HOT TIPS ABOUT ESI

Hot Tips From the Coolest Family Law Attorneys

Friday, September 27, 2013

Melissa Fuller Brown
145 King Street, Ste. 405
Charleston, SC 29401
843-722-8900
melissa@melissa-brown.com
www.scdivorcelawyer.com

What is ESI?

ESI stands for Electronically Stored Information. ESI is information created, manipulated, communicated, stored, and best utilized in digital form, requiring the use of computer hardware and software. It can be found on any technology having electrical, digital, magnetic, wireless, optical or electromagnetic capabilities.

Where is it found?

ESI is found on PDA's, cell phones, digital cameras, GPS devices, portable hard drives, external hard drives, internal hard drives, thumb/flash drives, servers, workstations and laptops.

How did ESI become relevant? A brief history:[1]

ESI first became relevant in the case against Ollie North over the Iran-Contra affair. In the late 1980's, US Senate investigators were able to retrieve 758 email messages sent by Ollie North that confirmed his involvement in the operation. North thought he had deleted these emails and had denied their existence. Subsequently, he was convicted of lying under oath to a congressional committee.

In 2006, formalized changes were made to the Federal Rules of Civil Procedure in regard to the use of electronic discovery. Even dating back to 1999, the ABA adopted Civil Discovery Standards. Judge Shira A. Scheindlin, who wrote the decision in *Zubalake v. UBS Warburg,* 216 F.R.D. 280, 283 n. 30 (S.D.N.Y. 2003)(**Exhibit A**), cited these standards. She was also one of the keynote speakers last year at the University of South Carolina Law Review's Technology Symposium and is regarded as a leading ESI expert.

Now, over 49 states have enacted e-discovery rules and ESI is explicitly covered by the 2006 amendments to the Federal Rules.

Why do I need to understand ESI?

In the near future, we will see more and more attorneys held liable for not ensuring their client were properly advised to preserve data and for not insuring that the client properly complying with an e-discovery request. Cases such as *Green v. McClendon*, No. 08 Civ. 8496 (JGK) (S.D.N.Y. Sept. 8, 2010) (**Exhibit B**) held that the "Litigation Hold duty" runs first to the lawyer and only then to the client.

Further, lawyers must understand when there is an obligation to preserve ESI. The simple answer:

> **"Yes," there is a duty if litigation is likely**. But, what does that mean? Does this mean we have to advise potential clients who consult us about divorce

---

[1] Olson, Bruce A. and O'Connor, Tom, Electronic Discovery for Small Cases: Managing Digital Evidence and ESI. (2012).

and are simply in our office to gain a better understanding of the law, but they are not convinced they actually want to file? Is this situation considered "litigation is likely?" How can we be held responsible for potential clients actions? These are the scary questions and right now, there are no clear answers.

"No," in some states the duty does not start until the suit is filed. This seems to be the answer, but isn't this situation ripe with potential risks? Does this mean a lawyer could advise a client to safely delete all incriminating ESI and hold-off filing until all damaging evidence has been destroyed? Doesn't this smell like a rat?

What is the safest route? The safest route is to assume that any potential client's case is one where litigation is likely. Thus, the lawyer should advise the client to preserve the ESI.

So, what does it mean to explain to a client their preservation obligations?[2]

1. Duty to preserve is clear.
2. Duty to marshal data to avoid sanctions.
3. Initial meet and confer start even earlier than required.
4. Take charge and see information is preserved.
5. Mostly federal law applies at this point.
6. Put the other side on notice early and often re: preservation.

What is the best way to explain preservation duties to a client? Use a preservation letter. (**Exhibit C**, Email memo from Gordon Cruse to Ms. Client dated March 20, 2012.)

Obtaining ESI

A new device and software created by the Israelis and used by many law enforcement groups and computer forensic experts is called Cellebrite Touch. It is a product that creates images of cell phones. A one year license costs $5,000. Once one is properly trained to use the device, using Cellebrite allows the expert to copy a cell phone and create a verifiable copy for later use at court.

