## V. Real-World Examples, Handy How-to's and Sample Screen Shots

Sara Anne Hook, M.B.A., J.D.

[N.B.: Case summaries retrieved from the K&L Gates database are designated as KLG. Case summaries retrieved from the Kroll Ontrack database are designated as KO. Case summaries from Exterro are designated EX. An effort has been made to select a variety of recent cases, particularly cases from 2014-2017, as appropriate to each type of electronic evidence. Note that the most recent cases were very quickly being decided by applying the 2015 amendments to the Federal Rules of Civil Procedure.]

It is quite interesting to search for the technologies and tools mentioned in Sections B. through K and note how the cases about them ebb and flow throughout the years. For example, some of the technologies are rarely mentioned in more recent case summaries in the K&L Gates and Kroll Ontrack databases, but cases about them were prominent beforehand. Lawyers are encouraged to consult the websites of K&L Gates (https://www.ediscoverylaw.com/, accessed 10/13/17), Kroll Ontrack (https://www.krollontrack.com/, accessed 10/13/17), Exterro (https://www.exterro.com/, accessed 10/13/17) and Sensei Enterprises, Inc. (https://senseient.com/, accessed 10/13/17) for the latest information, guidance and resources about electronic discovery issues and challenges, particularly with social media.

### A. Preservation, Spoliation and Authentication Obstacles

There are a number of excellent sources for information on preservation, spoliation and authentication of social media as evidence. A presentation on social media as evidence at the ABA Annual Meeting in 2013 provides a number of information about authentication:

> **Authentication**. FRE 901 establishes the requirements for authentication or identification as a condition precedent to the admissibility of non-testimonial evidence. FRE 901(b) gives examples of how authentication can be accomplished. Generally, the proponent of the internet printout must provide testimony by live witness or affidavit that the printout is what it purports to be. *See In re Carrsow-Franklin*, 456 B.R. 753, 756-57 (Bankr.D.S.C. 2011) (noting that blogs are not self-authenticating and rejecting blog evidence due to failure to present authentication testimony) and cases cited there. The Lorraine case gives an excellent discussion of how Rule FRE 901 works with FRE 104 and the necessity for the court to decide authentication as a preliminary question. However, if the evidence is not relevant to begin with, it cannot be authenticated because it cannot meet the requirements under FRE 104 and 401.

> These evidentiary rules do not appear to be consistently applied between the criminal and civil contexts. Some state criminal courts appear to fail to apply or misapply the evidentiary rules. For example, in *Griffin v. State*, 419 Md. 343, 19 A.3d 415 (Md. Ct. App. 2011), the court overturned conviction for felonies including second-degree murder because MySpace pages of defendant's girlfriend on which there were threats ("snitches get stitches") against a key witness lacked a proper foundation as they were not properly authenticated. The court analyzed a Maryland rule of evidence that was, in part, similar to FRE 901 and looked at decisions in other states. The court held that the prosecutor's effort to authenticate through the police investigator rather than the girlfriend, who testified at trial, was insufficient. The court noted that the prosecution could also have searched the computer of the person who allegedly created the profile and the posting or sought information from the social media website. The Griffin opinion appears to be based more on the court's skepticism about admitting internet evidence in general. The court focused on the fact that the evidence may have been created by someone other than its putative creator, even in the absence of any evidence that this in fact happened, and then excluded the evidence on the grounds that there was inaccurate authentication. The reasoning in Griffin conflicts with FRE 104 and 901 and Lorraine in which Judge Grimm stated that authentication "as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims . . . This is not a particularly high barrier to overcome . . . as [a] party seeking to admit an exhibit need only make a prima facie showing that it is what he or she claims it to be . . . [and] '[t]he court need not find that the evidence is necessarily what the proponent claims, but only that there is sufficient evidence that the jury might ultimately do so.'" 241 F.R.D. at 541–42 (internal citation omitted).
>
> In *People v. Clevenstine*, 68 A.D.3d 1448, 891 N.Y.S.2d 511 (2009), the court held that MySpace messages were properly admitted in a rape case. Defendant asserted that someone else accessed his account and posted the messages. Both victims testified that they had engaged in MySpace instant messaging with defendant about sexual activities, a police investigator retrieved the messages from the hard drive of the computer of the victims, and a MySpace employee testified that the messages had been between the victims and users of accounts created by the defendant. The court applied New York case law on authentication without any reference to evidentiary rules. [Gary L. Beaver, Steven Brower, Amy Longo, Cecil A. Lynn, III, & Mark Romance, *Social Media Evidence – How to Find It and How to Use It*, ABA Annual Meeting, Aug. 8-12, 2013, at 20-21.]

Additional information is provided on identification of parties using social media, relevant, hearsay and unfair prejudice. [*Id.* at 21-22.] The authors also offer a number of helpful recommendations for the discovery of social media evidence. Discovery requests/subpoenas for social media evidence should be drawn narrowly. (This is especially important given the 2015 amendments to the Federal Rules of Civil Procedure.)

- Tie your discovery requests to information already in hand that shows that the request is seeking evidence that likely exists and, therefore, is not a fishing expedition.

- Compulsion efforts are better targeted at the users of social media, not at the social media providers.
- If you have evidence that the producing party has improperly withheld evidence, go to the court for sanctions and/or for more social media discovery.
- Consider closely who "owns" the social media link. You may have more than one potential discovery target.
- *In camera* review by the court may be needed.
- If the request is too broad, the court may limit it or deny it altogether. (Be sure to review the 2015 amendments to the Federal Rules of Civil Procedure.) [*Id*. at 15-19.]

Nelson and Simek provide some excellent suggestions for dealing with social media as evidence, including preservation and authentication. [Sharon D. Nelson & John W. Simek, Social Media: Preservation, Harvesting and Authentication, Sensei Enterprises, Inc, 2014, https://senseient.com/articles/social-media-preservation-harvesting-and-authentication/, accessed 10/13/17.]

A recent article by Foster discusses the admissibility of social media evidence in federal courts. [Angela Foster, *Admissibility of Social Media Evidence in Federal Courts: Is It What It Purports to Be?* The Computer & Internet Lawyer, June 2016, pp. 13-16.] Noting that the admissibility of social media evidence as increasingly become a highly litigated issue, Foster begins her article by explaining why merely accessing social media is not enough to authenticate is. [*Id*. at 13-14.] She then describes why evidence from fake social media accounts may be admissible, citing *U.S. v. Gaston* (Instagram) and *U.S. v. Meregildo* (Facebook). [*Id*. at 14-15.]

She discusses why caution is needed when thinking about whether to delete social media evidence, citing *Gatto v. United Air Lines, Inc.* (Facebook). [*Id*. at 15-16.] It is important to note that *Gatto* was decided in 2013, which pre-dates the 2015 amendments to the Federal Rules of Civil Procedure. As she summarizes,

> Because courts have different holdings regarding the authenticity and admission of social media evidence, attorneys must know their jurisdiction. Moreover, proper authentication differs based on the purpose and context of the evidence being presented. Accordingly, careful consideration must be given to requirements needed to properly authenticate social media evidence *before* the trial. The Federal Rules of Evidence provides some guidance on how to authenticate evidence. Specifically, Federal Rules 901(b) and 902 may be applied to social media evidence. [*Id*. at 16.]

Interestingly, amendments to the Federal Rules of Evidence, specifically Rules 803, Rule 902(13) and 902(14) are being considered and, if approved, would become effective on December 1, 2017.

If you really want to understand each type of electronic evidence, how it is generated, by which software and devices, how to retrieve it and preserve it and how to uncover evidence that has been hidden or tampered with, please read *Electronically Stored Information: The Complete Guide to Management, Understanding, Acquisition, Storage, Search, and Retrieval*, 2nd ed. [David R. Matthews, *Electronically Stored Information: The Complete Guide to Management, Understanding, Acquisition, Storage, Search, and Retrieval*, 2nd ed. CRC Press, 2016.] I use it as one of my textbooks in the semester-long course I teach on electronic discovery, which is part of the legal informatics certificate offered by the Indiana University School of Informatics and Computing at IUPUI. You will enjoy the history of how each new technology developed, from analog to digital, the electronic discovery implications of this technology and the clear explanations for how computing programming works, down to the zeros and ones of binary computer code.

