Cumberland Employment Law Update 2014

TECHNOLOGY TRAPS DURING DISCOVERY AND TRIAL

DAVID J. CANUPP & CHARLES E. GUERRIER

Agenda

- *Requesting and Resisting Disclosure of Electronic Information*
  - What the defense lawyer should ask for
  - The plaintiff's guide to preventing overreaching
- *Discovery Disputes*
  - Addressing e-discovery in the Rule 26 planning meeting
  - Discovery motions and fee-shifting
- *Using E-Discovery at Trial*
  - Authentication
  - Experts

Requesting and Resisting Disclosure of Electronic Information

Defense Perspective: Discovery Requests

- Defending an employment case requires understanding not only employer policies and expectations but the psyche of the plaintiff who you intend to show violated them.
- It is critical to piece together a full picture of the plaintiff so that you can demonstrate to the court, and the jury, who the plaintiff is.
- That has never been easier than it is today, with many of us living our lives in the cloud. As Chief Justice Roberts remarked earlier this year in *Riley v. California,* "[t]he sum of an individual's private life can be reconstructed" using information on a single smartphone.

Defense Perspective: Discovery Requests

- We live our lives in the cloud, communicating daily – even hourly – through electronic hosts:

Social Media	Communication Tools
Facebook (including Messenger)	Snapchat
Twitter	Text messaging (SMS)
LinkedIn	Emails
Tumblr	IMessage
Online Comments (e.g., www.AL.com)	Job Sites (Monster, CareerBuilder, Hot Jobs)
Reddit	Internal messaging
Blogs	

- If your stock employment discovery requests do not seek information about EACH of these (and more), you are already behind the curve.

Defense Perspective: Discovery Requests

- Smartphones (and embedded apps) almost always have background tracking of GPS data, and if not that, cell tower data.
- In cases in which the location of a plaintiff on a given day matters, this is a great resource – but expert consultants are likely to be needed.

Defense Perspective: Discovery Requests

- Text messages are key to ANY employment case.
  - Don’t have internal documentation: check texts.
- Likewise, internal messaging software may provide valuable evidence.
- And do not forget voicemails that may be stored on a smartphone or in emails

Defense Perspective: Discovery Requests

- Considerations in Seeking Data
  - Ownership of data
  - Trustworthiness of request target
  - Stored Communications Act, 18 U.S.C. 2701
- How do you obtain the information?
  - GPS Data
    - Directly from platform
    - Directly from plaintiff
  - Text Messaging / SMS
    - Almost certainly directly from plaintiff
      - Inspection of smartphone vs. request for production
  - Social Media Sites / Web-Based Messaging
    - Directly from platform
    - Directly from plaintiff
  - Emails
    - Directly from platform
    - Directly from plaintiff

Defense Perspective: Discovery Requests

- **Step One:**
  - Issue a **litigation hold** letter to plaintiff's counsel on the SAME DAY you receive word that you will defend the lawsuit. Be sure to request that smartphones and computers THEMSELVES be retained.
  - Issue a similar letter to your own clients. Follow up with a phone call or two.
- **Step Two:**
  - Use **interrogatories** to identify (a) types of / provider of social media and communication tools utilized; (b) identity of any smartphones and computers from which these tools were accessed and their present location and operability; (c) log-in and user name/ phone number for any accounts; (d) passwords for any accounts; (e) whether these social media and communication tools have been used to discuss relevant information.
    - Understand that many courts will not require passwords be turned over, but may consider appointment of a special master to receive such information. See *Original Honeybaked Ham*, 2012 WL 5430974 (D. Colo. Nov. 7, 2012)
  - Use a **request for production** to seek full copies of social media accounts and communications.
    - Again, understand some courts may limit such access to posts or entries "related to" the facts of the case. See *Ogden v. All-Star Career School*, 2014 WL 1646934 (W.D. Pa. Apr. 23, 2014); *Smith v. Hillshire Brands*, 2014 WL 2804188 (D. Kan. June 20, 2014).
    - However, many courts support broad production. See *Meyer v. DG Retail*, 2013 WL 5719508 (D. Kan. Oct. 21, 2013).
- **Step Three:**
  - Upon receipt of information from plaintiff, consider whether **subpoenas** to the provider are worth the time and effort.
    - The main barrier is the Stored Communications Act (SCA).
    - The SCA clear that production is **permissible** when the originator of a message consents (see Al *Noaimi v. Zaid*, 2012 WL 4758048 (D. Kan. Oct. 5, 2012)) . Accordingly, you should pursue a signed consent form from the plaintiff.
    - However, a signed consent alone does not **mandate** production. A court order (subpoena) is also required under the SCA. See *In re Facebook,* 923 F. Supp. 2d 1204 (N.D. Cal. 2012).
    - Even with a court order and signed consent, some social media sites still resist production.

