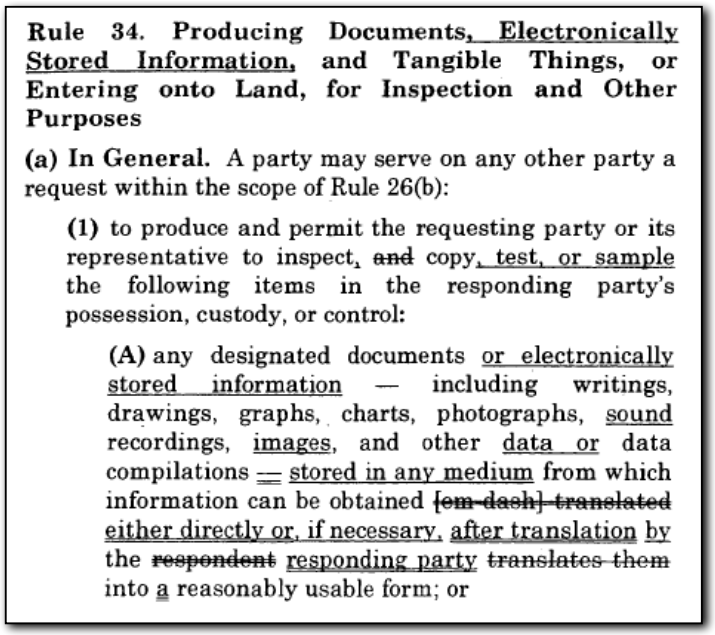
2006 Amendments

On December 1, 2006, the Federal Rules of Civil Procedure received some of the most sweeping amendments to bring the Rules into the 21st-century, and apply them to the reality of a world comprised of digital and electronic communication.

Establishing that Electronic Information is Discoverable
One of the primary amendments to the FRCP was the fact that the Advisory Committee wanted to absolutely and definitively establish that electronic information is discoverable and on par with paper discovery.

In Rule 34, they added the phrase "*electronically stored information*" to the title which up until that time, at only referenced "documents" and "tangible things."

The phrase was meant to include any type of information that can be stored electronically, with the foresight that the phrase was broad enough to cover any current type of computer based information, and flexible enough to encompass future changes and technological developments.



Rule 34. Producing Documents, Electronically Stored Information, and Tangible Things, or Entering onto Land, for Inspection and Other Purposes

(a) In General. A party may serve on any other party a request within the scope of Rule 26(b):

(1) to produce and permit the requesting party or its representative to inspect, ~~and~~ copy, test, or sample the following items in the responding party's possession, custody, or control:

(A) any designated documents or electronically stored information — including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations — stored in any medium from which information can be obtained ~~[em-dash] translated~~ either directly or, if necessary, after translation by the ~~respondent~~ responding party ~~translates them~~ into a reasonably usable form; or

Early Attention to Electronic Discovery Issues
Recognizing that early attention to electronic discovery issues was paramount to the success and speedy resolution of issues, and to lower the frustration level of parties dealing with these issues, the Advisory Committee included several points to emphasize the need to discuss these issues early on the litigation process.

First, Rule 26(a)(1)(B) added electronically stored information to the list of items to be included in a party's initial disclosures.

Second, Rule 16(b)(5) adds provisions for the disclosure of discovery of electronically stored information as an item that maybe appropriately included in the court's scheduling order.

And lastly, Rule 26F(f) expands the list of issues that must be discussed as a part of the meet and confer process, and includes a requirement that parties develop a discovery plan that addresses issues relating to the discovery electronically stored information including the form or forms in which it will be produced.

Format of Production
Rule 34(b) address is the format of production of electronically stored information, and permits the requesting party to designate the form or forms in which it wants electronically stored information produced. The rule does not *require* the requesting party to choose a form of production, however, since a party may not have a preference or may not know what form the producing party uses to maintain their electronically stored information.

If a party does not specify a form of production, the responding party must notify the requesting party of the form in which they intend to produce the electronically stored information with the option of producing either 1) in a form in which the information is ordinarily maintained, or 2) in a reasonably usable form.

Collecting and Producing Electronically Stored Information from Sources that are "Not Reasonably Accessible"
Amended Rule 26(b) seeks to provide a balanced, equitable approach to resolve the unique problem presented by electronically stored information which is often located in a variety of locations of varying accessibility.

Rule 26(b)(2)(B) creates a two tiered approach to the production of electronically stored information, making a distinction between that which is reasonably accessible, and that which is not. Under the new rule, a responding party need not produce electronically stored information from sources that it identifies as "not reasonably accessible" because of undue burden or cost. This does not, however, relieve the party from *PRESERVING* the potentially relevant electronically stored information.

"Safe Harbor"
Because the Advisory Committee was concerned about the potential of relevant electronically stored information being easily deleted or modified, they included the new Rule 37(f) which became known as the "Safe Harbor" provision.

This rule provided that, absent exceptional circumstances, the court may not impose sanctions on a party for failing to provide electronically stored information lost as a result of the routine good faith operation of an electronic information system. It specifically responds to the routine modification, overriding, and deletion of information that attends the normal use of electronic information systems.

The Advisory Committee further observed that such features are "essential to the operation of electronic information systems," and that there is no "no direct counterpart in hardcopy documents."

2015 E-Discovery Amendments to the FRCP

In 2006, the FRCP received major amendments to recognize the role of electronically stored information (ESI) in litigation matters. By adding the phrase "electronically stored information" to Rule 34, the FRCP Advisory Committee explained that it was to "confirm that discovery of electronically stored information stands on equal footing with discovery of paper documents. "

Other changes to accommodate ESI included an emphasis for both parties to discuss the discovery and production of ESI early in the process, including the "form or forms" in which ESI would be produced to the other party. The addition of Rule 37 to the FRCP allowed a Court to impose sanctions on parties who failed to properly preserve ESI for litigation.

Almost 10 years later, the FRCP Advisory Committee examined the impact of the so-called "e-discovery amendments" and have now submitted a handful of significant changes that were approved by Congress on December 1, 2015.

> **First,** in FRCP 1 the Advisory Committee deemed it important to encourage increased cooperation between parties especially when dealing with ESI
>
> **Second,** the Advisory Committee placed more of a spotlight on the concept of "proportionality" in litigation that involves ESI. This concept already existed in the FRCP but the amendments now includes some specific elements that the Court can consider.
>
> **Lastly,** FRCP 37 was almost completely re-written to create a more effective and consistent mechanism for Courts to impose sanctions when dealing with the loss of ESI.

States Love E-Discovery Too! (even Colorado!)

There has been a lot of attention placed on the "e-discovery amendments" to the Federal Rules of Civil Procedure that it seems like most people have forgotten that the majority of attorneys in the U.S. litigate in state courts. The FRCP amendments have certainly created their place in history, but what use are they to attorneys who practice in state courts?

The good news is that all of the long, long hours of intense discussion and scrutiny that the amendments to the Federal Rules experienced provide a solid foundation for the establishment of similar state rules. This is evident in the Prefatory Note to the "Uniform Rules Relating to the Discovery of Electronically Stored Information" as drafted by the National Conference of Commissioners on Uniform State Law (NCCUSL):

> "... the Drafting Committee decided not to reinvent the wheel. It was the Drafting Committee's judgment that the significant issues relating to the discovery of information in electronic form had been vetted during the Federal Rules amendment process. Accordingly, this draft mirrors the spirit and direction of the recently adopted amendments to the Federal Rules of Civil Procedure. The Drafting Committee has freely adopted, often verbatim, language from both the Federal Rules and comments that it deemed valuable. The rules are modified, where necessary, to accommodate the varying state procedures and are presented in a form that permits their adoption as a discrete set of rules applicable to discovery of electronically stored information."