A very thorough article about common problems with electronic discovery and suggested solutions is provided by Hernandez. [Andres Hernandez, *Common Problems With E-Discovery and Their Solutions*. The Federal Lawyer, Sept. 2016, pp. 63-68.] Among the issues that he highlights and provides recommendations for are:

- There's just too much data
- Data is everywhere
- Data collection – including the issues with self-collection
- Not all data is created equal
- What to do if you know exactly what you are looking for, such as using metadata analysis and textual analytics
- What to do if you are trying to fill in knowledge gaps, including the importance of using keywords intelligently
- What to do if you are still trying to understand your case, including using concept-clustering, using a word frequency hit count or using TAR (Technology-Assisted Review)
- Dealing with the expense of the process, with a list of URLs for vendors offering cost-effective solutions
- Falling into the trap of "scope creep"
- Not starting the e-discovery process early enough

- E-discovery approached as a project, with the recommendation to help clients set up better information governance programs (a potential practice-building opportunity for law firms?)
- When your analytics are not good enough
- Lack of convergence
- Unwillingness to work cooperatively with opposing parties and their lawyers
- Difficulty recovering the costs of e-discovery
- Laws are complex and constantly changing
- It is almost impossible to compare e-discovery providers
- Technological incompetence – see Rule 1.1 and Section VI. of this seminar manual
- Data is sorely mismanaged

B. Facebook, Twitter, LinkedIn and Tumblr

- *Rhone v. Schneider Nat'l Carriers, Inc.*, 2016 U.S. Dist. LEXIS 53346 (E.D. Mo. Apr. 21, 2016).
  (Facebook, motion to compel, social media, burdensome, overbroad)

  In this personal injury case, the defendants moved to compel the plaintiff to produce her "Download Your Info" report from Facebook, from the date of the accident to the present. The plaintiff objected that the request, arguing that it was overbroad as found in FRCP 26(b)(1), and moot because she already submitted hundreds of pages of Facebook postings. The court found that the plaintiff did not comply with the discovery request, since the "[p]laintiff did not initially disclose the existence of any social media accounts," and ordered the plaintiff to produce the requested information. In reaching its decision, the court noted the insufficiency of the plaintiff's objection, stating, "[a]lthough Plaintiff maintains that [defendant's] request is overbroad and asserts that such a production would be unduly burdensome, Plaintiff does not explain how it is overbroad or burdensome." [KO]

- *Thurmond v. Bowman*, 2016 WL 1295957 (W.D.N.Y. Mar. 31, 2016).
  (Social media, relevance, spoliation)

  In this Fair Housing Act case, the defendants motioned for sanctions against the plaintiff for deleting Facebook posts. The plaintiff argued that the posts were not deleted intentionally, but rather they were "hidden" from public view. The plaintiff produced a printed set of Facebook posts, which supplied most of the missing posts, but three posts remained missing. The court found that these posts, because of their nature (photographs of the plaintiff's children, supplied as "screen shots" by the defendants), were not relevant to the case. In addition, rather than relying on public privacy settings, the court noted that the defendants could have requested the information through discovery. The court denied the defendants' motion, stating that the claim that every social media post is relevant "sweeps far too broadly." However, because the plaintiff did change privacy settings in violation of a court order to maintain the "status quo" of social media accounts, the plaintiff was warned that further conduct in this manner could result in sanctions. [KO]

- *Keller v. National Farmers Union Property & Cas. Co.*, 2013 WL 27731 (D. Mont. Jan. 2, 2013).
  (Motion to compel, production, social networking, social network, expectation of privacy)

  In this insurance dispute, the defendant insurance company moved for an order compelling the plaintiffs to respond to discovery requests for the production of their social network content, "including, but not limited to, Facebook, Myspace, Twitter, LinkedIn, LiveJournal, Tagged, Meetup, myLife, Instagram and MeetMe," as well as pre-accident medical records. As to the social network content, plaintiffs objected that the request was "overly burdensome and meant to harass . . . insureds." In response, the

defendant cited *Romano v. Steelcase*, in which the court ruled that social networking content is often relevant in determining whether a plaintiff is actually injured, and that a plaintiff has no legitimate expectation of privacy in those communications. However, the court, citing *Tompkins v. Detroit Metropolitan Airport*, ruled that the defendant must make a threshold showing that publicly available information on social networking sites undermines the plaintiffs' claims, so as to guard against the "proverbial fishing expedition." The court determined that the defendant had not made this requisite threshold showing, and is thus not entitled to "delve carte blanche" into the nonpublic sections of the plaintiffs' social networking accounts. [KO]

- *People v. Harris*, 2011NY080152 (NY Crim. Ct. New York Co. June 30, 2012).
(Twitter, tweets, social media, Stored Communications Act, standing, third party respondent, motion to quash, subpoena, metadata, posts)

  In this criminal matter arising out of the Occupy Wall Street protests, the court reviewed Twitter's motion to quash a subpoena, which ordered the production of tweets and pertinent metadata from a user's account. The threshold determination required an assessment of whether the criminal defendant or the third party respondent (Twitter) had standing to quash the subpoena. In line with the court's previous ruling on this matter, the court pointed to Twitter's terms and policy, holding that Twitter—not the criminal defendant—had standing to challenge the subpoena. Addressing Twitter's contention that responding to numerous subpoenas would result in an undue burden (and thus barred by the SCA), the court held that because all third party respondents bear this burden, the argument "cannot be used to create standing for a defendant where none exists." Further, the court noted that "it does not take much to search and provide the data to the court." The court found that Twitter's services fall within the statutory definition of both an Electronic Communication Service (ECS) (generally, a communication service) and a Remote Communication Service (RCS) (generally, a storage service for substantive posts and metadata produced by the chat service). Equating public tweets to yelling on the street, the court further determined that the posts were not "private" and thus not outside of the scope of the SCA. Ultimately, the court largely denied Twitter's motion to quash the subpoena, holding that the prosecutor must obtain a search warrant for tweets within 180 days of the decision date to comply with the SCA. [KO]

- *Lemon Juice v. Twitter, Inc.*, No. 502898/14, 2014 WL 4287049 (N.Y. Sup. Ct. Aug. 29, 2014).
(Twitter subscriber information sufficient to identify the individual(s) who owned or operated particular Twitter account and logged into or "tweeted" on the account)

  Where unknown person created Twitter account in plaintiff's name and in violation of criminal court's order took photo of child victim in court testifying against her tormentor and posted it to Twitter account, court ruled that plaintiff had met his burden of demonstrating a meritorious claim for intentional infliction of emotional distress and that the discovery sought from Twitter was needed in order to identify who should be named as a defendant, and that anonymous Twitter account creator's behavior constituted an actionable tort and was not speech covered by First Amendment protection such that

anonymity of creator had to yield to plaintiff's need to redress the actionable wrong perpetrated against him; court directed Twitter to disclose basic subscriber information, records, internet protocol addresses and other similar information sufficient to identify owner of the bogus Twitter account and to preserve certain evidence. [KLG]

- *Wilson v. Indiana* No. 45A03-1409-CR-317, 2015 WL 1963860 (Ind. Ct. App. Apr. 30, 2015). – NOTE: Indiana case.
(Twitter)

  In a criminal matter, the court said that Twitter messages could be authenticated under Indiana Rules of Evidence Rule 901(b) by, for example, "(1) Testimony of a Witness with Knowledge" and by "(4) Distinctive Characteristics and the Like" and these examples were satisfied where a witness testified that she had communicated with the defendant on Twitter via the account in question and testified that the account contained both pictures of the defendant and references to activities that were sufficient to indicate that the posts had been authored by the defendant. [KLG]

- *Del Gallo v. City of New York*, 997 N.Y.S.2d 98 (Table) (N.Y. Sup. Ct.2014).
(Social media contents (e.g., LinkedIn))

  Addressing request for discovery of Plaintiff's social media contents, specifically LinkedIn, court indicated that "[t]o warrant such discovery, 'defendants must establish a factual predicate for their request by identifying relevant information in plaintiff's [social media] account -- that is, information that contradicts or conflicts with plaintiff's alleged restrictions, disabilities, and losses, and other claims'" and, although it acknowledged that Defendants could obtain information pertinent to Plaintiff's communications with recruiters related to job offers and related inquiries, indicated that Defendants had not shown that they were entitled to Plaintiff's communications with former colleagues about her condition or to the other materials on LinkedIn. [KLG]

- *Brown v. Ferguson*, No. 4:15CV00831 ERW, 2017 WL 386544 (E.D. Mo. Jan. 27, 2017).
(Social Media/social network (Facebook, etc.))

  Court clarified discoverability of relevant social media content but indicated that disclosure of passwords was not required and not permitted by the Federal Rules of Civil Procedure. [KLG]

- *Gordon v. T.G.R. Logistics, Inc.*, No. 16-cv-00238-NDF, 2017 WL 1947537 (D. Wy. May 10, 2017).
(Social media (Facebook))

  In this personal injury case, Defendant requested production of Plaintiff's entire "Facebook account history" for her two accounts (and later limited the relevant timeframe of the request to information from three years prior to the accident through the present). In response, Plaintiff produced information that referenced the at-issue auto

accident or her injuries and also provided information identified by a set of keywords set forth by Defendant. She objected to further production based on a lack of relevance, undue burden, and invasion of privacy. The court granted Defendant's subsequent motion to compel, but imposed significant limits on the scope of production. [KLG]

- *Zamora v. Stellar Mgmt. Grp., Inc.*, 3:16-05028-CV-RK, 2017 WL 1362688 (W.D. Mo., Mar. 11, 2017).
  (ESI from cellular phones, Facebook)

  Where Plaintiff in an employment litigation failed to preserve a potentially relevant Facebook post, deleted her work phone before returning it and failed to preserve information contained on numerous other phones (e.g., because they were lost, etc.), court found that "Plaintiff cannot be relied on to disclose all relevant communications" and granted motion to allow access to the mirror image of a phone belonging to a former employee and co-worker of the plaintiff and to allow defendant to subpoena the former employee to produce a second phone for inspection and ordered production of Plaintiff's current work phone, to be reviewed by a Special Master for potentially relevant communications, with the cost of the Special Master to be split between the parties ; court found request for dismissal or an adverse inference was premature. [KLG]

