ACEDS | Detroit Chapter
ASSOCIATION OF CERTIFIED E-DISCOVERY SPECIALISTS

JUNE 2021

ACEDS DETROIT

Quarterly Newsletter
CO-EIC: Abby Melling
CO-EIC Denise Bach

WHATS INSIDE

- Events Schedule
- Case Law Summaries
- What to do if your business gets hacked
- Test your knowledge
- Comments from the Hon. Judge McCormack
- The difference between routine document destruction and spoilation
- The Trial Bubble is about to burst
- Blowing things out of proportion
- Resources
- Sponsors

Have something to share? Contact Abby Melling at abby.melling@conduent.com

MOVING FORWARD TOGETHER

Letter From The President
Jay Yelton

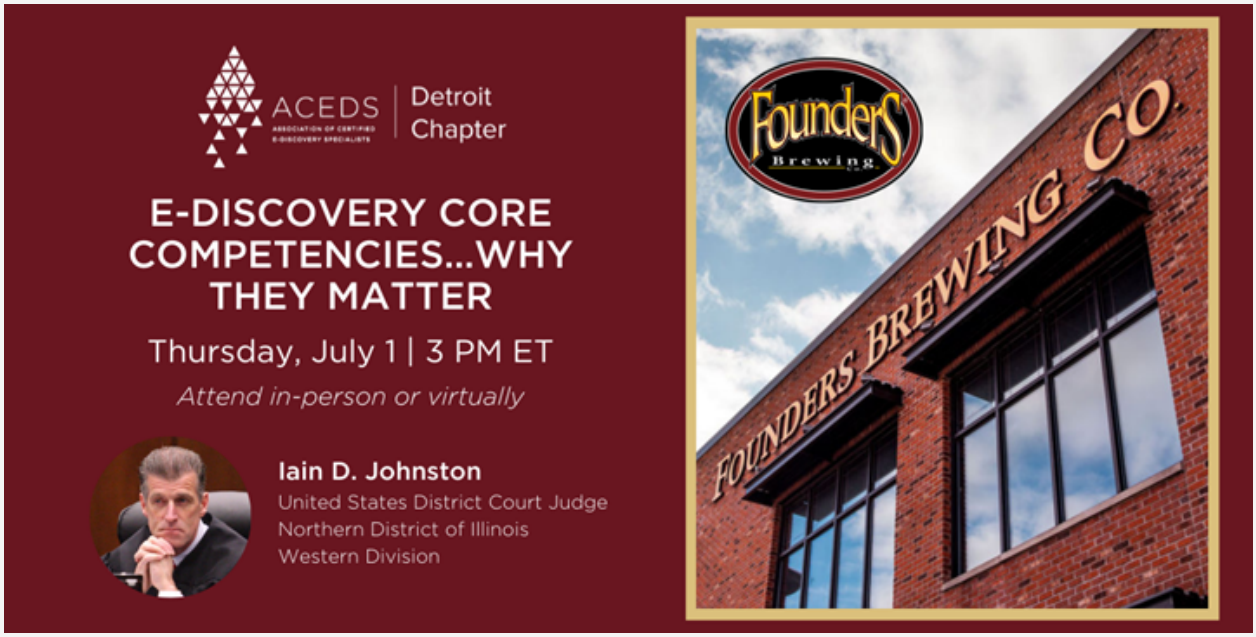
As we come to mid-year, my enthusiasm has significantly increased because it appears that we will be able to return to a somewhat normal means of collaborating, networking, sharing thoughts and coming together. We invite you to share our excitement and join us on July 1st as a kick-off to what the remainder of the year holds. On July 1st, starting at 3:00 pm EST at Founders Brewery in Grand Rapids we will have the privilege of welcoming and listening to the honorable Judge Iain Johnston (N.D. Illinois) regarding how federal judges value and expect us to understand and utilize eDiscovery best practices in all of our cases. Although we REALLY hope that you are able to join us in person for this event, it will also be offered remotely and via a recording. In preparation for that event, please read Judge Johnston's Memorandum Opinion and Order in DR Distributors, LLC v. Century Smoking, Inc, 12 CV 50324 (N.D. Ill. Jan. 19, 2021) and think of questions that you would like us to provide to Judge Johnston.