While the vast majority of states have simply adopted the language from the Federal Rules of Civil Procedure, Colorado is one of a handful of states that designed their own rule to apply to electronic discovery (although the language and intent is very similar to the Federal Rules).

On July 1, 2015, the scope of discovery under Colorado Rule of Civil Procedure 26(b)(1) was amended with language nearly identical to the changes in proportionality that is nearly identical to what the Federal Rules of Civil Procedure adopted in December 2015.

On July 2015, Rule 16(b)(15) was also added to the Colorado Rules of Civil Procedure to directly address electronically stored information and states in full:

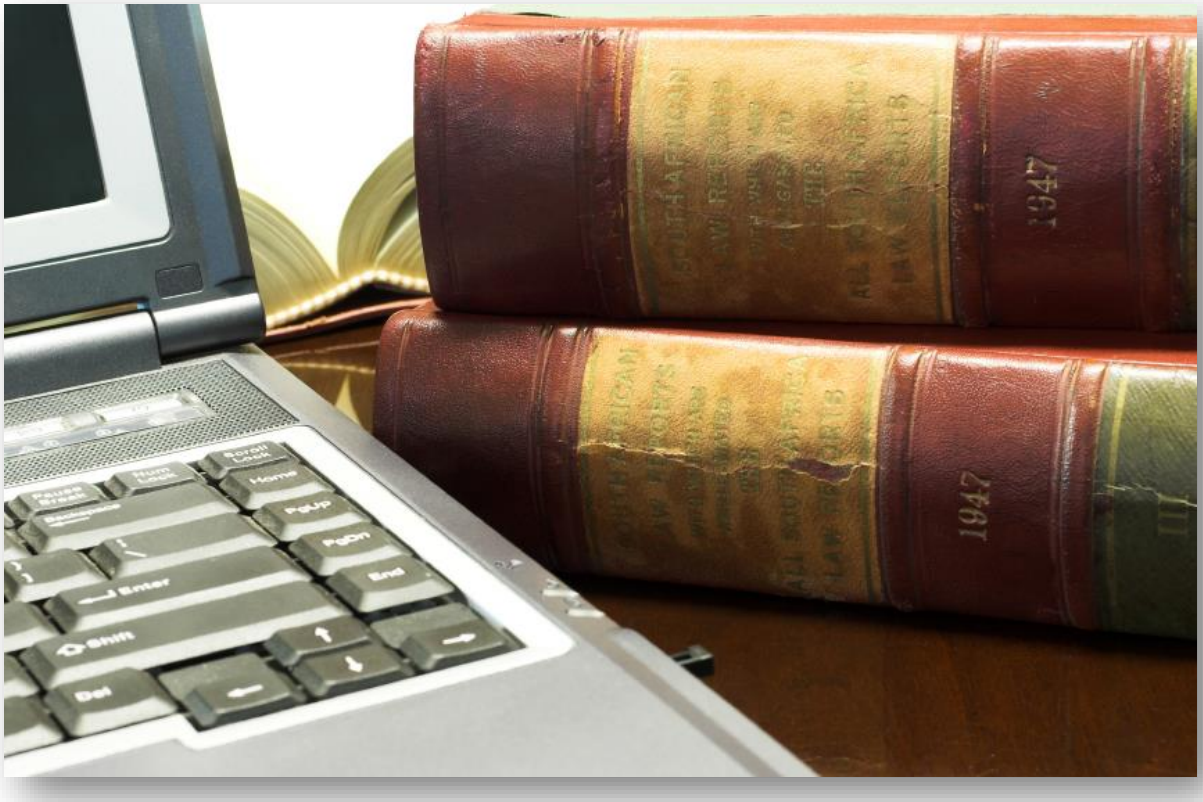
> **C.R.C.P. 16(b)(15) Electronically Stored Information.** If the parties anticipate needing to discover a significant amount of electronically stored information, the parties shall discuss and include in the proposed order a brief statement concerning their agreements relating to search terms to be used, if any, and the production, continued preservation, and restoration of electronically stored information, including the form in which it is to be produced and an estimate of the attendant costs. If the parties are unable to agree, the proposed order shall include a brief statement of their positions.

The E-Discovery Ethical Obligations You Can't Escape

Lawyers have two packages of often conflicting duties when it comes to electronic discovery: 1) duties to clients, and 2) duties to the adversarial system (opposing parties, courts, etc.).

When we discuss a lawyer's duties to a client, we're usually discussing the various ethics rules concerning confidentiality and competence. These rules govern the conduct of lawyers towards their clients and their clients' information. While the ABA Model Rules of Professional Conduct are frequently referenced, there are also common law duties that concern keeping a client informed.

A lawyer's duties to the adversarial system include adhering to the various ethics rules, as well as other laws and local court rules. These rules include a lawyer's candor towards the tribunal, and fairness to the opposing party and counsel.



Applicable Ethics Rules

The first ethical consideration that applies to e-discovery is the duty of competence. ABA Model Rule 1.1, Competence, provides:

> **A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.**

Competence requires that litigators and other attorneys who may face records preservation and e-discovery matters must understand at least the basic legal and technical issues, know their limitations, and know where to go for assistance with issues beyond their own level of competence.

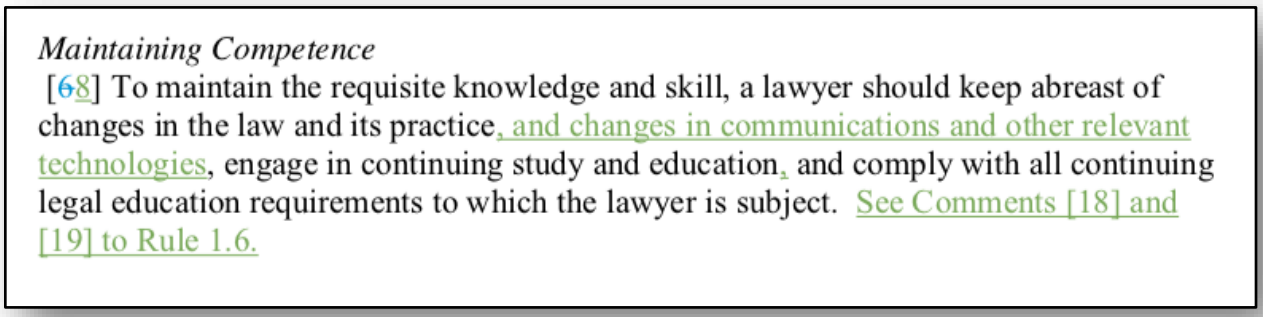
In 2012, the ABA House of Delegates approved the expansion of the Duty of Competence to include the understanding of "the benefits and risks associated with relevant technology." This phrase was included in Comment 8 to Model Rule 1.1:

> **To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.**

On April 6, 2016, Comment 8 to Rule 1.1 of the Colorado Rules of Professional Conduct was amended, but the language was slightly different from the ABA Model Rules. Instead of incorporating the phrase *"including the benefits and risks associated with relevant technology*," as the ABA Model Rule states, Colorado's Comment 8 uses the phrase "*changes in communications and other relevant technologies*":

> **Maintaining Competence**
>
> **[68] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, and changes in communications and other relevant technologies, engage in continuing study and education, and comply with all continuing legal education requirements to which the lawyer is subject. See Comments [18] and [19] to Rule 1.6.**

