Strafford

Presenting a live 90-minute webinar with interactive Q&A

Social Media Admissions in Personal Injury Cases: Mitigating Risk for Plaintiffs, Securing Admissions From Defendants

Complying With Duty to Preserve; Obtaining and Admitting Evidence Adverse to Defendants From Social Media Sites

WEDNESDAY, MAY 10, 2017

1pm Eastern | 12pm Central | 11am Mountain | 10am Pacific

Today's faculty features:

Frances Crockett Carpenter, Esq., **Law Office of Frances Crockett**, Albuquerque, N.M.

Robert J. Kasieta, Founder and Managing Member, **Kasieta Legal Group**, Madison, Wis.

Michael C. Maschke, CISSP, CCE, EnCE, Chief Executive Officer, **Sensei Enterprises**, Fairfax, Va.

The audio portion of the conference may be accessed via the telephone or by using your computer's speakers. Please refer to the instructions emailed to registrants for additional information. If you have any questions, please contact **Customer Service at 1-800-926-7926 ext. 10**.

APPENDIX A: Electronic Discovery:

Frances Crockett Carpenter
Law Office of Frances Crockett
925 Luna Circle NW
Albuquerque, NM 87102
(o)505.314.8884

- According to estimates published in Law Technology News, at least 93% of business documents are created electronically and more than 35% of corporate communications never reach paper.[1]
- Always ensure that you send notice to preserve all evidence, including electronic evidence when litigation is looming.
- The risks that Defendants face or even Plaintiffs for that matter are sanctions by the courts (e.g. spoliation) or regulatory bodies (see Sarbanes-Oxley Act wherein two increasingly important provisions were set forth in §§ 802 and 1102 and codified, respectively, at 18 U.S.C. 1519 and 18 U.S.C. 1512(c). These provisions impose substantial criminal penalties on any individual or entity -- public or private -- for destruction of evidence or obstruction of justice regarding any actual or "contemplated" federal investigation, matter or official proceeding.) Parties also face unpredictable costs (see section on costs associated with retention of computer forensics expert), and poor outcomes in litigation.
- The duty to preserve evidence arises from common law from which courts have established local rules.
- Dec. 1, 2006, amendments to the Federal Rules of Civil Procedure focus on retention and production of electronically stored information.
- [2]**FRCP Rule 16 (b)**

  Allows the court to establish rules around disclosure, privilege, methods and work product prior to electronic discovery commencing.

- Intent: Save court and attorney time by pre-establishing rules & process for managing discovery.

- Reality: Legal must understand IT environment for all federal cases within first 120 days, more motion practice around ED very early in case; court order higher stakes than party agreement.

- **FRCP Rule 26 (a)**

- Adds "electronically stored information" (ESI) as own category.
-

[1] http://www.sims.berkeley.edu/research/projects/how-much-info 2003/internet.htm
[2] http://www.fiosinc.com/case-law-rules/e-discovery-federal-rules-civil-procedure-frcp.aspx

Property of Law Office of Frances Crockett

- Intent: Remove ambiguity around the words "document" and "data compilations."
-
- Reality: No more wriggle room for instant messaging, Voice over IP, databases, PDA's.
-
- **FRCP Rule 26 (b)(2)**
-
- Sets up two-tier discovery for accessible and inaccessible data; provides procedures for cost shifting on inaccessible data.
-
- Intent: Remove uncertainty about who pays for requests for restoring backup tapes, forensics; make sure Zubulake remains a one circuit precedent.
-
- Reality: Will require more work and costs for defendants very early in a case to account for the backups and what data is on them; codifies Zubulake for entire US.
-
- **FRCP Rule 26 (b)(5)**
-
- Clarifies procedures when privileged ESI is inadvertently sent over to the requesting party (retrieval of that information).
-
- Intent: To allow "clawback" of privileged information; allow parties to push the cost of review to the requestor.
-
- Reality: Still huge risks involved; will not be able to capture/retrieve all sensitive data (e.g. trade secrets and other IP), embarrassing e-mails, waiver of privilege for other cases.
-
- **FRCP Rule 26 (f)**
-
- Requires all parties to sit down together before discovery begins to agree on some form of protocol.
-
- Intent: Rule encourages uniformity, structure and more predictable motion practice.
-
- Reality: Opportunity to shift preservation costs if prepared for these discussions; otherwise opportunity to get painted into a corner.
-
- **FRCP Rule 33 (d)**
-
- Includes ESI as part of the business records related to interrogatories.
-