Most if not all of our Detroit Chapter Board members will be attending this event in person, so July 1st is also a great opportunity to provide us your feedback on what we are doing well and what we can do to improve as a local chapter. Also, if you have been considering whether and how to get more involved with our local chapter, please attend this next event and express your interest to any of the Board members. There are numerous and varied ways for you to get more involved and to get to know others in the eDiscovery community.

2021 Remaining Events Schedule

- **July 1st-Judge Johnston** details below
- **August 5th Webinar-**managing total costs of review; a step by step view-acorn
- **Sept Webinar-**hosted by Trustpoint-details to come!
- **Fall Wine and Cheese Social-**educational networking-date and location TBD
- **Holiday Party-**date and location TBD

Join ACEDS Detroit- July 1, 2021



special thanks to Phil Favro of Driven for making our April Event a great success!

PHIL FAVRO - ABOUT THE JULY 1ST EVENT

Consultant, IG and eDiscovery- Driven, Inc.

The Honorable Iain Johnston will be joining the ACEDS Detroit Chapter on July 1, 2021 for an engaging discussion of key electronic discovery issues of which lawyers and litigation support professionals should be aware. Judge Johnston addressed many of those issues earlier this year in DR Distributors v. 21 Century Smoking, Inc., ---F. Supp. 3d---, 2021 WL 185082 (N.D. Ill. Jan. 19, 2021), a 256-page sanctions order that specifically reproved defendants and their counsel for failing to take even the most basic steps to preserve relevant information.

While Judge Johnston will not mention any aspect of DR Distributors as it remains an active case, he will likely discuss key eDiscovery principles that impact nearly every lawsuit in 2021. Many of those principles were featured during the ACEDS webinar discussion I moderated on April 15, 2021 and include (among others) the following:

1.The nature of an attorney's legal and ethical duties to supervise the discovery process;
2.The importance of custodian interviews (and who can or should conduct them);
3.Risks and best practices regarding client self-collection;
4.Memorializing discovery compliance efforts; and
5.Leveraging experts, service providers, and vendors as necessary to assist with discovery compliance.

That these issues are significant should be self-evident. Nevertheless, since DR Distributors, several additional cases have issued that emphasize the need for clients and their counsel to be proficient in ESI basics and best practices.

For example, Magistrate Judge Katharine Parker recently held in Bersztein v. Best Buy, Inc., 20-cv-00076, 2021 WL 1961645 (S.D.N.Y. May 17, 2021) that defendants improperly failed to preserve "highly relevant" ESI that they should have been kept pursuant to a litigation hold and their own company policy. In Thomas v. Cricket Wireless, LLC, 3:19-cv-07270, ECF No. 241 (N.D. Cal. May 18, 2021), the court is presently investigating defendants' "document retention and discovery response practices" that have apparently resulted in the spoliation of relevant documents from various custodians. And in Torgersen v. Siemens Building Technology, Inc., No. 19-cv-4975, 2021 WL 2072151 (N.D. Ill. May 24, 2021) the court issued a mandatory adverse inference instruction pursuant to Federal Rule of Civil Procedure 37(e)(2) against plaintiff for intentionally deleting his Facebook page, which contained relevant information.

Bersztein, Thomas, and Torgersen confirm that the preservation and production failings which permeated DR Distributors are not isolated shortcomings. As Judge Johnston has emphasized, lawyers and legal support professionals must work with clients to take charge of the discovery process to ensure relevant information is safely accounted for in litigation.

Summaries of Recent eDiscovery Cases
By Ken Treece and Jay Yelton

Sanctions Over Loss of Audio Recordings and Interview Notes
Root v. Montana Dep't of Corrections, 2021 WL 1597922 (D. Mont. Apr. 23, 2021)
Plaintiff brought suit alleging retaliation by his employer in its employment decisions concerning its denial of his applications for an open lieutenant position. Plaintiff filed a report against his supervisor for improper behavior with a female inmate. Based on his supervisor's reaction to his complaint, plaintiff filed a union grievance, which was investigated. The investigation included recorded interviews with key personnel. After the investigation, plaintiff twice applied for and was twice denied a promotion to lieutenant. Handwritten notes were taken during the course of each interview.

During the course of discovery, plaintiff requested that the recorded interviews taken during the investigation of his union grievance and the interview notes from his two applications for the lieutenant position be produced. Defendants produced the interview notes from his first application, but not the investigator's recorded interviews or the interview notes from his second application. Defendants were unable to locate the recorded interviews and claimed the second set of interview notes were immediately shredded in accordance with HR policy. Plaintiff moved for spoliation sanctions, including an adverse inference instruction, pursuant to FRCP 37(e).