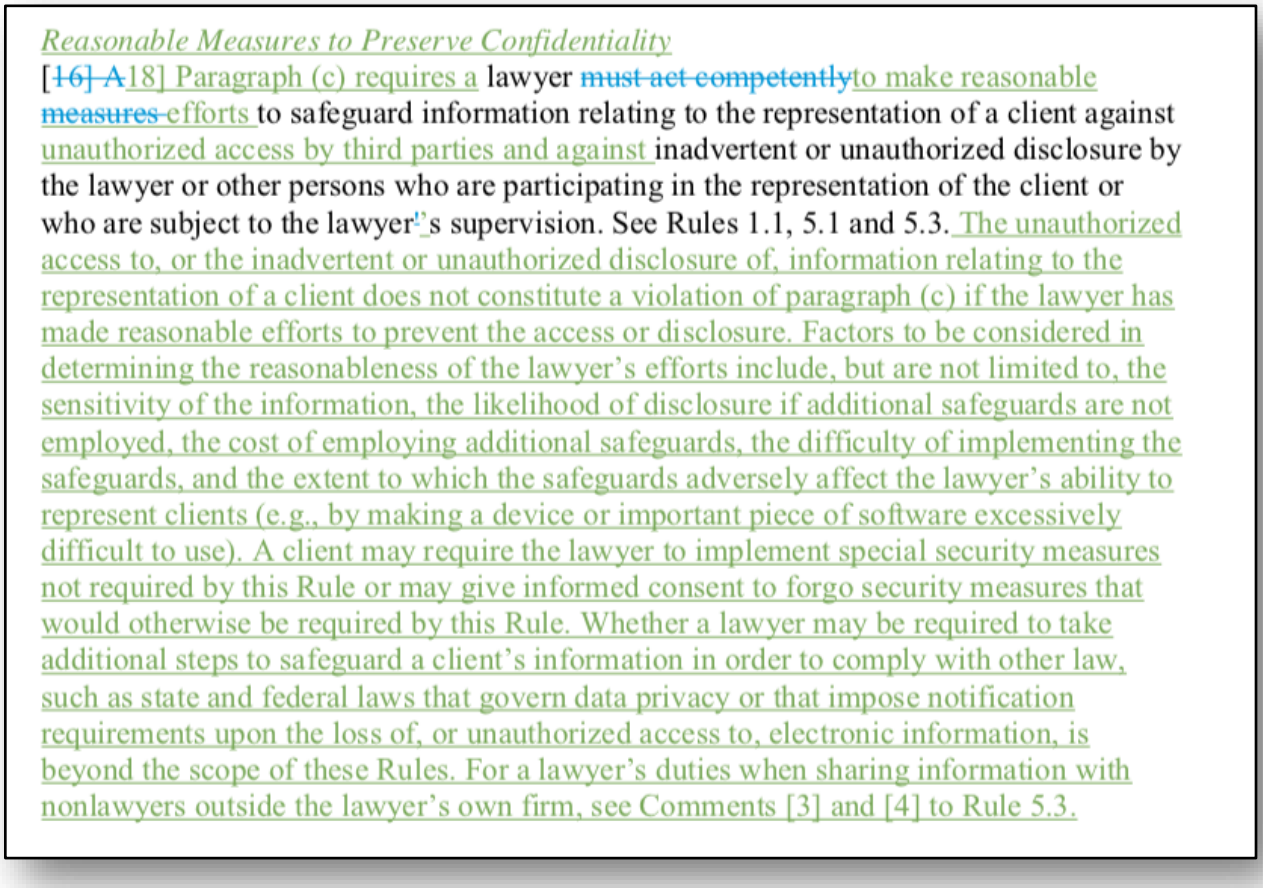
Here are the changes to Comment 8 of Rule 1.1 of the Colorado Rules of Professional Conduct:



Maintaining Competence

[68] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, and changes in communications and other relevant technologies, engage in continuing study and education, and comply with all continuing legal education requirements to which the lawyer is subject. See Comments [18] and [19] to Rule 1.6.

And since Comment 8 refers to "changes in communications" there was some language added to Comments 18 and 19 of **Rule 1.6 – Confidentiality of Information**:



Reasonable Measures to Preserve Confidentiality

[~~16] A~~18] Paragraph (c) requires a lawyer ~~must act competently~~to make reasonable ~~measures~~ efforts to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules. For a lawyer's duties when sharing information with nonlawyers outside the lawyer's own firm, see Comments [3] and [4] to Rule 5.3.

[~~17~~19] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these Rules.

Searching for Ethics

One area where lawyers have found it difficult to follow an ethical straight line in e-discovery is "search." This is not always an intentional disregard for the lawyer's ethical responsibilities, but because technology can be confusing and technical, many lawyers have found themselves lacking the skill and competence necessary to formulate effective and defensible search processes.

When we discuss "searching" in the context of e-discovery, we are commonly referring to the practice of applying search "keywords" and phrases to a set of documents in the hope of retrieving a select, focused group of those documents that are responsive to our search parameters. It sounds like an easy task, after all, everyone can run a Google search. But defensible search has become more problematic in the context of search and retrieval of relevant document sets than anyone anticipated.

This frustration has been borne out in several opinions such as *United States v. O'Keefe,* 537 F. Supp.2d 14 (D. D.C.2008), where Judge Facciola famously stated:

> "Whether search terms or 'keywords' will yield the information sought is a complicated question involving the interplay, at least, of the sciences of computer technology, statistics and linguistics. ... Given this complexity, for lawyers and judges to dare opine that a certain search term or terms would be more likely to produce information than the terms that were used is truly to go where angels fear to tread."

In that same year (2008), *Equity Analytics, LLC v. Lundin*, 248 F.R.D. 331 (D. D.C. 2008) opined in a similar fashion:

> "[D]etermining whether a particular search methodology, such as keywords, will or will not be effective certainly requires knowledge beyond the ken of a lay person (and a lay lawyer) and requires expert testimony that meets the requirements of Rule 702 of the Federal Rules of Evidence."

Other opinions have expressed similar frustration with the lack of comfort and continuity among lawyers to devise effective and defensible approaches to "searching" a set of documents and data.

How To Convince Your Client To Preserve ESI When All They Want To Do Is Delete It

The Rule of Professional Responsibility most directly affecting the issue of preservation of electronic data is Rule 3.4, entitled "Fairness to Opposing Party and Counsel." Rule 3.4(a) states: "[A lawyer shall not] unlawfully obstruct another party's access to evidence or unlawfully alter, destroy, or conceal a document or other material having potential evidentiary value. A lawyer shall not counsel or assist another person to do any such act."

The comment to Rule 3.4 provides further important guidance regarding its purpose and scope:

> **"The procedure of the adversary system contemplates that the evidence in a case is to be marshaled competitively by the contending parties. Fair competition in the adversary system is secured by prohibitions against destruction or concealment of evidence, improperly influencing witnesses, obstructive tactics in discovery procedure, and the like.**
>
> **Documents and other items of evidence are often essential to establish a claim or defense. Subject to evidentiary privileges, the right of an opposing party, including the government, to obtain evidence through discovery or subpoena is an important procedure right. The exercise of that right can be frustrated if the relevant material is altered, concealed or destroyed. Applicable law in many jurisdictions makes it an offense to destroy material for purposes of impairing its availability in a pending procedure or one whose commencement can be foreseen ... Paragraph (a) [of Rule 3.4] applies to evidentiary material generally, including computerized information."**

The annotation to Rule 3.4(a) points out that while a violation of the rule may expose a lawyer to professional discipline, "it is normally the judge hearing the matter who initially takes the corrective action through litigation sanctions, such as ... exclusion of evidence, and the payment of fines, costs, and attorneys' fees." While the ethics rule is a starting point, much of what is important regarding the ethical issues related to the duty to preserve electronic data is found in the case law discussing spoliation of evidence, the duty to preserve evidence, the sanctions available under the discovery rules, as well as the inherent authority of the court.