It is best for the client, not the attorney, to take the phone to the expert[3] to protect the Chain of Custody. The expert will identify and note the information about the phone, serial number, owner, condition of the phone including scratches and whether it was on or off when delivered, and the expert will photograph the phone.

---

[2] Cruse, Gordon & Hennenhoefer, Jim. (2013). *ESI Ethics* [PowerPoint slide 28] Used with permission.

[3] Forensic Computer Experts must be licensed in South Carolina by SLED.

Cellebrite simply creates images. It does not analyze the material. Obtaining the images can take a long time. For example, it takes one hour to download images from a phone with 1Gb of memory. Most phones have at least 16 Gb of memory and many have much more. Thus, it will take Cellebrite 64 hours to download images from an iPhone 5 with 64 Gb of memory.

Cellebrite captures contacts, emails, photographs and calendar entries, although if contacts and calendar entries are modified, it does not keep a historical track of information.

With emails, the device is able to identify the origin of the source or transmission. Then there is the data extraction. Interestingly, experts can generally get around the passwords on iPhones, but the outdated Blackberries have one major benefit over iPhones and that is that the Blackberries encryption is solid.

Text messages are also extractable, and there will be a timeline that accurately shows the users activity including time and date for photos and sometimes even the location where the photo was taken.

Preserving ESI

The other major issue is obtaining ESI evidence from the other party by requesting it. One of the most important tips is to specify the format that you want the other side to provide the material. It is also important to include a specific request for the type of format or the respondent gets to choose the format.

What is this process?

First send a spoliation letter (**Exhibit D**) or a Preservation of Evidence Letter (**Exhibit E**). These letters put the other side on notice that ESI evidence must be preserved and not destroyed. Again, why is this so important? Even if there are hard copies available of material, the hard copies do not contain the **metadata** and often it is in the metadata where the real gems are hidden.

Request the information early and try to be as specific with your requests as possible because the process is expensive and cumbersome.

Liability

No reported cases in South Carolina ----- yet. But, *Zubulake v. UBS Warburg, LLC*, 22 Ill.217 F.R.D. 309, 13 ILRD 578, 2003 ILRC 1815, 91 FEP Cases 1574 (S.D.N.Y. 2003)(**Exhibit A**) and *Qualcomm v. Broadcom*, 2008 Wl66932 (S.D.Cal.Jan. 7, 2008) (**Exhibit F, overview of case**) are cornerstone cases that make it clear, especially on the federal level that sanctions for both the attorney and client are real; violations may result in an attorney being reported to their State Bar Grievance Committee; fines are expensive; Clients who allege the attorney did not properly advise them

sue their lawyers and even if an attorney put on an otherwise brilliant case, the court can deny requests for fees and costs.

Summary of ESI from the DTI website: http://dtiglobal.com/services/discovery-review-services/welcome-fios-visitors/

“Key Concepts in E-Discovery

Accessibility

Under the “two-tier rule” established under FRCP 26(b)(2)(B), a party need not provide discovery of ESI from sources that the party identifies as not reasonably accessible because of undue burden or cost; on motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost.

Admissibility

The admissibility of electronic records is still evolving as most organizations strive to move from paper to paperless records. However, the admissibility of electronic information is somewhat more complex, raising issues as to the methodology used in data collection and the chain of custody of the electronic data once it has been collected.

Chain of Custody

Failure to maintain a complete chain of custody may result in the inadmissibility of electronic information.

Cost Sharing/Shifting

Understanding where your information lives and the information governance policies and procedures in place within your organization is critical to successful arguments for cost shifting and cost sharing. Discovery requests may cover email, databases, voice mail, instant messaging systems and other proprietary applications. These systems are rapidly evolving and do not represent the same burden for all companies when making arguments for cost shifting. Implementing legal holds or producing records from traditional voice mail systems takes considerable time and money; newer unified messaging systems often make responding to the same request relatively easy. Similarly, restoring records from traditional tape backup systems can be time and cost intensive; near-line storage, by contrast, does not present the same challenges.