- *Cohn v. Guaranteed Rate, Inc*., No. 1:14-cv-9369, 2016 WL 7157358 (N.D. Ill. Dec 8, 2016).
  (Emails (Gmail, but also LinkedIn))

  Defendant sought production of Plaintiff's emails, imposition of spoliation sanctions, and an extension of the discovery deadline. Plaintiff previously agreed to produce responsive documents from her Gmail and LinkedIn account, but failed to do so (later third party productions contained emails sent from her Gmail account). Plaintiff admitted she deleted emails from her Gmail account at various times, and evidence showed she instructed a subordinate to start using their personal email addresses and to delete various emails. The court found (i) a duty to preserve existed as of at least November 30, 2013, (ii) that Plaintiff breached that duty when she deleted emails, and (iii) there was a strong inference that the emails would have been unfavorable to Plaintiff because (iv) she deleted the emails in bad faith (to admittedly 'hide' the information). The court denied Defendant's motion for equitable relief, but allowed Defendant's alternate request that Plaintiff must provide full access to her Gmail account (details to be addressed in a meet-and-confer). [KLG]

C. Emails (Work-Related and Personal)

It is very clear that, absent some narrow exceptions, email messages are electronically stored information (ESI) that is discoverable and admissible in court. Indeed, email messages were the heart of the evidence in the *Zubulake v. UBS Warburg* case, the very foundation of electronic discovery. However, email as evidence continues to be the subject of dispute in many e-discovery cases, particularly when a party is using a personal device or a personal email. The issue of emails sent via a private server and the blending of personal, work-related and even classified communications haunted former Secretary of State Clinton's campaign for President and caused such consternation that Congress proposed H.R.3743 Securing Every Relevant and Vital Electronic Record Act of 2015 or the SERVER Act, which would prohibit:

> the Secretary of a cabinet-level executive department from maintaining a private email server to conduct official government business. The Inspector General of each such department shall ensure compliance with such prohibition. A Secretary who violates such prohibition is subject to a fine and/or prison term and shall forfeit his or her office and be disqualified from holding any U.S. government office. [Summary: H.R. 3743, 114th Congress (2015-2016).]

> *See also* H.Res.477 - Expressing the sense of the House of Representatives that a special counsel should be appointed by the Attorney General or his designee to investigate misconduct by former Attorney General Loretta Lynch and former Federal Bureau of Investigation Director James B. Comey with regard to the investigation of former Secretary of State Hillary Clinton for mishandling of classified data and use of an unauthorized email server. [Summary: H.Res. 477, 115th Congress (2017-2018).]

Congress and the administration continued to grapple with other issues related to email during 2015-2016. As reported by Moyer in March 2016,

> Congressional support for the modernization legislation called the Email Privacy Act has grown since its introduction several years ago. More than 300 House members today are co-sponsors of the measure, a number greater than any other bill pending in the House of Representatives and a reflection of the breadth of bipartisan support for privacy protection.
>
> Introduced in the House by Rep. Kevin Yoder (R-Kan.) and in the Senate by Patrick Leahy (R-Vt.), the Email Privacy Act (H.R. 699 and S. 356) would change the framework for law enforcement access to email (and texts and other electronic content) housed with Internet service providers, like Google and Yahoo, and bring the statute in line with the Sixth Circuit's opinion in *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010), which requires the government to obtain a warrant to access emails, regardless of

> their age. [Bruce Moyer, *You've Got Mail…and a Warrant for Its Disclosure*, The Federal Lawyer 6-7 (Mar. 2016).]

A second bill is H.R.4709, the Unsubscribe From All Act of 2016. Per the Summary,

> This bill amends the CAN-SPAM Act of 2003 to require commercial email messages to contain an "unsubscribe from all" option that recipients may select, with not more than one additional action required by the recipient, to send a reply requesting not to receive future emails from the sender.
>
> A commercial email message must remain capable of receiving such unsubscribe replies for at least 30 days after the transmission of the original message. [Summary: H.R. 4709, 114th Congress (2015-2016).]

The author notes that the last time Congress updated email privacy laws was in 1986 when it established the Electronic Communications Privacy Act (ECPA), which was intended to protect wire, oral and electronic communications when those communications were being made, were in transit and when stored on computers and includes email, telephone conversations and data stored electronically. [*Id*. at 6.] However, he observes that these distinctions and the motivation for the ECPA have been outpaced by technology. [*Id*.] As an example, he indicates that the ECPA permits the government to access email messages without a warrant if they are stored by the service provider for more than 180 days, but a court-imposed warrant must be secured for email messages that are stored for fewer than 180 days, a distinction that is quite outdated. [*Id*.] As part of his article, the author includes concerns expressed by the Department of Justice (DOJ) and various federal civil enforcement agencies, such as the Securities and Exchange Commission (SEC). [*Id*. at 6-7.] Additional bills have been introduced in Congress during 2017 that attempt to balance consumer privacy interests versus the need for law enforcement to have access to personal information. For example, S.1654 Email Privacy Act would "amend title 18, United States Code, to update the privacy protections for electronic communications information that is stored by third-party service providers in order to protect consumer privacy interests while meeting law enforcement needs, and for other purposes." [Summary: S.1654 Email Privacy Act, 115th Congress (2017-2018), *see also* H.R.. 387.]

On the other hand, email continues to be a rich repository of potentially relevant evidence. It is still the primary means of communication in many companies, non-profit organizations and government agencies. However, the issues with email as ESI become even

more complicated in an increasingly BYOD (Bring Your Own Device) environment, where employees are expected to be "on the clock" 24/7 and to use their personal systems and devices to do this. Nelson and Simek are especially blunt about the risks that employees pose in the workplace, especially in a BYOD environment, including the danger of compromising an electronic discovery process. [Sharon D. Nelson & John W. Simek, *Five Cybersecurity Worries to Give You the Willies*, Sensei Enterprises (2016), http://senseient.com/wp-content/uploads/Five-Cybersecurity-Worries-to-Give-You-the-Willies.pdf, accessed 10/16/17.]

> Employees are by nature rogues. In every study that's been made, they will ignore policies (assuming they exist) in order to do what they want to do. This often means that they bring their own devices (BYOD) which may be infected when they connect to your network. They may also bring their own network (BYON) or bring their own cloud (BYOC). Certainly your policies should disallow these practices (in our judgment) or at least manage the risks by controlling what it is done by a combination of polices and technologies.
>
> Oh, and they steal your data or leave it on flash drives, their home devices, etc. This means you have "dark data" – data you don't know about and over which you have no control. This means you may miss data required in discovery because you don't know it exists. Your data may not be protected in compliance with federal or state laws and regulations. Once again, a combination of policies and technology should be in place to prevent these issues. [*Id.* at 1-2.]
>
> A few recent cases involving disputes about email are as follows:

- *FiTeq Inc. v. Venture Corp.*, 2016 WL 1701794 (N.D. Cal. Apr. 28, 2016). (Prejudice, Rule 37, spoliation, sanctions, emails)

  In this contract law case, the plaintiff moved for sanctions against the defendant for failing to produce emails related to the litigation. Namely, the plaintiff asked the court to grant a Motion *in Limine* to allow a jury instruction for spoliation of evidence. The defendant argued that the recently amended FRCP 37(e) only allows sanctions when the evidence "cannot be restored or replaced through additional discovery," and the plaintiff never sought additional discovery. Secondly, the defendant argued that FRCP 37(e) requires a "finding [of] prejudice to another party from the loss of the information," and here, the "missing" emails were already available to the plaintiff. Finally, the defendant argued that there was no intent to deprive the plaintiff of any evidence, as the recovered emails were deleted as part of "routine housekeeping." The court agreed with the defendant, and denied the plaintiff's Motion *in Limine*, stating that the plaintiff "failed to prove that the other . . . documents ever existed." [KO]

- *Sunderland v. Suffolk Cty.*, 2016 U.S. Dist. LEXIS 77212 (E.D.N.Y. June 14, 2016). (Personal computer, Rule 26(b)(1), email, undue burden, relevance, documents)

NOTE: Personal computers and email accounts

In this civil rights case, the plaintiff motioned the court to compel the defendants "to search for and produce certain documents from their personal computers and email accounts." The defendants argued that while their electronic work devices and accounts can be searched, their personal items are not discoverable. The court granted the plaintiff's motion to compel, explaining that the personal documents are relevant under FRCP 26(b)(1), even after the December 2015 amendments. The court elaborated that the nature of the case made it likely that relevant information would have been kept on a personal device or account rather than a work one. In its reasoning, the court further explained that such a search is not overly burdensome because the parties already agreed to the terms to be used, the searches had a limited temporal scope, and the plaintiff insisted that the defendants' computers would not have to undergo forensic inspection. [KO]

- *Mathew Enter. v. Chrysler Grp. LLC*, No. 13-cv-04236-BLF, 2016 U.S. Dist. LEXIS 67561 (N.D. Cal. May 23, 2016).
(Sanctions, spoliation, preservation, email, Rule 37(e))

  In this price discrimination case, the plaintiff's internal and external emails concerning its dealership business practices were irretrievable because the plaintiff made no effort to preserve documents. After threatening the defendant with litigation, the plaintiff not only switched email systems, but also failed to notify its database vendor of the potential for litigation. Emails continued to be deleted regularly per normal business practices. The defendant motioned for sanctions against the plaintiff for the loss of these communications, stating that there was no effort made to preserve and urged the court to utilize spoliation sanctions. The judge, Magistrate Judge Paul Grewal, issued FRCP 37(e) sanctions by expanding the scope of evidence the defendant is allowed to bring to trial and awarding reasonable attorney's fees. "[Plaintiff's] lackadaisical attitude towards document preservation took away that opportunity. Not only has spoliation occurred, but it also has prejudiced [defendant]." [KO]

- *Matthew Enter. v. Chrysler Grp.*, 2015 WL 8482256 (N.D. Cal. Dec. 10, 2015).
(Motion to compel, personal email)

  NOTE: Personal email accounts.