The court granted in part and denied in part the plaintiff's motion. The court found that plaintiff was prejudiced by the loss of the recorded interviews because "the audio recordings made during that investigation would likely have supplied probative evidence of what occurred, including providing context and tone to the witness statements. This type of contextual information cannot be restored or replaced through additional discovery." But, the court found no "intent to deprive" by defendants and limited the plaintiff to the presentation of evidence and argument concerning the lost audio recordings.

As for the interview notes from plaintiff's second application, the court denied the plaintiff's motion for sanctions. The plaintiff's second interview occurred after he filed suit. He did not amend his complaint to add any claim based on the second denial of promotion to lieutenant. Since plaintiff failed to put his second application at issue, the interview notes were not relevant to his case—although, the court did note that those interview notes should have been retained.

Default Judgment Sanctions for Pattern of Discovery Misconduct
Staubus v. Purdue Pharma, Case No. C-41916 (Tenn. Cir. Ct. Apr. 6, 2021)
Plaintiffs filed suit against numerous drug manufacturers for violation of the Tennessee Drug Dealer Liability Act for facilitating in the over-prescription and diversion of opioids resulting in injury to a baby while in utero. During the course of discovery, plaintiffs requested records related specifically to defendant Endo Pharmaceuticals operations and sales in Tennessee. However, Endo produced records only from higher level executives and none from its Tennessee operations or sales personnel.

Plaintiffs moved on multiple occasions for the production of Tennessee-specific records. Despite the court's order compelling Endo to do so, it did not identify any Tennessee-specific records. At the discovery-cutoff, and in response to the court's order to certify it had produced all responsive documents, Endo certified its compliance and stated it had conducted a "reasonable search," even though it had still not included Tennessee-specific custodians within its search.

Eventually, after the discovery cut-off and after having been held in contempt, Endo produced almost 400,000 Tennessee-specific records. Based on what the court identified as twelve false statements made to Plaintiff or to the Court by Endo concerning its document production, the court determined that the only appropriate sanction for Endo's discovery misconduct was a default judgment as it was "obvious that monetary sanctions [were] not sufficient. Endo and its attorneys have not shown any remorse, admitted their wrongdoing or apologized to opposing counsel or the Court for their actions."

Possible Sanctions for Deactivation of Facebook Account

Brown v. SSA Atlantic, LLC, 2021 WL 1015891 (S.D. Ga. Mar 16, 2021)

Plaintiff filed suit against defendant for injuries sustained in a vehicular collision involving one of defendant's drivers. In response to written discovery and at his deposition, plaintiff revealed the existence of one "deactivated" Facebook account. Despite stating in his written discovery responses that the account was deactivated before the litigation, he admitted at his deposition that the account was deactivated after he filed suit. Defendant later discovered other Facebook accounts under plaintiff's name. Plaintiff admitted that he had no more than three "burner" accounts.

Defendant moved that, based on the court's inherent power, plaintiff's complaint be stricken or, alternatively, an adverse inference jury instruction be given at trial as a sanction for plaintiff's spoliation. The court denied the defendant's request for sanctions. The court found that the deactivation of the accounts did not result in any loss of information. Hence, no spoliation sanctions were warranted. Instead, the court ordered that plaintiff produce data from his Facebook accounts for the relevant time period. In addition, the Court ordered plaintiff's counsel to show "substantial justification" for his certification under FRCP 26(g)(3) given the inaccuracy of the discovery responses concerning the plaintiff's multiple Facebook accounts.

Production of Personal Email in Company Dispute

Tradeshift, Inc. v. Buyerquest, Inc., 2021 WL 1586283 (N.D. Cal. Apr. 23, 2021)

Plaintiff brought a claim for tortious interference with contract against defendant, a subcontractor hired by plaintiff on a project for its client, Smucker. Plaintiff separately filed suit for interference against Smucker in New York. Plaintiff requested emails sent between defendant's CEO and a representative of Smucker using their personal email accounts in both actions. In the action against defendant, counsel permitted the CEO to search his own personal email account for responsive documents. He turned over one email. In the New York action, Smucker turned over two different emails—one from defendant's CEO that was highly disparaging of plaintiff and lobbying for the project to be turned over to defendant.