The duty to preserve relevant information is actually not specifically defined in the Federal Rules of Civil Procedure – it's born out of case law. The duty usually encircles the concept of a "litigation hold." Three concerns around the litigation hold include:

1. When the duty arises – the "trigger"

2. What must be preserved – the "scope"

3. How should it be preserved – the "process"

The "Trigger"

The duty to preserve evidence is triggered when litigation or an investigation begins, or when litigation or an investigation can be "reasonably anticipated." In *Byrnie v. Cromwell,* 243 F. 3d 93 (2d Cir. 2001), the obligation to retain arises when a "party has notice that evidence is relevant to litigation … but also on occasion in other circumstances, as for example, when the party should have known that the evidence may be relevant to future litigation."

For an example of preservation obligations being triggered prior to the commencement of litigation, read a good summary of a sanction ruling in *Voom HD Holdings LLC v. EchoStar Satellite LLC.*

The "Scope"

"Corporations are not obligation, upon recognizing the threat of litigation, to preserve every shred of paper, every e-mail or electronic document, and every backup tape. Indeed, such a rule would cripple large corporations." *Zubulake v. UBS Warburg LLC,* 220 F.R.D. 212, 217 (S.D.N.Y. 2003)

Nevertheless, "[w]hile a litigant is under no duty to keep or retain every document in its possession, … it is under a duty to preserve what it knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery, and/or is the subject of a pending discovery request." *Wm. T. Thompson Co. v. General Nutrition Corp. Inc.,* 593 F.Supp. 1443, 1455 (C.D. Cal. 1984)

"[A]nyone who anticipates being a party or is a party to a lawsuit must not destroy unique, relevant evidence that might be useful to an adversary." *Zubulake v. UBS Warburg LLC,* 220 F.R.D. 212, 217 (S.D.N.Y. 2003).

In its "*Commentary on Legal Holds: The Trigger & The Process*," highly respected e-discovery think tank The Sedona Conference says factors that dictate the scope of preservation include "the nature of the issues raised in the matter, the accessibility of the information, and the relative burdens and costs of the preservation effort." Generally, courts expect parties to apply a standard of "reasonableness" and "proportionality" to their preservation demands and efforts, recognizing that the costs and burdens associated with preserving ESI should always be in balance with the value of the dispute.

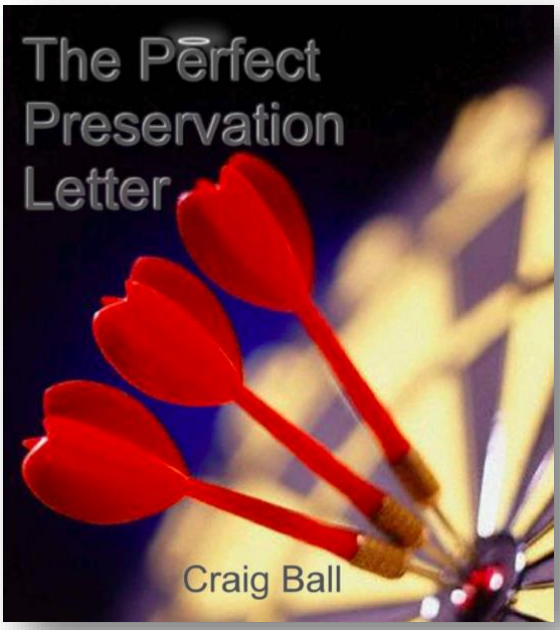
The "Process"

A party must take reasonable steps to identify and preserve relevant information as soon as practicable. Judges expect a good faith, reasonable process that is defensible and documented.

The "Zubulake" Duty was outlined in *Zubulake v. UBS Warburg, LLC,* 229 F.R.D. 422 (S.D.N.Y. 2004):

1. Issue a "litigation hold" at outset and periodically reissue"
2. Communicate directly with the "key players"
3. Instruct all employees to produce copies of relevant electronic files
4. Make sure that all ... media which the party is required to retain is identified and stored in a safe place.

Though preservation letters are not a formal component of civil discovery procedure, they are very common. In his popular paper "The Perfect Preservation Letter," (http://www.craigball.com/perfect%20preservation%20letter.pdf) e-discovery attorney and expert Craig Ball explains that preservation letters are not just about educating or reminding opponents out of professional courtesy. "The preservation letter can establish such awareness, bolstering a claim that the party destroying evidence knew of its discoverability and recklessly or intentionally disregarded it," Ball writes.



Protecting Privilege

There is an increased risk of waiver of privilege in e-discovery because of the volume of data involved, the multiple locations where data can be stored, and the confusion that accompanies the collection and preservation of electronically stored information.

Courts have taken three different approaches to the inadvertent disclosure of electronically stored information:

1. Strict waiver from inadvertent production;

2. An intermediate approach (weighing several factors);

3. And no waiver absent client agreement.

Model Rule 4.4(b) states that "a lawyer who receives a document relating to the representation of the lawyer's client and knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender."

Federal Rule of Civil Procedure 26(b)(5)(B) states: "after being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has; must not use or disclose the information until the claim is resolved; must take reasonable steps to retrieve the information ... and may promptly present the information to the court under seal for a determination of the claim."

In *Victory Stanley, Inc. v. Creative Pipe, Inc.*, 250 F.R.D. 251 (D. Md. 2008), Judge Grimm ruled that there was a waiver of privilege through inadvertent production of electronic records because the defendants failed to establish that they took reasonable measure to prevent inadvertent disclosure. The defendants used an untested keyword search, failed to engage in sampling the verify its results, and were "regrettably vague" in their description of the keyword search.

In Alcon *Mfg., Ltd. v. Apotex, Inc.,* 2008 U.S. Dist. LEXIS 96630 (S.D. Ind. Nov. 26, 2008), the court applied Federal Rule of Evidence 502 and found no waiver by inadvertent production:

> "Perhaps the situation at hand could have been avoided had Plaintiffs' counsel meticulously double or triple-checked all disclosures against the privilege log prior to any disclosures. However, this type of expensive, painstaking review is precisely what new Evidence Rule 502 and the protective order in this case were designed to avoid."

Federal Rule of Evidence 502 was enacted in 2008 to protect against the waiver of privilege or other protections upon the disclosure of protected information in discovery. There were two primary goals for FRE 502: (1) to resolve a longstanding circuit split concerning the effect of the inadvertent production of privileged material and (2) to respond to widespread complaints that protecting against waiver of privilege through

exhaustive document review had become cost prohibitive in a regime where any disclosure may effect a subject matter waiver.

Federal Rule of Evidence 502(b)

> **Inadvertent Disclosure. When made in a federal proceeding or to a federal office or agency, the disclosure does not operate as a waiver in a federal or state proceeding if:**
>
> > **(1) the disclosure is inadvertent;**
> >
> > **(2) the holder of the privilege or protection took reasonable steps to prevent disclosure; and**
> >
> > **(3) the holder promptly took reasonable steps to rectify the error, including (if applicable) following Federal Rule of Civil Procedure 26 (b)(5)(B).**

Federal Rule of Evidence 502(d)

> **Controlling Effect of a Court Order. A federal court may order that the privilege or protection is not waived by disclosure connected with the litigation pending before the court — in which event the disclosure is also not a waiver in any other federal or state proceeding.**

Under FRE 502(d), the court may issue an order providing that a party's disclosure of documents protected by the attorney-client privilege or work product protection does not waive the privilege (unless there was an intent to waive the privilege).

An FRE 502(d) order is a unique discovery tool because:

- The no-waiver effect also applies in other federal AND state court proceedings.
- The parties may incorporate into the order a specific and detailed agreement regarding its scope and effect in the litigation.
- Privileged documents must be returned to the disclosing party "irrespective of the care taken by" the party in reviewing them prior to production.
- The court may issue the order sua sponte, without the parties' agreement.