  In this case, the defendant moved to compel additional ESI, including emails from employees' corporate Gmail accounts and financial documents. The plaintiff did not provide all of its employees with a company email account, and many used their personal email accounts for business. The plaintiff argued that it could not comply with the defendant's motion because those accounts were not in its "possession, custody, or control" and were thus outside the scope of discovery. The defendant argued that the plaintiff's employee handbook "instructs employees to keep 'internal information' in the 'sole possession'" of the plaintiff's business. The court rejected the defendant's argument, holding that the handbook was not a contract and did not create a "legal right" for the plaintiff to "take back any such information now stored in personal accounts." The

court also concluded that the defendant had not identified any authority by which the plaintiff could force its employees to produce the desired emails. Therefore, the court denied the motion in part as to the personal email accounts, although it granted it in part as to the plaintiff's vendor-maintained database. [KO]

- *Brown Jordan Int'l, Inc. v. Carmicle*, Nos. 0:14-CV-60629, 0:14-CV-61415, 2016 WL 815827 (Mar. 2, 2016).
(ESI, spoliation, personal device, emails, alteration of metadata)

  Upon determining that "applying the new version of Rule 37(e) would be neither unjust nor impractical," the court found that Defendant failed to take reasonable steps to preserve the information at-issue, despite a duty to do so; that the lost information could not be restored or replaced through additional discovery; and that Defendant acted with the intent to deprive Plaintiffs of the information's use in the litigation. Accordingly, the court presumed that the lost information was unfavorable to the defendant. Specifically, Defendant's spoliation included the remote wiping of his company-owned laptop, the alleged loss of his personal iPad, and the accessing of 2.4 million files on his personal laptop, thus changing the metadata prior to forensic examination, among other things. [KLG]

- *CAT3 LLC v. Black Lineage, Inc*, No. 14 Civ. 5511 (AT) (JCF), 2016 WL 154116 (S.D.N.Y. Jan. 12, 2016).
(Email)

  Court found "clear and convincing" evidence that Plaintiffs had manipulated emails to gain an advantage in the litigation where Defendants' forensic analyst found the original versions of emails that had been altered and then deleted and imposed recently amended Rule 37(e) upon determining that the original emails had been "lost" and could not be "restored or replaced" because the "fact that there [were] near-duplicate emails showing different addresses casts doubt on the authenticity of both"; applying Rule 37(e) court determined that subsection (e)(2) applied because of the intentional nature of the manipulation but, noting the enumerated sanctions were not mandatory, instead precluded Plaintiff from relying upon "their version" of the emails to establish certain elements of their claim and imposed payment of reasonable attorney's fees incurred by Defendants; notably, court's analysis also concluded that sanctions would also be available under the court's inherent authority to impose sanctions for bad faith spoliation. [KLG]

- *Agility Pub. Warehousing Co. v. Dep't of Defense*, 14-1064 (JDB), 2017 WL 1214424 (D.D.C. Mar. 30, 2017).
(Email)

  Where Plaintiff sought sanctions for a government agency's failure to preserve and produce emails in response to a Touhy request (an APA action was eventually filed), court denied Plaintiff's request to depose the Agency's attorneys as a way to "replace" the lost information (thus, according to Plaintiff, avoiding further analysis under Rule

37(e)), reasoning that the rule's Committee Notes appeared to "contemplate that the 'replacement' of lost information would come from another electronic source," and declined to impose the requested sanction under any authority (either Rule 37(e) or the court's inherent authority) where Plaintiff's requested sanction was not appropriately targeted to the harm claimed and where no prejudice was established. [KLG]

- *Edelson v Cheung*, No. 2:13-cv-5870 (JLL)(JAD), 2017 WL 150241 (D.N.J. Jan. 12, 2017).
(Email)

  Where Plaintiff sought spoliation sanctions for Defendant's deletion of emails and argued that Defendant intended to keep the at-issue account hidden and deleted emails after it was discovered through another party's production and that those emails revealed Defendant's intent to keep the at-issue account hidden and other elements of Plaintiff's claims, the court found that the deletions were "intended to deprive Plaintiff of the information" contained within and reasoned that Defendant's claim that he deleted the emails because of computer performance lacked credibility, but declined to impose default judgment absent a sufficient degree of prejudice and instead ordered that a permissive adverse inference instruction would be given to the jury. [KLG]

- *Omnigen Research v. Wang*, No. 6:16-cv-00268-MC, 2017 WL 2260071 (D. Or. May 23, 2017).
(Email, metadata, other ESI)

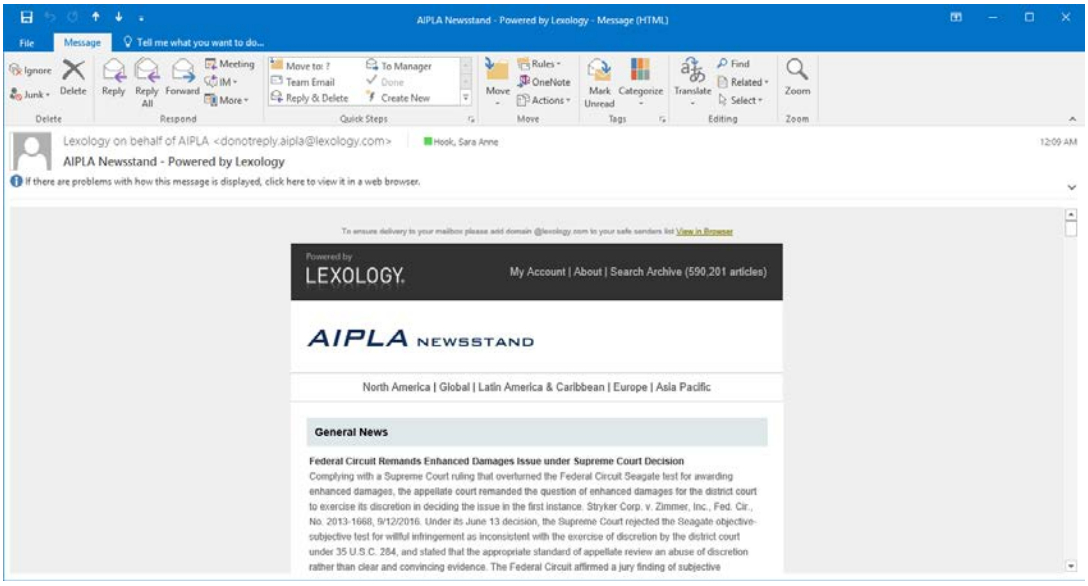
  For egregious intentional spoliation of ESI, including deletion of emails and metadata and donating a relevant computer to charity despite repeated requests for preservation, a preliminary injunction and court orders to produce ESI, the court imposed default judgment pursuant to FRCP 37(b)(2), FRCP 37(e) and the court's inherent authority. [KLG]