Given the paucity of emails produced, and the fact that defendant did not produce the highly probative email found in the New York action, plaintiff subpoenaed Google for a log of emails between CEO and Smucker's representative, including any deleted emails. Defendant moved to quash the subpoena on the grounds that it was duplicative and not proportional to the needs of the case. The court disagreed.

While acknowledging that the information sought by plaintiff from Google was duplicative of information sought from defendant, the court noted that the information was not duplicative of the information produced by defendant. The court also noted that defendant had no standing to object to any burden on Google—especially where Google was not itself complaining about the subpoena being burdensome. The court also ordered that defendant's counsel conduct a review of the CEO's personal email account in order to comply with its Rule 26(g)(1) obligation to certify the completeness of defendant's document production. The court found that "asking [the CEO] to search his own emails to see if he can find any wrongdoing he committed is ridiculous. No reasonable person could have any confidence in that process."

Compelled Production of Legal Hold Letters

Thomas v. Cricket Wireless, LLC, 2021 WL 1017114 (N.D. Cal. Mar. 16, 2021)

Plaintiffs filed a putative class action, alleging a fraudulent scheme by defendant to market and sell 4G/LTE devices/service plans to customers nationwide through false advertisements concerning the extent of its 4G/LTE coverage. A prior putative class action had been brought against defendant. That action was settled as to the two named plaintiffs prior to class certification. Upon dismissal after the settlement, defendant "discarded certain documents and data from the putative class period that plaintiffs believe would help substantiate their class allegations." Defendant claimed that it "'was entitled to stop preserving documents after [dismissal of the prior action" and "'[i]n any event, [it] has been transparent about what documents were not retained.'"

Plaintiff moved to compel the production of defendant's litigation hold letters in order to establish what records were subject to the hold and might no longer be available in discovery. Defendant objected, requesting that it be allowed to produce documents and 30(b)(6) representatives sufficient to establish what records fell under the hold letters. While the court did not agree with defendant's position concerning its preservation obligations after dismissal of the prior suit, the court did agree that it was generally accepted that production of litigation hold letters was not appropriate until there was some showing of necessity.

At the 30(b)(6) depositions, defendant repeatedly invoked the attorney-client privilege to prevent its witnesses from answering questions regarding records covered by the hold letters. And, in many instances, the witnesses had no knowledge regarding defendant's litigation hold instructions. Plaintiffs then renewed their motion to compel the production of defendant's litigation hold letters. Given that these depositions were necessitated by defendant's admission that it had destroyed potentially relevant records, the court granted plaintiffs' motion and ordered the production of defendant's litigation hold letters.