Data Production

Electronic evidence must be delivered to multiple parties involved in a legal matter, including opposing counsel, partner firms, requesting government agencies and others. Depending on the recipients, you may require different delivery formats.

Good Faith

A showing of good faith has always been necessary when responding to discovery or any other court-ordered instruction; however, the burden of showing good faith is now significantly greater on the part of the responding party. Attorneys cannot claim that they did not know about those backup tapes stored in a closet or have proper access to IT personnel. Counsel must have proactive conversations with ESI custodians and IT stewards to create and maintain documentation regarding what preservation actions were taken when the obligation arose, how chain of custody was assured and how both custodians and relevant ESI repositories were systematically identified.

International

The convergence of globalization, technology proliferation and evolving e-discovery rules creates challenges for organizations with internationally dispersed operations. Demands from U.S. courts and government agencies often conflict with foreign privacy and data protection laws, leaving a corporation and its outside counsel uncertain of their rights and obligations. The following cases represent a selection of decisions that address cross-border e-discovery.

Legal Hold/Preservation

A legal hold is an essential element of a company's overall records management program, particularly when it comes to electronic information. It needs to be issued to demonstrate a company's good faith and reasonable effort to comply with its discovery obligations. The reality, however, is that the full implications of the legal hold process may not be fully understood by all parties, particularly outside the legal department. Proactive coordination and planning among corporate counsel, outside counsel, IT and other key stakeholders are imperative to ensure good faith compliance in the face of anticipated litigation.

Meet and Confer 26(f) Conference

The "meet and confer" conference for electronic discovery has moved from a nice-to-have to a requirement under the amended Federal Rules of Civil Procedure. A major component of preparing for a 26(f) meet and confer conference is a "map" of the litigant's ESI content: where it is, what it is, how to preserve it, how to collect it, etc. This defensive requirement can be turned into a strategic advantage when counsel is well informed as to the location and nature of ESI, as well as the costs necessary to produce it.

Metadata

Handling and processing electronic evidence present new and unique challenges that are vastly different from working with traditional printed documents. Unique among these is the handling of metadata – document attributes as to creation, modification, authorship and potentially more details based on the application used to create the electronic documents. Metadata may be used for admissibility purposes, demonstrating the chain of custody for a particular piece of ESI. It may also be used in the preservation and review processes, identifying information to be held and facilitating the culling of duplicate documents respectively. Simply opening a file or copying it to another location may modify the hidden metadata. In order to prevent spoliation, proper methods must be used in the collection and review of electronic documents. Similarly, metadata that represents privileged information must be carefully removed prior to production. This can be a complex process requiring deep technical expertise and experience.

Privilege

Technology, when properly applied, has the ability to rapidly increase the rate of productivity exponentially. However, when improperly utilized, small mistakes can have large-scale effects – particularly when dealing with the inadvertent disclosure of privileged documents. Clawback and quick-peek agreements may help buffer the risk, but are only partially effective. And without proper steps to maintain privilege, courts may find it has been unintentionally waived.

Sanctions

The preservation of ESI can be costly for many large organizations. Over-preservation may result in escalating costs as information is produced at an exponential rate. Failure to preserve enough can result in a wide range of possible penalties, including monetary, issue, expert and case-related sanctions. Companies need to develop defensible processes that strike the balance between preservation and business needs. Such policies must also be effective and supportive of good faith efforts to identify and preserve potentially responsive ESI.

Spoliation

While FRCP 37(f) provides a safe harbor for routine, good faith deletion of e-discovery, FRCP 37 also provides for sanctions where the producing party fails to provide e-discovery outside of the safe harbor. In addition to sanctions, spoliation of ESI may result in an adverse inference, an award of attorneys' fees and possibly an adverse judgment. These risks can be mitigated through documented good faith efforts to preserve potentially responsive ESI."