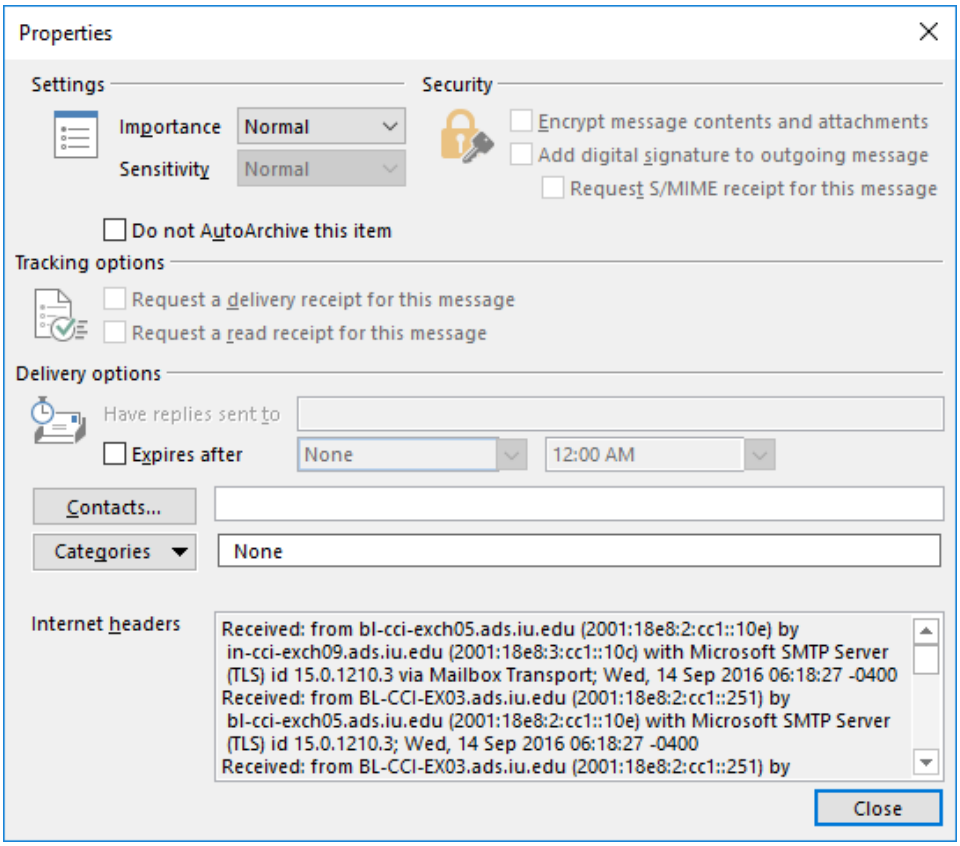
- *Snider v. Danfoss*, LLC, 15 CV 4748, 2017 WL 2973464 (N.D. Ill. July 12, 2017).
(Email)

  In this case, the court addressed Plaintiff's request for sanctions for Defendant's failure to preserve emails and, concluding the information did "not appear to be relevant" and that Plaintiff was not prejudiced, denied Plaintiff's motion for sanctions. [KLG]

- *See also Cohn v. Guaranteed Rate, Inc.*, No. 1:14-cv-9369, 2016 WL 7157358 (N.D. Ill. Dec 8, 2016), *supra*, Section B.
(Emails - Gmail, but also LinkedIn)

- *See also* Dave Stafford, *Krieg DeVault Seeks Private Emails of Ex-Partners Who Sued for Owed Compensation.* The Indiana Lawyer, Aug. 29. 2017. NOTE: Requesting private emails.


AIPLA Newsstand - Powered by Lexology - Message (HTML)
Lexology on behalf of AIPLA <donotreply.aipla@lexology.com>
AIPLA Newsstand - Powered by Lexology
If there are problems with how this message is displayed, click here to view it in a web browser.
LEXOLOGY.
My Account | About | Search Archive (590,201 articles)
AIPLA NEWSSTAND
North America | Global | Latin America & Caribbean | Europe | Asia Pacific
General News
Federal Circuit Remands Enhanced Damages Issue under Supreme Court Decision


Properties
Settings
Importance
Normal
Sensitivity
Normal
Do not AutoArchive this item
Security
Encrypt message contents and attachments
Add digital signature to outgoing message
Request S/MIME receipt for this message
Tracking options
Request a delivery receipt for this message
Request a read receipt for this message
Delivery options
Have replies sent to
Expires after
None
12:00 AM
Contacts...
Categories
None
Internet headers
Received: from bl-cci-exch05.ads.iu.edu (2001:18e8:2:cc1::10e) by
in-cci-exch09.ads.iu.edu (2001:18e8:3:cc1::10c) with Microsoft SMTP Server
(TLS) id 15.0.1210.3 via Mailbox Transport; Wed, 14 Sep 2016 06:18:27 -0400
Received: from BL-CCI-EX03.ads.iu.edu (2001:18e8:2:cc1::251) by
bl-cci-exch05.ads.iu.edu (2001:18e8:2:cc1::10e) with Microsoft SMTP Server
(TLS) id 15.0.1210.3; Wed, 14 Sep 2016 06:18:27 -0400
Received: from BL-CCI-EX03.ads.iu.edu (2001:18e8:2:cc1::251) by
Close

D. Video Surveillance (Private and Public)

- *Abdulahi v. Wal-Mart Stores E., L.P.*, 76 F. Supp. 3d 1393 (N.D. Ga. Dec. 2014).
(Video surveillance footage)

  Where plaintiff was fired for failure to lock a gate—which he disputed—during the pendency of separate EEOC investigations into plaintiff's charges of discrimination and where the at-issue manager claimed to have viewed footage confirming the gate was unlocked but failed to preserve it, the court determined that Defendant was under a duty to preserve ("due to an ongoing EEOC investigation during the applicable time period, Wal-Mart's own investigation into the alleged employee misconduct including a review of the video footage, and litigation being reasonably foreseeable"), that plaintiff was prejudiced by the loss because neither the at-issue manager's testimony or emails were equivalents for the video, and that plaintiff showed "more than mere negligence" in the destruction, the court ordered an adverse inference creating a presumption that "Wal-Mart's stated reason for terminating Plaintiff was pre-textual and that retaliation was the but-for cause of Plaintiff's termination" and awarded attorney's fees. [KLG]

- *Ballard v. Williams*, No. 3:10-cv-01456, 2015 WL 179071 (M.D. Pa. Jan. 14, 2015).
(Surveillance video)

  Where surveillance footage of hallway in which alleged assault occurred was overwritten, the court reasoned there was no indication that the evidence was intentionally lost or destroyed, that the named defendants were not responsible for the video system, and that defendant was not "materially prejudiced" because he could still testify as to what happened and therefore denied the motion for sanctions. [KLG]

- *Bloom v. Toliver*, No. 12-CV-169-JED-FHM, 2015 WL 5344360 (N.D. Okla. Sept. 14, 2015).
(Video surveillance footage and call recording)

  Where prisoner alleged that he was attacked by another inmate and that corrections officers failed to properly respond, court found prison had a duty to preserve relevant surveillance footage and the recording of the involved-officer's phone call to his wife immediately following the incident and that the failure to do so resulted in prejudice; court ordered evidentiary sanctions for the loss of certain footage, but reserved a determination re: sanctions as to lost video of the aftermath of the attack and the officer's phone call. [KLG]

- *Amtrak v. Guy M. Turner, Inc.*, NO. 4:15-CV-68-BO, 2016 U.S. Dist. LEXIS 61073 (E.D.N.C. May 9, 2016).
(ESI, Discovery, Relevance, Video Data, Rule 26(b)(1))

  In this personal injury case, the plaintiffs brought a suit against the owner of a tractor-trailer after a non-fatal collision between a passenger train and the vehicle. The defendant moved to compel responses to twenty-eight discovery requests, including video footage

and locomotive data captured before the incident. The plaintiffs, citing FRCP 26(b)(1), argued that the relevant materials had already been provided, and that these requests were overly broad and irrelevant. The court joined the widely held view that the 2015 FRCP amendments encouraged courts to take an active role in the discovery process, by considering each request in turn and weighing it for relevancy. The court then granted parts of the defendant's motion for the additional video and locomotive data. The court noted that while the defendant articulated why the requested information was relevant, the plaintiff "has failed to demonstrate grounds on which to deny the request." [KO]

- *Brown v. Albertsons, LLC*, 2:16-cv-01991-JAD-PAL, 2017 WL 1957571 (D. Nev. May 10, 2017).
(ESI, including *video*)

  In response to Plaintiff's Motion for Spoliation Sanctions, the Court engaged in an analysis of four types of available sanctions: Evidentiary, Monetary, Dispositive and Adverse Inference Instructions. The Plaintiff argued the Defendant intentionally destroyed evidence in the form of an incident report, a surveillance video and correspondence between Defendant and a third-party claims adjuster. The Court found that information from the incident report and the lost emails with the claims adjuster were available elsewhere and that the loss of the video surveillance was due to a system-wide outage that affected several stores. The Court found no evidence that Defendant acted intentionally or recklessly and denied Plaintiff's request for Dispositive Sanctions but instead imposed lesser Evidentiary Sanctions by allowing the Plaintiff to introduce evidence that the incident report was lost or destroyed, that the Defendant failed to preserve the third-party communications and that Defendant's video system failed to record the incident. [KLG]

- *Patrick v. Tractor Supply, Co.*, No. 16-10755, 2017 WL 396301 (E.D. La. Jan. 30, 2017).
(Video surveillance footage)

  Where Defendant had a duty to preserve evidence relevant to the litigation and the video in question was found to be relevant, court indicated the "thrust" of its analysis would focus on whether the destruction occurred in bad faith and reasoned that Plaintiff's request for preservation of "all video footage of the incident" did not indicate a request for footage of the surrounding area, thus allowing the destruction of the video prior to filing of the lawsuit, and that the failure to retain the footage was "not the result of a directed action to delete the information but rather a failure to stop the automatic deletion" which "at best amounts to negligence and does not rise to the level of bad faith" and denied Plaintiff's motion for sanctions but indicated that the parties would be allowed to "admit evidence of these issues during trial." [KLG]

- *Storey v. Effingham Cnty.*, No. CV 415-149, 2017 WL 2623775 (S.D. Ga. June 16, 2017).
(Surveillance footage from jail)