How To Avoid Being Cyber-Bullied By The Other Side In E-Discovery

Agree to Disagree – Cooperation in E-Discovery

The concept of "cooperation" among litigating parties has become a clarion call from the bench as judges have grown increasingly frustrated with the delays and unnecessary hand-wringing surrounding the procedural fights around e-discovery.

In July 2008, the Sedona Conference issued the "Cooperation Proclamation" which sought the "open and forthright sharing of information by all parties." It stated:

> **"Cooperation does not conflict with the advancement of their clients' interests – it enhances it. Only when lawyers confuse advocacy with adversarial conduct are these twin duties in conflict."**

In discussion the "Cooperation Proclamation," Ken Withers, the Director of Judicial Education and Content for the Sedona Conference, stated:

> **“If the goal of discovery is to uncover facts to be used during settlement conferences or at trial, why not cooperate in the discovery process, and utilize advocacy and persuasion skills to argue the interpretation of the facts and the application of the facts to the law?”**

In *Mancia v. Mayflower Textile Services Co.,* 253 F.R.D. 354 (2008), Judge Grimm cited the Sedona Conference Cooperation Proclamation and stated "there is nothing inherent in [the adversary system] that precludes cooperation between the parties and their attorneys during the litigation process to achieve orderly and cost effective discovery."

What information get from your client to be prepared to share with the other side…

If cooperation is the goal for civil litigation today, then there is specific information that is necessary to glean from your client before entering into fruitful discussions with the opposing party.

First, you should have a good general understanding of how your client accesses and manages their email, since email will typically be the primary source of potentially relevant electronically stored information. Does your client use Gmail? Does your client use the Microsoft Outlook software to connect to an Exchange server? Is your client’s email hosted by their Internet service provider?

Next, you need to have a good general understanding of how your client accesses and manages files stored on a network share drive at the organization. Do they have access to departmental file shares? Does each individual have access to a personal storage area on network servers?

Lastly, you need to have a good general understanding of how your client employees manages and stores files on their personal computers. How much information do they store on their local hard drive vs. the network file shares? Do they use a cloud-based storage service such as Box or Dropbox to sync files locally to their computer?

Having this information will help to ensure that your discussions with the opposing party will be fruitful and frankly provide you with a sense of confidence when you enter the preliminary discussions. Since you expect the opposing party to provide you with this type of information, it makes sense that you enter the discussions with the same information from your clients.

What questions to ask the opposing party…

Here are a few questions that you should be prepared to pose to the opposing party in your preliminary discussions regarding the collection, review, and production of electronically stored information:

- How do you plan to review documents we produce to you? Will you be using a document review platform?
    - *The answer to this question will, to some extent, help you determine in what "form or forms" you will need to produce the electronically stored information that you collect and review.*
- What types of electronically stored information do you plan to produce? Email? Microsoft Word documents? PDF files? Audio or video? Invoices? Medical records? Database exports? Social media feeds?
    - *The answer to this question will enable you to specify the "form or forms" in which electronically stored information will be produced to you as you have the right to do under both the Federal and Colorado state rules.*
- Determine how you will direct the opposing party to produce electronically stored information to you – native electronic files? (*my recommendation)* Load files for review platforms? Paper? (*not recommended!*)

Forging Your Way Through Forensics

Not every case requires the use of computer forensics professionals, but when computer systems and data must be preserved for litigation purposes, it's imperative to employ professional help as soon as possible.

Computer forensics can be scary – professional examiners can literally scrape information from your computer about e-mails you've sent, websites you've visited, and old documents you thought you deleted. This session will inform you what computer forensics professionals can do for you and your client, and also help you obtain the electronic evidence you need from the other side.

Defining Computer Forensics

Computer forensics can be defined broadly or narrowly. But it is generally accepted that the science of computer forensics involves the identification, preservation, examination, and interpretation of magnetically-stored information (e.g. computer hard drives).

The identification phase does involve some technology, but it really begins at the physical level. Before you retain the services of a computer forensics professional, it's important to already have a good idea of which computers and/or external hard drives need to be copied or "imaged." The computer forensics professional isn't going to be able to help identify the key players in the litigation, but once they hear the facts of the matter, they can usually make some important suggestions as to where to look on the computer to find relevant electronic data.

Preservation is the most important job of a computer forensics professional. The main reason one calls a computer forensics professional is to ensure that sensitive and relevant data on a computer is protected against accidental or unauthorized deletion (spoliation). Preserving the electronic data for future examination is the ultimate goal of every computer forensics project.

“The obligation to preserve evidence arises when the party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation.” *Zubulake v. UBS Warburg*, (Zubulake IV) 220 F.R.D. 212 (S.D.N.Y. 2003) The role of a computer forensics professional helps an attorney appropriately accomplish the duty to preserve relevant evidence when it is located on individual computers. While the Zubulake IV opinion states that a party is obviously not required to preserve "every shred of paper or e-mail," they must actively preserve important, relevant data that may easily be found "hiding" in computers. While it may not be easy for a non-technical person to find "hidden" information in a computer, a skilled computer forensics professional can quickly and easily discover many details that are not readily apparent to a normal computer user.

Examination and interpretation are important in communicating what is found on a computer to attorneys. A computer forensics professional will examine the data collected from a computer with the goal of retracing the steps of the computer user. Craig Ball (www.craigball.com) is an attorney and a well-respected certified computer forensic examiner, and he calls this part of the job "telling the story" of what happened on the computer.

Craig is in a unique position because he is an attorney himself, and therefore is able to competently interpret his findings to the attorneys that hire him. It takes a special skill to describe and explain how Web cookies, for example, work and operate on a computer that surfs the Web. It's important to find a computer forensics professional that can comfortably translate technical terms and scenarios into an easily understood story – not only so that you understand it, but so you are confident they can describe their findings to a judge or jury.

The science of computer forensics has been abundantly deployed in the criminal world, and it is steadily becoming the norm in civil litigation matters. Law enforcement officials have long used computer forensics to track down criminals that have used the Internet to lure children and other victims into compromising situations. A good example of this is a story found in Popular Mechanics magazine entitled "Computer Forensics: The New Fingerprinting" (online at http://www.popularmechanics.com/technology/military_law/2672751.html). In that story, FBI computer forensic examiners tracked down a kidnapper who had communicated with a 13-year old girl through chat rooms over the Internet. The examiners found clues to the kidnapper's identity by combing through files left on the girl's computer.

In civil litigation, computer forensics professionals are routinely called upon to ensure that electronic evidence is pristinely preserved, and then to retrieve relevant evidence from the images of the hard drives. Both parties to a civil litigation have to understand, however, that they are must engage in several balancing acts in regard to the hard drive images. For example, taking the hard drive out of a computer renders the computer useless, and so it can be a crippling situation for someone's business to image the hard drive during working hours. Additionally, many computer hard drives will contain a vast mix of both personal and business-related information. While an opposing party may have a right to see the business-related data, precautions must be taken so that non-relevant personal information is adequately protected.

Computer Forensics Concepts and Terminology

The first and most important thing to remember is to NOT TOUCH a computer that you have determined must be imaged to preserve the data it holds. Electronic data is very volatile and although it can remain in a fixed state for a long time (i.e. on a backup tape, hard drive, etc.), it is possible to change many files just by turning on the computer. It's always tempting to turn on a computer just to get a "quick peek" at the contents; but in so doing, relevant information can be erased or modified. The best thing to do is keep the computer turned off and physically secured, and call a computer forensics professional as soon as possible.

An experienced computer forensics professional will start a project by observing the physical environment in which the computer is located. Many people will write usernames and passwords on "Post-It" notes and simply stick them to their computer monitor. This can be useful if a computer forensic examiner needs to access hidden or encrypted data on the machine. Depending upon the situation, it may be a good idea to photograph the environment before the computer is moved around to gain access to the hard drive.