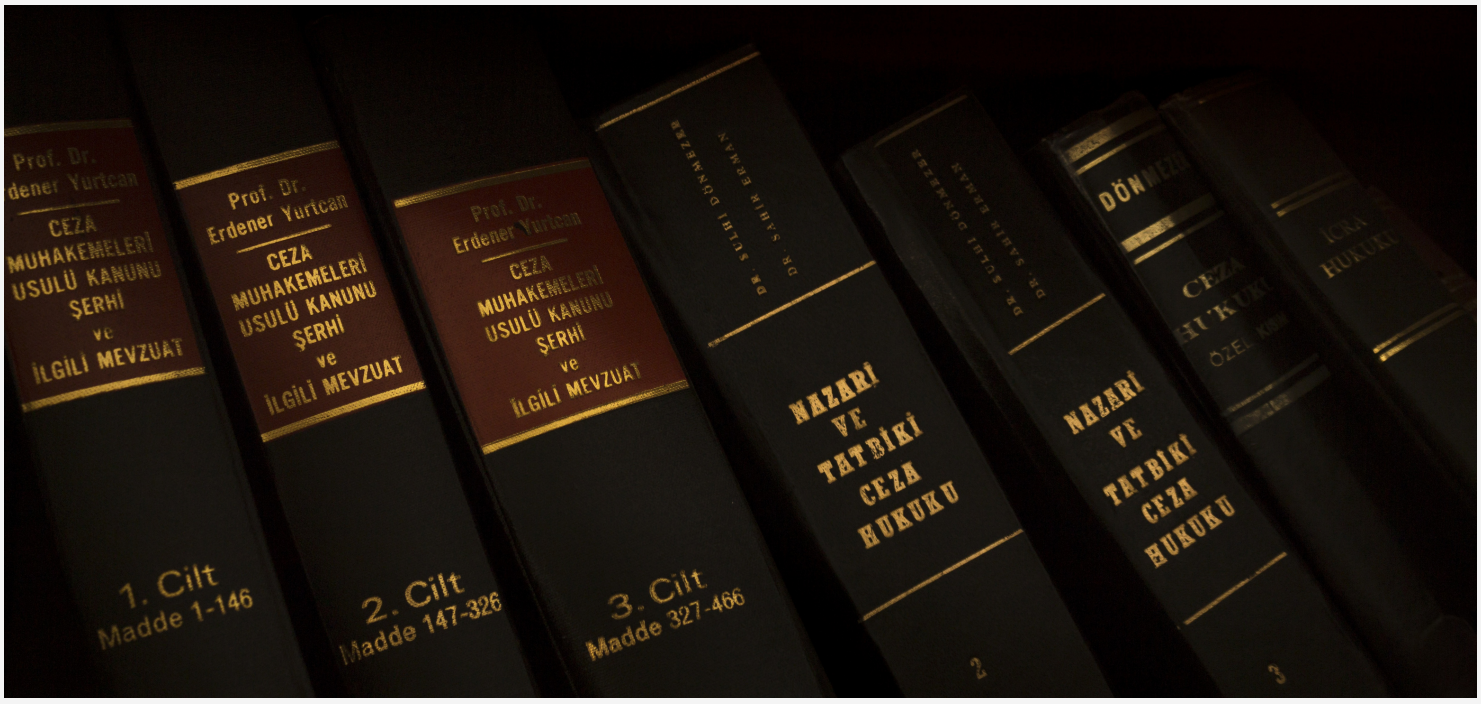
Discoverability of Slack Data

Benebone v. Pet Qwerks, 2021 WL 831025 (C.D. Cal. Feb. 18, 2021)

In this case involving claims over intellectual property, defendant learned during an early discussion regarding discovery that plaintiff used the Slack messaging platform as well as standard email for internal business communications. Defendant requested that plaintiff's Slack messages be included in a Stipulated ESI Order. However, plaintiff objected, citing that it had over thirty thousand Slack messages, making review and production of those messages disproportional to the needs of the case.

During a court-ordered meet and confer, plaintiff reiterated its view that Slack review and production would not be proportional to the needs of the case. Plaintiff estimated that it would cost between $110,000 to $225,000 to extract, process, review and produce responsive Slack messages. This estimate was provided by counsel with no expert opinion in support. Defendant disagreed, and the dispute over the Slack messages found its way before the court.

On defendant's motion to compel, defendant produced an expert declaration from an eDiscovery vendor. The expert stated that he had been involved in numerous suits involving production of Slack messages. He referred to a number of software tools that could be used to streamline the process. He also provided a cost estimate of approximately $22,000 to find and produce plaintiff's responsive Slack messages. The estimate included first level review by contract attorneys at an hourly rate of forty dollars. Plaintiff stood by its unsupported estimate, using an hourly rate of $400 for data review. The court noted that there was no dispute concerning the relevancy of the Slack messages as plaintiff used the platform for its internal business communications. As to the burden, the court noted that while it did not accept either estimate given at face value, it believed the actual cost would lean closer to defendant's estimate. The court concluded that "requiring review and production of Slack messages by [plaintiff] is generally comparable to requiring search and production of emails and is not unduly burdensome or disproportional to the needs of this case – if the requests and searches are appropriately limited and focused."



What to Do if Your Business Gets Hacked

By: Denise B. Bach, CEDS

The Data Breach - Ransomware Attack

The Beer Store is almost a century old, with an established date of 1927. It's one of the largest beer distributors in Canada, serving customers more than 800 beer brands, in over 450 retail stores, from 200 brewers around the world. And, as the business entered the second half of 2020, they were still struggling to respond to a data breach where hackers deployed ransomware on their corporate computer system **(1)**.

Some of The Beer Stores' retail locations were only accepting cash, and their online ordering system had been unavailable for several weeks. This came at a time when alcohol sales had seen a 500%+ increase due to governmental stay-at-home orders. It left brewery partners frustrated, customers and staff worried about handling cash, and experts puzzled about why it took so long to fix the problem. What can your business do to avoid this scenario?

Quick Action is Needed

After a potential data breach is identified, time is the enemy. A quick response can exponentially help organizations that have been placed in a compromised position. Here are the steps that a business should take to respond to a data breach:

1. Execute your organization's data breach response plan
2. If your business doesn't have an established data breach response plan, immediately contact an Incident Response expert

The first step isn't helpful if organizations are behind the eight ball and in the middle of a data breach. The best thing to do in this scenario is not to panic. It is crucial to develop a plan if a data breach occurs to strengthen your business proactively.