For Defendants' negligent (or even reckless) failure to preserve relevant video footage following Plaintiff's release from jail despite the "distinct possibility" of litigation in light of the injuries Plaintiff suffered while in custody and his specific threats to sue, the court imposed sanctions to redress the prejudice to Plaintiff and ordered that the court would tell the jury that the video was not preserved and that the parties could present evidence and argument regarding that failure for the jury's consideration. [KLG]

- *Houston v. Coveny*, No. 14-cv-6609, 2017 WL 972124 (W.D.N.Y. Mar. 13, 2017).
(Audio and video recordings)

  Court granted motion for preservation order as to relevant audio and video recordings reasoning that a court "may grant a preservation order if a party can demonstrate that the evidence is in some danger of being destroyed absent court intervention" and that in light of the Department of Corrections and Community Supervision retention policy such an order was appropriate to ensure preservation through the pendency of the case. [KLG]

- *Charles v. City of New York*, No. 12-CV-6180 (SLT)(SMG), 2017 WL 530460 (E.D.N.Y., Feb. 8, 2017).
(Lost phone containing video footage of incident leading to arrest – NOTE: personal device)

  Where Plaintiff lost the phone containing relevant video footage of the incident leading to plaintiff's arrest when she attended a "gala" carrying a "really small purse" and thus had to hand-carry or lay down her phone and where she failed to call the banquet hall to determine if her phone was recovered (although she apparently did call her phone's service provider and a relevant cab company in furtherance of her recovery efforts), the court declined to find that the loss was intentional and reasoned that the evidence suggested "at most mere negligence" and that because there was a "genuine issue of material fact regarding what transpired during the videotaping, the court [could] not find that the lost videotape was likely to favor Defendants" and thus denied the motion for sanctions without prejudice to renewal at trial if "Defendants could adduce evidence … that the lost video recording was likely to be favorable to them"; notably, court applied common law spoliation analysis for loss of the phone, recognizing that the common law applied, "except in cases involving electronically stored information." [KLG]

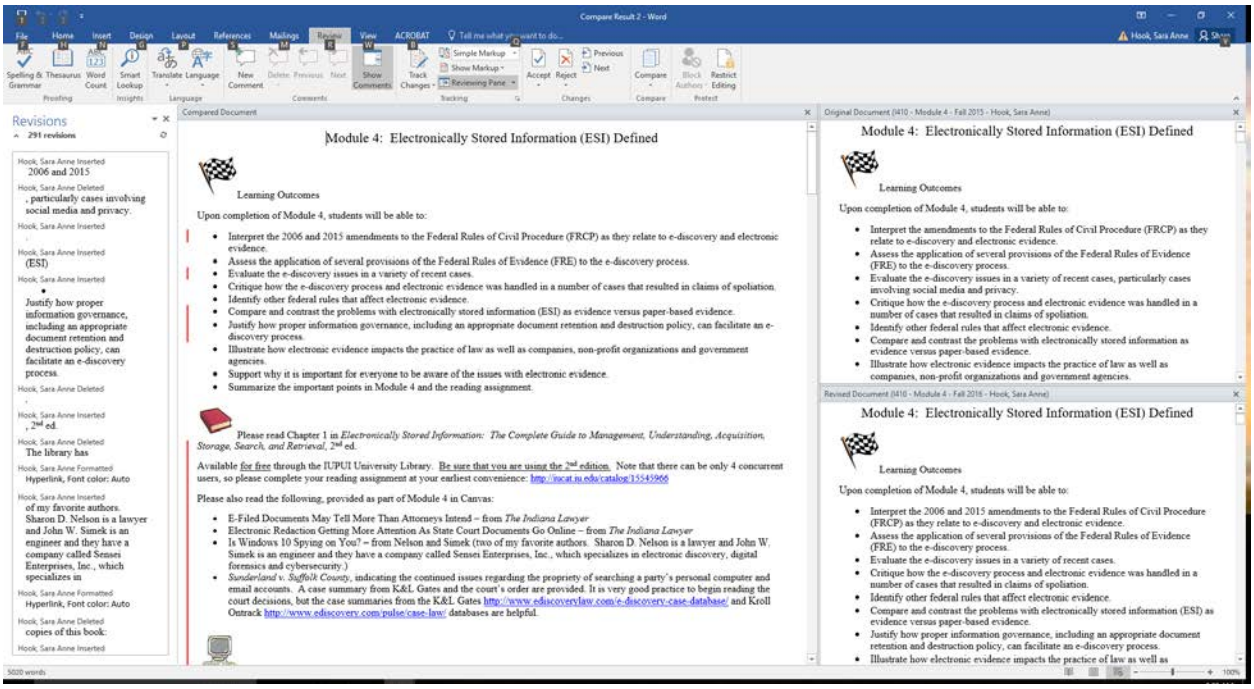
- *Harleysville Ins. Co. v. Holding Funeral Home, Inc.*, 2017 U.S. Dist. LEXIS 18714 (W.D. Va. Feb. 9, 2017).
(Video)

  In this arson insurance fraud claim, the plaintiff moved the court to disqualify the defendant's counsel for violating the attorney-client privilege and work-product doctrine. For the purpose of sharing information electronically, a senior investigator for the plaintiff's parent company uploaded surveillance video footage to a shared file site, and sent an email to the National Insurance Crime Bureau ("NICB"). The email contained a URL link to the video, along with a standard confidentiality disclosure. Several months later, the plaintiff uploaded all claim and investigation files to the same site, and sent the same URL link to plaintiff's counsel. The uploaded files were not password protected,

and the plaintiff later conceded that "any person who had access to the internet could have accessed the [site] simply by typing in the URL address in a web browser." In response to a subpoena, the NICB sent the defendant a copy of the email containing the link, which defense counsel accessed and downloaded. The defendant argued that the plaintiff waived its privilege by placing the information on a site with open access. Applying state law to the privilege doctrine, the court considered the "reasonableness of the precautions to prevent inadvertent disclosures," the "time taken to rectify the error" and the "extent of the disclosure," and found that the attorney-client privilege was waived. The court called the plaintiff's disclosure "vast", likening it to "the cyber world equivalent of leaving its claims file on a bench in the public square and telling its counsel where they could find it." Likewise, the court held that the plaintiff also waived work-product doctrine protection under Federal Rule of Evidence 502. The court reasoned that the plaintiff's disclosures were not inadvertent, as the action of posting the information online was not unintentional. Additionally, the plaintiff knew the information was not protected, and "did not take reasonable steps to prevent its disclosure or to rectify the situation." The court also advised that under public policy, it is the responsibility of businesses who choose to use evolving technology to know how to use it and to ensure confidential information cannot be accessed by anyone not entitled to view it. [KO]

E. Computerized Versions of Contracts and Other Documents

One of the major reasons to request all electronically stored information (ESI) is in native format with the metadata intact. As opposed to a paper-based world, where only the final, signed version of a contract or other document would likely be available, in the electronic world, a multiplicity of drafts and versions might exist, all of which could go to who was involved in the process of preparing a document, what changes were made and when and how much time was spent. The prevalence of using Track Changes, particularly with contracts, means that there will be a long list of revisions revealing important facets of a dispute, such as intent, chronology of events and timing, parties participating, etc. It is very easy to compare various versions of a document side-by-side, including in Word using its Compare feature.




- *Columbia Valley Reg'l Med. Ctr. v. Bannert*, 112 S.W. 3d 193 (Tex. App. 2003). (Word document) – older case, but still interesting

  Reversing jury verdict of over $1.5 million in compensatory and punitive damages, court found evidence not legally sufficient to support finding that manager authored offending memorandum; computer experts testified regarding creation of memo, history of revisions and locations of copies. [KLG]

- *Iridex Corp. v. Synergetics, Inc.*, 2007 WL 781254 (E.D. Mo. Mar 12, 2007). (Email and draft expert reports)

Where defense expert witnesses testified that defense counsel prepared the first drafts of reports, and revisions and changes were often exchanged through email, and plaintiff contended that it could not tell whether all drafts were produced, nor could it tell who created and/or revised each draft, court ordered defendant to produce copies of all drafts of all expert opinions, together with all communications between defendant's employees or counsel and expert witnesses regarding the drafts; court further ordered defendant to provide a declaration of counsel confirming full production and explaining the chronology of the revisions and the author of each set of revisions; declaration would be binding on defendant and could be used for cross-examination of expert witnesses. [KLG]

- *E.E.O.C. v. Forge Ind. Staffing, Inc.*, No. 1:14-mc-00090-SEB-MJD, 2014 WL 6673574 (S.D. Ind. Nov. 24, 2014). – NOTE: Indiana case.
(Versions of employment application form used by staffing agency between January 1, 2012 and May 31, 2014, including all pages of and revisions to each form)

  Where former employee filed claim with EEOC alleging sexual harassment and retaliation, and EEOC issued a subpoena to employer staffing agency seeking information to determine how long the staffing agency had required applicants to waive statutorily protected statutes of limitations, court declined to enforce the subpoena, finding that the EEOC's subpoena exceeded its authority in that the information sought went beyond the issues arising out of former employee's individual charge; court further determined that the burden imposed on the staffing agency far exceeded the minimal relevance of the evidence sought, given that staffing agency processed 130,000 temporary employee applications during the time period covered by the subpoena, applications were not kept in a central repository or electronically, and compliance would require manual review of each employment application maintained in paper format at each of its ten office locations and would disrupt agency's day-to-day operations. [KLG]

F. Text Messages and Voicemail (*see also* Section I, *infra*)

- *Bailey v. Scoutware, LLC*, No. 12-10281, 2014 WL 1118372 (E.D. Mich. Mar. 21, 2014). (Text messages and voicemail messages on cell phone of plaintiff's former co-worker).