Defense Perspective: Discovery Requests

- Facebook Requests
  - According to its website, Facebook takes the position that "Federal law does not allow private parties to obtain account contents (ex: messages, Timeline posts, photos) using subpoenas. See the Stored Communications Act, 18 U.S.C. § 2701 et seq."
  - However, it suggests that users "satisfy party and non-party discovery requirements relating to their Facebook accounts by producing and authenticating the contents of their accounts and by using the "Download Your Information" tool.
  - Facebook relies upon *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 965 (C.D. Cal. 2010), a decision that certainly can be questioned.
  - Regardless of the merit of Facebook's position, it has tremendous resources and a disinclination to cooperate: so a fight is likely if you choose this route.

Defense Perspective: Discovery Requests

- Despite the wealth of information available, consider the potential backlash of overbroad requests:
  - If a plaintiff's social media accounts and smartphone GPS data are relevant, a plaintiff could argue that the social media accounts and text messages of all managers and co-workers are relevant.
  - It is helpful to identify what information your client's managers have (and do not have) before entering an e-discovery war with the other side.

Plaintiffs' Perspective: Discovery Requests and Objections

- DO WE EVEN KNOW WHAT WE WANT?
- Will paper do?
- Will PDF's do?
- Spreadsheet: Printout or native format?
- Access to the raw data?

Do We Understand What Is Available?

- Does your client understand what ESI is kept by the employer?
- Do you or your colleagues have prior experience with this employer?
- What can you learn on line?

How do we ask for it?

- Ask for it!
- Rule 34(b)(1)(C) allows the requesting party to specify the form or forms in which ESI is to be produced.
- Rule 26(f) directs the parties to discuss discovery of ESI during the discovery-planning conference.
- Do it and cooperate!

Objections

- Responding party must either produce ESI in form requested or object and designate an alternate form.
- Obligation exists even if no specific form of production was requested.
- Party need not produce ESI in more than one form.
- Objection to form can be part of production.

Don’t encourage delay!

- Do not wait until the production date to learn about objections to the form of production.
- Address this early in the planning stage so as to avoid, to the extent possible, documents being produced in a form that is not preferred.
- Raise this issue with the Court during the planning conference.

Discovery Disputes

Anticipating Discovery Disputes at the Rule 26 Meeting

- Are you considering these provisions of Rule 26 at your parties' planning meeting?
  - Fed. R. Civ. P. 26(a)(1)(A) requires that parties provide in their initial disclosures "a copy – or a description by category and location – of all . . . electronically stored information" that the parties may use to support their positions.
  - Fed. R. Civ. P. 26(f)(3) explicitly directs the parties to discuss the form or forms in which electronically stored information might be produced.
  - Fed. R. Civ. P. 26(b)(2)(B) provides that: "A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost."
    - 2006 Committee Comments note that: "A party's identification of sources of electronically stored information as not reasonably accessible does not relieve the party of its common-law or statutory duties to preserve evidence."

Anticipating Discovery Disputes at the Rule 26 Meeting

- Plaintiffs' attorneys should know what social media and communication tools their clients use before ever filing suit, and should have a list ready for the Rule 26 meeting
- Defense attorneys should investigate whether their organizational clients have a social media presence and should inquire as to all communication tools utilized to confer with the plaintiff.
- Defense attorneys also need to have a basic under-standing of relevant software programs and backup tools utilized by organizational clients. This is something an IT department ought to be able to produce in a list form for defense counsel at the very beginning of any case.
- Counsel for the parties should freely discuss this information at the planning meeting. Yes, this means it is more likely you will have to "deal with" electronic discovery, but it also makes the process a lot easier.

Anticipating Discovery Disputes at the Rule 26 Meeting

- Consider stipulations in the Parties' Planning Meeting Report concerning the outward limits of electronic discovery:
  - "Will not seek X, Y, and Z"
  - "Must act to preserve A, B, C"
  - "Must deliver list of M, N, O"
  - "Stipulate to authenticity of J, K, L"
    - If too early to stipulate, consider including a requirement that counsel meet 90 days prior to close to discovery to consider what stipulations can be made about authentication to avoid expert expenses

Discovery Motions and Fee-Shifting

- Presumption is that responding party must bear the expense of complying with discovery requests. *Zubulake v. UBS Warburg LLC*, 216 F.R.D. 280 (S.D.N.Y. 2003)
- Cost-shifting potentially appropriate only when inaccessible data is sought.

Discovery Motions and Fee-Shifting

- Active, online data, near-line data, and offline storage/archives are “accessible” ESI.
- Backup tapes and erased, fragmented or damaged data are typically “inaccessible.”

Zubulake Factors

- Specifically tailored request
- Availability from other sources
- Cost of production/amount in controversy
- Total cost of production
- Relative ability to pay and incentive
- Importance of the issue at stake
- Relative benefits to the parties

Duty when responding to request

- Respondent must conduct a reasonable search for responsive documents. Parties and attorneys have a duty to act competently, diligently, and ethically when discharging discovery obligations. This requires a joint effort to identify all employees likely to have been authors, recipients or custodians of documents responsive to the requests.