Property of Law Office of Frances Crockett

- Intent: To reduce time spent gathering and analyzing data to answer interrogatories.
-
- Reality: Can provide transaction detail in electronic form in answer to interrogatories; may need to provide direct access or decent tools.
-
- **FRCP Rule 34 (b)**
-
- Establishes protocols for how documents are produced to requesting parties.
-
- Intent: Stop arguments about the form of production, decide early to save costs.
-
- Reality: Requesting party gets to choose form of production; most advantageous form is native files which are more difficult to review and have potentially damaging metadata or track changes.
-
- **FRCP Rule 37**
-
- Provides "safe harbor" when electronic evidence is lost and unrecoverable as a matter of regular business processes.
-
- Intent: Help calm fears (and avoid sanctions) when data is lost or overwritten in the normal course of business (gut Zubulake).
-
- Reality: Puts GC on notice to ensure litigation holds and data destruction policies are legally defensible; hard to prove without third-party validation (codifies Zubulake).
-
- **FRCP Rule 37 (f)**
-
- Allows for sanctions against parties unwilling to participate in the 26(f) discovery conference planning process.
-
- Intent: Bring collaboration and agreement to the discovery process in the early stages of litigation.
-
- Reality: Places a greater requirement on both parties to be prepared for the "meet and confer" negotiations.
-
- **FRCP Rule 45**
-
- Subpoenas to produce documents includes ESI.

Property of Law Office of Frances Crockett

-
- Intent: Clarifies rules for subpoenas to ensure consistency.
-
- Reality: No more arguing whether ESI is a "document."
-
- **FRCP Form 35**
-
- Standardizes discovery agreements.
-
- Intent: Avoid downstream delays and motion practice around discovery.
-
- Reality: Automatic reminder to include ESI where it is often overlooked.
-
- **Procedurally:** Once litigation has begun you may want to consider a motion to preserve documents. Within your motion make sure to elaborate on what documents you in good faith believe may exist or for that matter may have been or are likely to be destroyed.
- The Order is important because although negligent e-discovery conduct has been sanctioned in all 12 federal judicial circuits[3] the sanctions are not imposed for honest mistakes but against parties that destroy electronic evidence in violation of a court order to preserve said evidence. Note that dates of destruction are easily obtainable by IT experts.
- Once the opposing party is on notice you are ready to hire your IT Expert or if dealing with a small job having the opposing party produce the documents per your discovery request and Order per your motion to preserve.
- Key things are to look for evidence of mass deletions, backup drives should be searched, CDs and External hard drives as well, and most important don't forget to analyze print logs. Some may think they are savvy by covering up their electronic trail but you can get the print logs which showed the docs were printed and thus created and destroyed at one time after printing. Make sure to have the opposing party understand the keywords you are looking for in searches. May corporations and government municipalities have an archive so even of someone thinks they have deleted an email or memo it is still saved on the archive. The same is true of email folders such as a .pst files in Outlook for example.
- The case of *Zubulake v. USB Warburg, LLC* No. 02 Civ. 1243 (SAS) (S.D.N.Y. May 13, 2003) speaks to the burden of costs.
- Depositions: Make sure to have the IT person for Defendants identified and during discovery make sure to ask the company's document retention policy and practice and document management system structure.
- The typical cost of doing what I could consider a large job i.e. a complete search of The City of Albuquerque and the Albuquerque Police computer systems, including archives, was priced at $30,000.00. It is important to use a reputable outside agency, many can be found by doing a

[3] "The E-discovery Missteps that Judges Love to Hate," by Paul Neale, Law Practice Today, February 2005

Property of Law Office of Frances Crockett

simple Google search for Computer Forensic Expert. That way you avoid any issue as to admissibility.

- Examples of the types of data included in e-discovery are e-mail, instant messaging chats, documents, accounting databases, CAD/CAM files, Web sites, and any other electronically stored information that could be relevant evidence in a law suit. Also included in e-discovery is "raw data", which Forensic Investigators can review for hidden evidence. The original file format is known as the "native" format. Litigators may review material from e-discovery in one of several formats: printed paper, "native file,", PDF format, or as single- or multi-page TIFF images.
-
- Links/Resources:
  http://www.fjc.gov/public/home.nsf/autoframe?openform&url_l=/public/home.nsf/inavgeneral?openpage&url_r=/public/home.nsf/pages/196
  www.kenwithers.com
  Article and materials on Social networking regarding law enforcement:
  http://www.aele.org/los2010_sm-visual.pdf http://www.aele.org/los2010s&s.pdf
  http://www.aele.org/los2010_sm-glossary.pdf http://www.aele.org/los2010_sm-glossary.pdf

Property of Law Office of Frances Crockett