Next, a computer forensics professional must get direct access to the computer's hard drive to make the forensic image. While this can sometimes be done without disturbing the computer very much, it normally requires opening the computer to unplug and take out the hard drive. This is easier to do on a desktop computer, and can sometimes get a little tricky on a laptop.

Once the hard drive is extracted from the computer, it gets hooked up to a "write-blocker" which prevents any information on the hard drive from being modified or "written to." On the other end, the write-blocker is usually hooked up to a laptop computer that is running software to create the compressed forensic image of the hard drive. One of the most popular forensic software packages is EnCase Forensic from Guidance Software (www.guidancesoftware.com).

Software like EnCase compresses the information stored on the hard drive (makes it take up less space); creates and copies the image on to another storage device (i.e. an external hard drive); and then provides a nice interface for scrolling through the thousands of files copied into the disk image. It sounds simple enough, but it takes many hours of training and experience to make sure the whole procedure is performed perfectly. Software like EnCase allows computer forensics professionals to run searches and create reports on what is found on the hard drive.

A skilled computer forensics professional understands more than just how to push a button on a software package – they have studied the intricate details of how data is saved, organized, and managed on a computer. Computer hard drives allocate space for data based on very logical rules. It's important to understand the intricacies of how the technology works in order to know where to look for deleted data - which usually turns out to be where the juiciest and most revealing information is found. Terms like "slack space" and "unallocated space" are regularly mentioned in regard to the "hidden" areas of the hard drive where computer forensics professionals commonly find old, deleted information.

Computer forensics professional are also well-informed on how specific software applications store data on a hard drive. For example, web browser will store "temporary files" and "cookies" on the hard drive as part of their routine operation. Also, applications like Microsoft Outlook store e-mail messages and calendar information in a specific file format that is not easily readable outside of the Outlook environment. Lastly, computer forensic examiners know how to view the "metadata" of a file so they can tell you specifically when the file was last opened and modified.

How to Find a Computer Forensics Professional

I hope by now it's obvious why a computer forensics project must be handled by a trained, experienced professional. Many IT professionals are very qualified to do a simple "copy" of a hard drive, but they are not trained in creating forensically sound "images" of hard drives that will properly preserve the data for litigation purposes.

Finding a competent computer forensic examiner is not really that much different from finding any other expert. The best place to start is by asking your peers for recommendations on computer forensics professionals that they have used in the past. This is by far the best way to find and retain a computer forensics professional because you will be able to get a feel for the work they do and their experience from talking with your peer.

There are several professional organizations that you can contact for recommendations. One of the most notable include the International High Technology Crime Investigation Association (www.htcia.org).

Before you retain a computer forensics professional, you certainly need to inquire about their qualifications. Obviously, a lot of this can be accomplished by reading over their resume or C.V. You need to be sure they are formally trained for their position and have received the appropriate certifications for the work they perform. Common certifications include Certified Computer Examiner (CCE) and Certified Forensic Computer Examiner (CFCE). Just having a certification, however, may not be enough. They should have a solid amount of experience to accompany their certification. Above all, you need to personally converse with the computer forensics professional so that you feel comfortable with their style and communication ability. The worst thing you can do is hire a computer forensics professional that constantly uses confusing technical jargon without adequate explanations. This will frustrate you and confuse a judge or jury.

Further Reading: "Computer Forensics for Lawyers Who Can't Set a Digital Clock," (http://www.craigball.com/CF.pdf) by Craig Ball who is an attorney and a certified computer forensic examiner.

Data Collections Without Data Disasters

When it comes to electronic discovery, the best defense is a good offense.

One of the most expensive phases in an e-discovery project is the collection of e-mail and electronic documents. It is important right off the bat to start learning where your client stores their e-mail and electronic documents. For example, if they are a company it's a safe assumption that they have an e-mail server that handles the distribution of company e-mail, although this is not always the case – many companies today have moved their email servers to “the cloud” on services such as Microsoft Office 365 or G Suite (from Google).

Collecting electronic evidence for the purpose of producing it to the other side requires the input of both legal professionals (i.e. what is relevant from a legal standpoint) and technology professionals (i.e. where is e-mail stored and how can it be exported off the system).

Preservation of electronic data doesn't always mean it must be exported off a computer server. Often, employees or clients will store information on the desktop and laptop computers that they use every day. It is not recommended that these individuals preserve the e-mail or documents themselves because there is a lot of hidden information contained in computer files (often called "metadata") that will be fatally disturbed if the preservation is not done in a forensically sound manner.

This is where computer forensics professionals are necessary. Such professionals can make a bit-by-bit copy of a computer's hard drive (usually called an "image") that will preserve ALL of the information contained in that hard drive without making any changes to the underlying data. This practice is common and is admissible in court provided the hard drive image is made by an experienced forensics professional.

A computer forensics professional uses an exhaustive approach to recover, convert, review, and present the findings of any forensics investigation. They investigate media types such as PCs, laptops, cell phones, digital cameras, servers, tape backups, thumb drives, GPS, and PDAs. They have the ability to track computer usage history, retrieve deleted emails, hidden files, and documents. They can even create a timeline of events, determine malicious intent and violation of agreements. The most important services that a computer forensics professional can do is provide expert testimony.

The main lesson to take away in the preservation and collection phase is that ignorance can be expensive. You will be much better served in being proactive on talking with your clients about where they store electronic information and having a better idea of their individual practices. Indeed, the Committee Notes to the FRCP amendments recognize the fact that attorneys today must have better knowledge of where and how their clients stored information.

Is Social Media the New E-mail?

In the 1990's when e-mail was just beginning to become a de facto method of communication for the business world, lawyers and litigators were just beginning to understand the importance of collecting those messages for litigation. It seemed like people would say ANYTHING in an e-mail message which meant it was a juicy source of some of the most damaging (or beneficial) information related to a litigation matter or investigation.

The problem was that lawyers had a devil of a time learning how to adequately collect and process e-mail in those early days. Fortunately, we've come a long way in the last couple of decades and today, e-mail collection is one of the easiest sources of electronically stored information (ESI) to collect today. In fact, services such as Microsoft Office 365 and Google Apps have begun to incorporate e-mail collection tools right into their services.

But with the internet and social media, we see some of the same types of challenges arising for litigators. One reason is because there are simply so many forms of social media today and they seem to be changing almost every day. Today's it's Twitter and Facebook, but tomorrow it's Snapchat and Instagram. Social media services have their own unique formats and metadata that must be preserved. And people use social media from a variety of different mobile devices as well as computers.

With e-mail, corporations and lawyers could plead ignorance because it was a new world part of the "digital revolution" that everyone was getting used to. But today, since we've already learned so many lessons from collecting and reviewing e-mail messages, we don't have many excuses for staying behind the eight ball. It's important for every lawyers (not just litigators) to learn the basics about collecting and producing social media.

Some Basics on Collecting and Preserving Social Media

Everyone, including lawyers, is using social media today to record their thoughts, actions, feelings, whereabouts, and much more. This provides a rich and sumptuous insight into the daily history of an individual. If you're not considering this information in your litigation matters, you're missing some of the most salient information relevant to a matter.

No one would ethically suggest that you "friend" an opposing party under false pretenses, but a public profile is open for the world to see and completely fair game. It's no different than Googling your adversary and opposing party.

We've made valiant efforts to collect the web-centric and social media evidence using primal, inadequate tools such as the "print screen" command in an attempt to snap a picture of the content in our web browser. We've printed this to paper, thus converting a dynamic, living web page into a degraded version of the original (the equivalent of producing a toy replica handgun in place of the actual murder weapon).