  Because defendant was able to examine the subject cell phone with its expert, court ruled that plaintiff should also have the ability to examine the phone to determine if additional relevant text or voicemail messages exist or if there is evidence that text or voicemail messages were deleted, and ordered defendant to produce the current and old cell phones to plaintiff's expert; court deferred ruling on other requested sanctions as premature and found that neither side was entitled to attorneys' fees in connection with the motion. [KLG]

- *Cochran v. Caldera Med., Inc.*, No. 12-5109, 2014 WL 1608664 (E.D. Pa. Apr. 22, 2014). (ESI, text messages, voicemail messages)

  In case where defendant represented that it was currently defending approximately 1,709 claims nationwide involving its various products, and that it had limited financial resources, court denied defendant's request that plaintiffs share in the cost of producing documents and ESI as defendant did not demonstrate that ESI sought by plaintiffs was inaccessible; court further noted that, given the importance of the discovery requests to plaintiffs' ability to prove their claims, and the seriousness of the injuries alleged by plaintiffs, the burden or expense of the discovery requests was outweighed by the likely benefit to plaintiffs. [KLG]

- *Superior Performers Inc. v. Meaike*, No. 1:13CV1149, 2015 WL 471429 (M.D.N.C. Feb. 4, 2015).
  (Voicemail)

  Where Plaintiff's agent deleted an original voicemail from his phone by way of a factory reset but had produced a copy and also claimed to have transferred the voicemail to his new phone and where Defendants sought sanctions and argued that the deletion would prevent them from showing the voicemail was fabricated, as they suspected, the court declined to impose sanctions for the alleged fabrication, despite evidence the presentation of evidence that could lead to that conclusion, but did order that Plaintiff be prevented from using the voicemail at trial as a sanction for spoliation, reasoning that although the voicemail was not on one of Plaintiff's phones (but rather on its agent's), it "likely" had a duty to preserve the evidence and that Plaintiff did not attempt to provide access to the phone or provide notice of the voicemail's possible destruction. [KLG]

- *Nuvasive v. Madsen Med.*, 2016 WL 305096 (S.D. Cal. Jan. 26, 2016).
  (Fed. R. Civ. P. 37(e), text messages, spoliation, sanctions, adverse inferences)

  In this case, the court granted the plaintiff's motion to vacate a prior order that imposed an adverse inference for the plaintiff's failure to preserve text messages. Prior to the 2015 amendments to the Federal Rules of Civil Procedure, the court had granted the defendant's motion for sanctions against the plaintiff for spoliation of evidence. Citing the recent amendments to Fed. R. Civ. P. 37(e), the plaintiff argued that that the rule now

permits an adverse inference for failure to preserve ESI "only upon the finding that the [spoliating] party acted with the intent to deprive another party of the information's use in the litigation." Citing the new rule, the court agreed that it would be improper to give the adverse instruction given that there was no evidence to suggest that the failure to preserve was intentional. The court also addressed the timing of the amended rules in context of the case, stating that "[g]enerally a new procedural rule applies to the uncompleted portions of suits pending when the rule became effective." Since the trial had not yet taken place and the court had not given the adverse inference, the court concluded that the "new rule applies to the trial proceedings." [KO]

- For another case on voicemail, s*ee Margolis v. Dial Corp.*, *infra*.
  (Voicemail, instant messages, backup tapes)

- *See also Zamora v. Stellar Mgmt. Grp., Inc.*, 3:16-05028-CV-RK, 2017 WL 1362688 (W.D. Mo., Mar. 11, 2017), *supra*, Section B.
  (ESI from cellular phones, Facebook)

- *Montgomery v. Iron Rooster-Annapolis*, 2017 U.S. Dist. LEXIS 71338 (D. Md. May 9, 2017).
  (Text messages)

  In this case, the plaintiff alleged that her rights under the Fair Labor Standards Act and the Maryland Wage and Hour Law were violated when working for the defendants' restaurant. The defendants contend that the plaintiff was exempt for a large part of her employment due to the managerial nature of her position. During the time the defendants' claim the plaintiff was exempt, the plaintiff used an HTC cell phone from Verizon. The defendants believed the phone contained text messages between her and other employees, which would show she was acting as a manager, as well as text messages to her former supervisor who brought a similar claim against the restaurant. The plaintiff claimed that she began having problems with her phone around August 15, 2016 and brought the phone into the Verizon store. The plaintiff opted to participate in a trade-in program in which she would receive $200 for returning her phone to Verizon when a shipping box arrived. The shipping box took longer than expected to arrive, the plaintiff ultimately shipped the phone back at some point in September 2016, and the account was credited with the $200 on October 4, 2016. Both parties agree that the plaintiff was on notice of litigation as early as May 4, 2016 and on June 23, 2016 the plaintiff, through counsel, threatened the defendants with criminal action and requested they preserve all electronic information. The defendants filed a motion to compel sanctions, citing FRCP 37(e), for the plaintiff's failure to preserve the cell phone data. The magistrate judge found that there was no intent behind the plaintiff's failure to preserve the ESI and noted the defendant's counsel had yet to try to retrieve the sought after ESI from other employees. As a result, the magistrate judge recommended that jury instructions be provided that there was a duty to maintain the ESI on the HTC cell phone and that there should be consideration of whether the defendants can prove the phone contained text messages during the relevant time period and whether there is any evidence that proves text messages on the HTC phone would be favorable to the defendants. [KO]

- *Tingle v. Hebert*, 2017 U.S. Dist. LEXIS 88936 (M.D. La. June 8, 2017).
  (Email, text messages, personal cell phone and employer-issued cell phone)

  In this wrongful termination case, the defendant brought a motion to compel, requesting that the plaintiff produce email and text messages sent or received on his personal cell phone and through his personal email accounts, as well as information that the plaintiff deleted from his employer-issued cell phone prior to returning it to his employer. The court found that while the defendant's requests for "all text messages" and "all e-mail messages" were not proportional to the needs to the case, communications on the plaintiff's personal cell phone were potentially relevant in this case. As such, the court limited the scope of discovery on the plaintiff's personal phone and email accounts to the pertinent time period giving rise to the issues in this case, protecting confidential information via a protective order. Additionally, the court found that the defendant's requests for deleted information on the plaintiff's company issued phone appeared to be a "fishing expedition". The court pointed to the plaintiff's deposition where he stated that he deleted private information from the company phone such as communication between family members and banking information. The plaintiff stated that he did not delete any communications between himself and former co-workers. As such, the court found that the defendant's requests for deleted data would produce irrelevant information. However, the court did order the production of communications deleted by the plaintiff on his employer-issued cell phone that were exchanged with former co-workers during the pertinent time period and referencing the issues in the case. [KO]

G. Chats and Instant Messages

- *Ballai v. Kiewit Power Constructors, Co.*, No. 110166, 2015 WL 423795 (Kan. Ct. App. Jan. 23, 2015).
  (Laptop; chat log)

  Court of Appeals of Kansas found no abuse of discretion by the district court for failing to order sanctions related to the recycling of the laptop computer used by appellant during his employment, as the district court did not issue an order to preserve and there is no statutory or common-law duty to preserve evidence in Kansas; court further found no abuse of discretion by the district court for excluding evidence of recycling the computer; court also found that a chat log was relevant, material, and probative and the appellant was protected from prejudice because the district court only allowed the redacted version of the chat log into evidence. [KLG]

- *United States v. Shah*, No. 5:13-CR-328-FL, 2015 WL 3605077 (E.D.N.C. June 5, 2015).
  (Gmail emails and chats)

  Court declined to find that contents of email and chats from gmail account could be authenticated as Google's business records pursuant to ER 902(11) where the contents of the emails were automatically copied to and maintained upon Google's servers finding that the "knowledge" requirement was not satisfied and reasoning: "Neither SHAHNN28@GMAIL.COM, nor any other originating source whose statements appear in the records produced by Google were under a "business duty" to convey accurate information in their correspondence. Because the proffered "finished product" is not the collective effort of "business insiders," who share a duty to ensure the accuracy of their statements, the court cannot allow those statements to be authenticated on the theory that they are Google's self-proving business records under Federal Rules of Evidence 803(6) and 902(11)." [KLG]

- *Day v. LSI Corp*., No. CIV 11-186-TUC-CKJ, 2012 WL 6674434 (D. Ariz. Dec. 20, 2012).
  (Emails, instant messages, miscellaneous ESI)