Duty when responding (cont.)

- Parties jeopardize the integrity of the discovery process by engaging in halfhearted and ineffective efforts to identify and produce relevant documents. Party does not meet its obligations "by sticking its head in the sand and refusing to look for [documents]. It is inexcusable . . . to respond to a request for production without reviewing the computer of a primary actor in the sequence of events leading to litigation." *Robinson v. City of Arkansas City, Kan.*, 2012 WL 603576 (D. Kan. 2012)

Using E-Discovery at Trial

Authentication

- Fed. R. Evid. 901 governs authentication. Rule 901 merely requires that the proponent of an item "produce evidence sufficient to support a finding that the item is what the proponent claims it is."
- In addition, Fed. R. Evid. 1002 requires that when evidence offered is a "writing," the "original" must be offered as the "best evidence." However, under Fed. R. Evid. 1001(3), when records or data are stored "in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an 'original.'"
- Accordingly, the inquiry under both Rules often compresses into a single question of whether the item can be reasonably show to reflect the data accurately.

Authentication

Courts and practitioners alike have a tendency to “freak out” about authentication of electronic items.

- It can get complicated:
  - For example, if your client was the recipient of a text message, s/he may not be able to verify WHO sent the text message.
  - Compare *United States v. Winters*, 530 Fed. Appx. 390 (5th Cir. 2013) (holding that photographs of drugs and weapons on a website were not properly authenticated because it was not established who posted the photographs or who owned the items depicted, even though defendant admitted he owned the website itself)
- But consider whether authentication is really a problem:
  - A photograph offered merely to show what it depicts can be authenticated by anyone who can attest that it reasonably depicts what it purports to depict. *U.S. v. Clayton,* 643 F.2d 1071 (5th Cir. 1981). Why can’t a screenshot of a Facebook status or the like do the same?
  - Although you may not be able to prove who created the content, is it enough on your facts that the recipient believed the other party sent the message or posted the photograph?
  - Can you get the sender of the message to admit sending it?
  - Can you use background details to show that it is likely the content was generated by your opponent?
  - These alternatives may be the reason that there are very few reported cases regarding authentication of electronic evidence.

Authentication

- Where authentication is really an issue, keep in mind the relative burdens:
  - At summary judgment, Rule 56 only requires the use of evidence that ***can be*** produced in admissible form ***at trial***. *Abbott v. Elwood Staffing Services, Inc*., 2014 WL 3809808 (N.D. Ala. 2014).
    - In other words, following the 2010 Amendments to Rule 56, there is no requirement that documents be authenticated at the summary judgment stage.
  - At trial, authentication is governed by Fed. R. Evid. 901, which "only requires a proponent to present sufficient evidence to make out a prima facie case that the proffered evidence is what it purports to be." *U.S. v. Lebowitz,* 676 F.3d 1000 (11th Cir. 2012). "After meeting the prima facie burden, the evidence may be admitted, and the ultimate question of authenticity is then decided by the jury." *Id.*

Authentication

- The Eleventh Circuit has been fairly realistic when it comes to authenticating electronic evidence.
- In *U.S. v. Lebowitz*, 676 F.3d 1000 (11th Cir. 2012), the Court held that printouts of internet chat conversations offered into evidence at trial were admissible since a witness testified that he printed out the chats and that the printouts were accurate reflections of the chat messages he viewed.
  - The Court also considered relevant the fact that other testimony confirmed events consistent with the chat messages.
- The Court rejected any attempt to insist that the best evidence rule required use of the original messages at trial.

Authentication

- The Court in *U.S. v. Grant*, 2011 WL 6015856 (Air Force Ct. Crim. App.) confronted a question of whether Facebook messages were properly authenticated under Mil. R. Evid. 901.
- The Court allowed the messages to be introduced when a victim testified that the defendant “added” her as a Facebook friend shortly after meeting her, and that his profile picture was an accurate depiction of him.
- The Court also found it significant that the defendant gave the victim his number on Facebook and she subsequently used it with success to reach him.

Using Experts at Trial

- Unless you are particularly knowledgeable and have nothing else to do, you need an expert to consult with during discovery.
- You will probably need an expert to help you understand and analyze the data.
- The parties might consider jointly hiring an expert to image computers or compile/extract a common database.

Using Experts At Trial

- You may need an expert to interpret metadata.
- You may need an expert to testify about what the data means.
- You may need a forensic expert to identify whether ESI has been altered, deleted, or damaged.

Questions?

David J. Canupp
Lanier Ford Shaver & Payne, P.C.
Huntsville, AL
djc@lanierford.com
(256) 535-1100
www.lanierford.com

Charles Guerrier
Haynes & Haynes, P.C.
Birmingham, AL
ceguerrier@haynes-haynes.com
(205) 879-0377
www.haynes-haynes.com