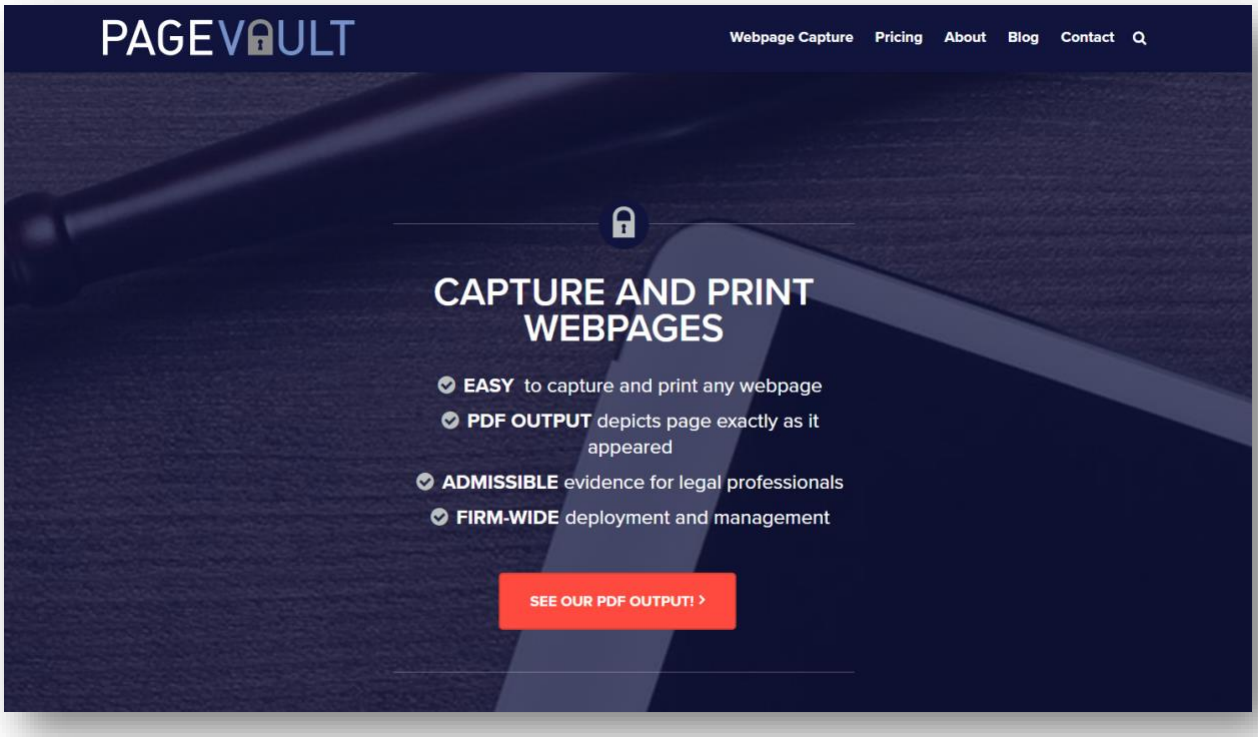
We've also converted webpages to PDF. This is similar to printing a webpage to paper, except that some PDF software captures dynamic pictures and active content. At least the information stays in digital format and keeps the hyperlinks active. Many of these PDF conversions will also include at least a date and time stamp on the page that someone can testify to.

Lastly, there have been "web crawlers" that can suck down webpages to your local computer several links deep. This process allows you to surf the page from a local machine and works just fine in some scenarios for taking a snapshot of a website and preserving a webpage.

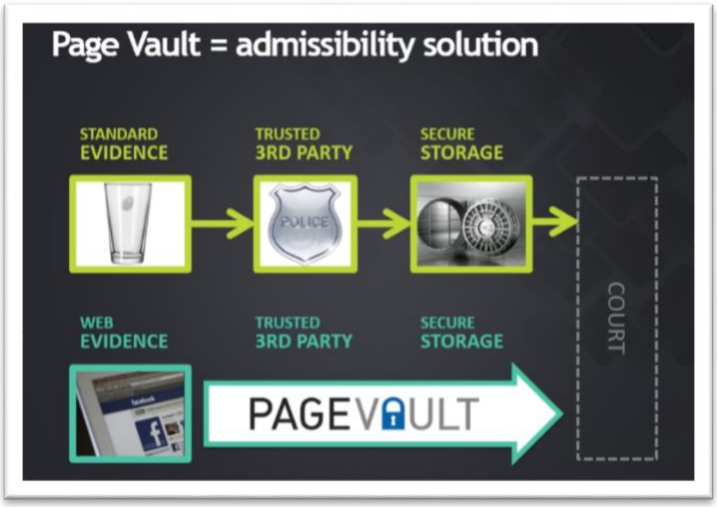
The ideal method is to utilize the application programming interface (API) offered by social media publishers so that information can be collected directly from the platform. This allows the product to capture all of the user-facing data along with the metadata straight from the publisher. Bonus if the product can preserve the information for searching, reporting, and exporting.

Tool: Page Vault

Page Vault is an online service that was completely designed for lawyers to capture web pages. The service does more on the preservation side than tools like Adobe Acrobat, but still generates a usable PDF file that can be admitted in court.



Page Vault features a one-click capture process and then stores the PDF output in a cloud account for the sake of preservation.



E-Discovery Tools For Mere Mortal Lawyers

For many years, the world of litigation support and e-discovery was ruled by comprehensive systems such as Summation iBlaze and Concordance. These applications boast histories going back several decades and they have weathered fairly well over the years. Unfortunately, they still require sizable investments in software, hardware and training to run fluently and many law firms are just not willing to make that investment.

Today, lawyers can turn to cloud-based litigation support platforms instead. These services offer most of the major features found in the larger server-based products, and offer more flexibility in accessibility and management.

In one sense, e-discovery has utilized cloud-based platforms for many years. High-end vendors have always delivered their platform over the Internet via a variety of technologies. The difference today is that the cloud-based tools (also known as "software-as-a-service" or SaaS) are built from the ground-up to be delivered over the Internet via a web browser. That typically means a less feature-rich experience than other high-end services, but the cloud-based e-discovery tools today are easy to use and require no setup.

Cloud-Based Tools vs. Discovery of Cloud-Based ESI

A common point of confusion is between e-discovery tools that are based in the cloud, and NOT the collection of cloud-based electronic data.

The discovery of cloud-based data is becoming a hot topic today with the proliferation of social media (e.g. blogs, Facebook, Twitter, etc.) and cloud-based storage services (e.g. Dropbox, OneDrive, etc.). Information that is stored on social media or cloud-based storage services is discoverable if it is relevant to a litigation matter, and more parties are seeking the production of such data.

Instead, this section focuses on cloud-based tools for e-discovery, specifically for the document review portion of an e-discovery project. Instead of relying on tools such as Summation or Concordance, lawyers can use cloud-based services such as Lexbe or Nextpoint to review the documents that have been collected. These services also allow lawyers to search, tag and produce documents.

The Advantages of Using a Cloud-Based E-Discovery Provider

There are several strong advantages of using cloud-based e-discovery tools:

- **No software purchases -** There is no need for a firm to purchase any software for cloud-based tools. Traditional software usually requires a significant up-front investment along with annual maintenance fees. With cloud-based tools, customers usually pay a monthly fee to access the service and the "software" is delivered through a Web browser. There is no software to purchase, install or update.

- **No hardware purchases -** Similarly, there are no hardware purchases for cloud-based tools. All of the hardware (servers) are hosted and maintained by the cloud provider instead of at the firm.

- **Easy data uploads** - You don't need to worry about storing ESI at your law firm, you simply upload the data to a cloud-based service where it is processed and presented to you in a database accessible through your web browser.