  Where plaintiff sought sanctions for spoliation, including the loss of documents belonging to a particularly relevant custodian, the court focused in particular on the failures of General Counsel (who the court found "knew or should have known" that the custodian's documents were relevant to the action and thus "at least acted willfully" in failing to preserve) and defendant's failure to follow its own document retention policies and granted partial default judgment as to one claim for which the risk of prejudice was "great" but awarded an adverse inference as to the other claims where the risk of prejudice was less and also awarded monetary sanctions. [KLG]

- *Doe v. City of San Diego*, No. 12-cv-0689-MMA (DHB), 2013 WL 2338713 (S.D. Cal. May 28, 2013).
  (Cellular phone records, including content)

Court found plaintiff had standing to challenge city's subpoena to Verizon Wireless seeking "any and all records" for Plaintiff's cellular phone, including texts, instant messages, etc. and found that Verizon was prohibited from disclosing such content by the Federal Stored Communications Act; Verizon was also prohibited from disclosing non-content records where such disclosure to a "governmental agency" is prohibited; court noted that alternative methods for discovery were available and specifically noted the availability of a Rule 34 request for production. [KLG]

- *Lakes Gas Co. v. Clark Oil Trading Co*., 875 F. Supp. 2d 1289 (D. Kan. June 21, 2012).
(Email and/or instant messages)

  In a brief discussion of spoliation, the court denied defendant's motion for sanctions where, despite the fact that it "seemed clear that there was some loss of evidence … in the form of email and/or 'instant messages' … at a time [Plaintiff] knew litigation was imminent," the evidence suggested that the loss was inadvertent, there was no claim of bad faith or evidence to support such a finding, defendant's claims of prejudice were largely speculative and defendant did not aggressively pursue the issue of spoliation; court's analysis stated that "in these circumstances" (referencing apparent inadvertence of the loss and lack of a claim of bad faith), "the court looks to the culpability of those involved and the relevance of the proof to the issues at hand". [KLG]

- *Margolis v. Dial Corp*., No. 12-CV-0288-JLS (WVG), 2012 WL 2588704 (S.D. Cal. July 3, 2012).
(Voicemail, instant messages, backup tapes)

  Court denied Plaintiffs' request for a preservation order as to voicemail and instant messages where defendants had already sent litigation hold notices requiring preservation such that Plaintiffs' request was moot; Court further declined to enter preservation order as to backup tapes where defendants established that their preservation would impose a significant burden and that the contents were likely duplicative and where the court found that the backup tapes did not fall within the exception identified in Zubulake v UBS Warburg, 220 FRD 212 (S.D.N.Y. 2003). [KLG]

H. YouTube and Vine

- *Teller v. Dogge*, No. 2:12-cv-00591-JCM-GWF, 2013 WL 5655984 (D. Nev. Oct. 16, 2013).
  (Videos defendant posted to YouTube, instructional DVD and manual)

  Where defendant failed to produce subject videos or make his hard drive available for mirror imaging as required by court's order, but plaintiff ultimately obtained the subject videos from Google, court denied plaintiff's request for case-dispositive sanctions but would impose an adverse inference instruction in the form of a mandatory presumption in light of multiple warnings to defendant that sanctions would result if he did not produce the information and in light of other "violative and unmannered conduct" of defendant in the litigation. [KLG]

- *People v. Torres*, No. E052071, 2012 WL 1205808 (Cal. Ct. App. Apr. 11, 2012).
  (YouTube video)

  Trial court did not abuse its discretion in permitting prosecution to show a YouTube video where, although officer testified "he did not know when the video was made or who produced it" he testified that the video was an accurate depiction of what it looked like on YouTube such that the trial court "could conclude that the video would assist jurors in determining the facts of the case and motivation for the crimes" and where the court determined that the issues of when and who produced the video spoke to issues of reliability and weight and that the images on the video (picture of the alleged victim with an "x" over his face, for example) coupled with evidence linking defendant to the crime of attempted murder "sufficiently link[ed] the video with the defendant". [KLG]

Vine is described as "[t]he entertainment network where videos and personalities get really big, really fast. Download Vine to watch videos, remixes and trends before they blow up." Vine's website includes its Terms of Service at https://vine.co/terms, its privacy policy at https://vine.co/privacy and its rules at https://vine.co/rules. The status of Vine has evolved in the past year. See Vine (service), Wikipedia, https://en.wikipedia.org/wiki/Vine_(service), accessed 9/29/17.

I.Instagram, Pinterest, Snapchat and WhatsApp

- For a case about Instagram, s*ee Keller v. National Farmers Union Property & Cas. Co.*, *supra*).
  (Motion to compel, production, social networking, social network, expectation of privacy)

- *Moulton v. Bane*, No. 14-cv-265-JD, 2015 WL 7776892 (S.D.N.H. Dec. 2, 2015).
  (Text messages (WhatsApp))

  Where Defendant unintentionally lost text messages when his service provider failed to transfer those text messages to his new phone—despite his request to transfer "everything"—and where the texts were later recovered by a forensic analysist, court declined to impose "punitive sanctions" and ordered Defendant to pay the cost of retrieving the messages. [KLG]

- For a thorough review of the electronic discovery issues with Snapchat, WhatsApp and other mobile messaging services, *see* Cori Faklaris & Sara Anne Hook, Oh, Snap! The State of Electronic Discovery Amid the Rise of Snapchat, WhatsApp, Kik, and Other Mobile Messaging Apps, *The Federal Lawyer*, May 2016, pp. 64-75.

- *Roof v. Newcastle Pub. Sch.*, 2016 U.S. Dist. LEXIS 14886 (W.D. Okla., Feb. 8, 2016).
  (Snapchat)

  "Plaintiff's asserts that, during the time Feroli was employed as a teacher by the District, he engaged in an inappropriate romantic relationship with A.S., plaintiff's minor daughter who was then a high school senior. Plaintiff describes the relationship as beginning with "snap chatting" and Facetime exchanges, including ones where Feroli would allegedly forward pictures to A.S. of himself disrobed and exposing his genitals. Plaintiff's evidence is that the relationship progressed to instances of kissing and petting in Feroli's classroom when the two were alone." [*Id.* at 2.]

- *See also U.S. v. Gaston* (Instagram), *supra*.

J. Wearable Devices and the Internet of Things

- For information on the Internet of Things as a source of evidence, *see* Sharon D. Nelson & John W. Simek, *The Internet of Everything: What It Means for Lawyers*, Sensei Enterprises, Inc., 2014, https://senseient.com/articles/the-internet-of-everything-what-it-means-for-lawyers/, accessed 9/29/17.

- For information on fitness trackers and wearable devices as sources of evidence, *see* Marilyn Odehdahl, *Fitness Trackers Add to Flood of Digital Evidence in Court*. The Indiana Lawyer, Aug. 10, 2016.

- Vishakha Kumari & Sara Anne Hook, *The Privacy, Security and Discoverability of Data on Wearable Health Devices: Fitness or Folly?* HCI International 2017, Vancouver, Canada, July 12, 2017, https://scholarworks.iupui.edu/handle/1805/13462, accessed 9/29/17.

- *See* Marc Salzman, *So You've Split From Your Fitness Tracker: Can You Get Your Data Back?* USA Today, Aug. 6, 2017.

- *See* Antigone Peyton, *A Litigator's Guide to the Internet of Things*. 22. Rich. J.L. & Tech. 9 (Mar. 30, 2016).

- Nicola Fabiano, *The Internet of Things and the Legal Issues Related to the Data Protection Law According to the New European General Data Protection Regulation*. Athens Journal of Law, July 2017, at 201.

K. Even Celebrities Have Issues with E-Discovery – and Issues with New Technology

- Scott Collins, *Deleted Recording Amplifies 'Bad Blood' Between Pop Icon, Disc Jockey*. The Indiana Lawyer, Oct. 4, 2017. (*Mueller v. Swift*, 2017 U.S. Dist. LEXIS 112276 (D. Colo. July 19, 2017)).

- The Duty to Preserve Extends to 3rd Parties and Their Texts (*Ronnie Van Zant, Inc. v. Artemis Pyle* (S.D.N.Y. Aug. 28, 2017)) – see Exterro case summary, https://www.exterro.com/case-law-library/new-data-types/ronnie-van-zant-v-artemis-pyle/, accessed 10/13/17.

- Boston Red Sox Caught Using Apple Watches to Steal Signals from Yankees During Games – see Exterro case summary, https://www.exterro.com/blog/boston-red-sox-using-apple-watches-to-steal-signals-from-yankees/, accessed 10/13/17.

- Text Messages MUST Be Accounted for in E-Discovery – see Exterro case summary, https://www.exterro.com/blog/text-messages-must-be-accounted-for-in-e-discovery/, accessed 10/13/17.

- Emojis (emoticons) as evidence – see Next Witness: Will The Yellow Smiley Face Take The Stand? (NPR, Feb. 8, 2015, http://www.npr.org/2015/02/08/384662409/your-honor-id-like-to-call-the-smiley-face-to-the-stand, accessed 10/16/17). *See also* Mark Walsh, *Emoijis Head to a Courthouse Near You*. ABA Journal, Oct. 2017, at 11.

- Wendy N. Davis, *Face Time: Facial Recognition Technology Helps Nab Criminals – and Raises Privacy Concerns*. ABA Journal, Oct. 2017, at 16.