- **Easily sharable** - Cloud-based tools are designed to be accessible from any computer with a web browser. New users (such as local counsel or clients) can be added by simply creating a new user account on the service.

- **Cross platform** - It does not matter if customers have Windows or Macs since cloud-based tools will work in just about any web browser. Many of the services we discuss can easily be accessed from iPads and other tablet devices.

- **Painless upgrades** - Since there is no software to purchase there is no need to worry about upgrading that software. Cloud-based tools can be upgraded quickly and frequently without any negative consequences to the customers.

- **Consistent backups and redundancy** - Cloud-based providers frequently back-up the data stored on their servers, and ensure that backups are stored in several places to ensure redundancy. This completely frees up the law firm from having to worry about backing up data, although it is a good practice for firms to keep additional local copies of their data.

- **24/7 support** - Cloud-based providers know they service a 24/7 world and they provide the same level of support for their services.

- **Scalable** - You never know when that 200 document case will escalate into 200,000 documents. If a firm has legacy systems such as Summation or Concordance, that kind of ramp-up would require more storage space and potentially an increase in license fees. In contrast, cloud-based services can immediately expand to accommodate drastic spikes in collected data

- **Frees up lawyers to focus on what lawyers should do** - Because cloud-based services are taking care of software maintenance, hardware requirements, backups and upgrades, this completely frees up legal professionals to focus on their own work instead of worrying about technical necessities.

Dis-Advantages of Using a Cloud-Based E-Discovery Provider

There are several concerns and hurdles that lawyers should be aware of when turning to cloud-based e-discovery tools:

- **Comfort level -** First, a lawyer must have a comfort level with using a cloud-based tool. This includes being familiar with the ethics of using cloud-based tools (discussed below) and understanding how they will access the tools. More importantly, the lawyer must be able to explain to their client the pros and cons of using a cloud-based tool.

- **Little to no project management support** - Many cloud-based services are bargains compared to some of the higher-end platforms. One area where costs are cut is in project management help.

- **Must be online** - Because cloud-based tools are delivered over the Internet via a web browser, customers must be connected to the Internet in order to use them. There is minimal "offline" access for these tools.

- **Monthly bill** - Where traditional software usually requires an annual maintenance fee, cloud-based tools are billed monthly.

- **Data is stored somewhere other than the law firm** - The very definition of "cloud-computing" means that the data is stored somewhere other than the law firm. And while this means that the service can operate better (high-powered servers connected to high-end Internet pipelines), many lawyers just cannot accept the fact that their client data is being stored on servers that they do not own or control.

- **Less feature-rich** - Because cloud-based tools are delivered via a web browser, it is inevitable that they cannot be as "feature-rich" as their traditional software counterparts. For example, platforms such as Concordance can "connect" to other software applications (e.g. CaseMap, Caselogistix, etc.) but this is almost impossible to do with cloud-based tools.

Selected Cloud-Based E-Discovery Tools

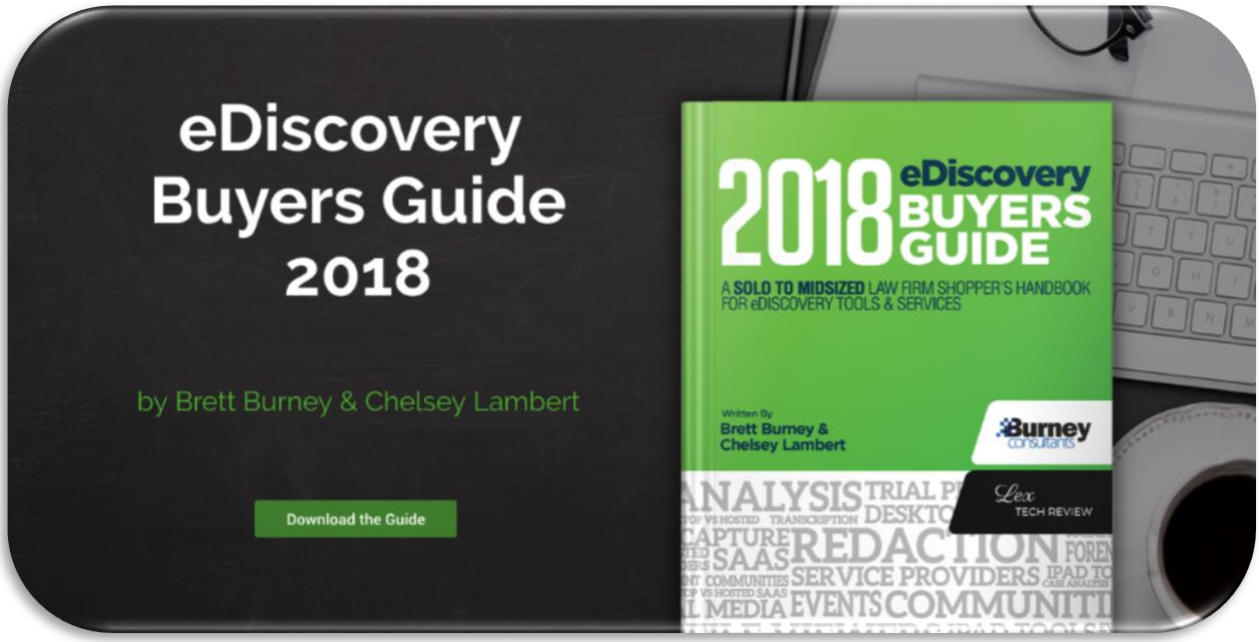
Lexbe - (www.lexbe.com)
Lexbe features a linear database listing of your documents with quick access to document images. One specific feature found in Lexbe is their "case analysis" tool that allows you to pluck key facts and issues out of certain documents and build a chronology of the case. Lexbe allows for native review of electronic documents and can produce document accompanied by a variety of load files (DAT, DII, etc.).

Nextpoint - (www.nextpoint.com)
Nextpoint features a "Google-like" interface to your documents, allowing for immediate search. If that's not enough, Nextpoint features an Advanced Search screen which allows a user to get granular in their search. Nextpoint can be used as a document review platform (Discovery Cloud) or as a trial presentation tool (Trial Cloud). Nextpoint can also produce documents in a variety of formats accompanied by appropriate load files.

CloudNine Discovery - (www.cloudninediscovery.com)
CloudNine Discovery (formerly Trial Solutions) features the "SelfLoader™" which allows customers to easily upload their data to the service. Accepts native files as well as OCR and scanned images.

Logikcull - (www.logikcull.com)
Logikcull is a newer entrant to the field of cloud-based e-discovery tools but promises to "blend all aspects of e-discovery and records management into one easy to use service accessible from anywhere." Logikcull has also promised to pay particular attention to mobile users who want to access the service from iPads and other tablet devices.

Thomson Reuters eDiscovery Point - (http://legalsolutions.thomsonreuters.com)
Announced in February 2016, Thomson Reuters entered into the cloud-based document review space with their own offering called eDiscovery Point. The platform was created based on Thomson Reuters' extensive experience with the legacy product, Case Logistix, and their wealth of experience from Pangea3 contract reviewers.



Download the **FREE** eDiscovery Buyers Guide

A Solo to Midsized Law Firm Shopper's Handbook for eDiscovery Tools & Services

www.ediscoverybuyersguide.com

Authored by
Brett Burney and **Chelsey Lambert**

Wouldn't it be nice if there was a handbook to explain when and how to use eDiscovery solutions without spending hundreds of thousands of dollars?

For solo, small and mid-sized law firms finding answers to eDiscovery tech questions hasn't been an easy task.

Brett Burney (Burney Consultants LLC) and Chelsey Lambert (Lex Tech Review) have teamed up to publish the 2018 eDiscovery Buyers Guide to solve exactly this problem.