How to Create a Data Breach Plan

Establish a Data Breach Response Team

Assemble a group of stakeholders from across the business to help reduce the organization's risk. Identify the data breach response team and empower them to develop and execute a sound plan. The best place to start is to understand what a data breach response plan is and how to create one.

Train the Team

With a growing list of readily available resources, provide your team with training and tools to assemble the best plan for the organization. The legal and regulatory elements of a data breach response, including notification requirements to clients and vendors, need to be in the team's knowledge base. Training elements and resources should be recorded as evidence that the organization has acted in its best interest.

Clear Communication
A written data breach plan should be published and an open line of communication established between the response team.

Plan Ahead
Plan by having master service agreements in place with key vendors (breach response notification specialists, call centers, credit reporting agencies, etc.). It is a critical step to reducing frantic actions if an incident response is necessary. Indemnification language is essential to establish in advance and not during a data breach.

Practice
Practice doesn't make perfect; it makes permanent. Errors made during a breach response can be extremely costly, so conducting tabletop exercises twice a year on data breach scenarios is a good standard.

How to Get Ahead of a Data Breach

Have a Data Back-up Strategy
With more companies falling victim to ransomware attacks, paying the ransom to regain access to your data is not a viable strategy, especially since ransom demand amounts are steadily increasing (up 43% this year). A recent example is the nearly $5,000,000 ransom amount paid by Colonial Pipeline to obtain the encryption key from the attackers. There are other intangibles such as business interruption, reputation and litigation costs that also come into play after an attack. A major part of the planning process should include a data back-up strategy that allows companies the ability to avoid paying the ransom by deploying data back-ups to restore their environment.

Invest in Technology
Employing the right security technology is vital to help circumvent and attack. This includes endpoint security software to swiftly isolate the attack, the use of automated privacy controls, antivirus software, firewalls, email protection, anti-spam and software vulnerability testing.

Proactive Data Security Awareness Training
Companies are only as protected from a data breach as their weakest security-minded employee. Data security training educates employees on best practices that protect data from destruction, loss, modification, theft, or disclosure. Since data security can be compromised either by mistake or intentionally, information security training should focus both on accidental data mishandling and protection from malicious attempts.

The Time is Now

While Fortune 500 companies most likely have the internal knowledge base and headcount to develop comprehensive data breach plans, medium and small businesses don't always have the resources to do this independently. If your business hasn't made a plan to respond to a data breach, it's time to take the necessary steps before an incident occurs. Organizations that need help in establishing a data breach response or evaluating your current plan should contact an expert or a firm that deals with incident response.

Like with any other business contingency plan, thinking about and preparing for incidences before they happen are key. Producing a plan is attainable for businesses large and small. Leverage the wealth of resources available to mitigate the risk of when, not if, a data breach impacts your organization.

Denise B. Bach, CEDS is a Business Development Manager for 4Discovery, where she advises organizations and their counsel on issues relating to digital forensic investigations, collections, eDiscovery processing and Data Breach/Incident Response. Based in Michigan, Denise can be reached at Denise@4Discovery.com | www.4Discovery.com

(1) Rubin, Josh. "Hacked almost three weeks ago, The Beer Store can't track inventory and some outlets still only accept cash", TheStar.com, April, 2020

TEST YOUR E-DISCOVERY KNOWLEDGE

1. When does a party have a duty to supplement discovery responses?

- a. Only upon a timely request of the party who served the discovery requests.
- b. Immediately prior to the close of discovery.
- c. One month prior to the final pretrial conference or as otherwise ordered by the court.
- d. Only if the failure to do so would be a knowing concealment.
- e. Only if the party learns that in some material respect the response is incomplete or incorrect, and if the additional information has not otherwise been made known to the other parties during the discovery process or in writing.

2. When are parties required to hold an ESI (Electronically Stored Information) Conference?

- a. When one or more of the parties anticipate requesting or producing ESI during discovery.
- b. When one or more of the parties have concerns that relevant ESI has been or is likely to be deleted or destroyed.
- c. When the parties agree to hold such a conference.
- d. When the court orders the parties to hold such a conference.
- e. Never, because most cases don't involve ESI and such a conference would be a waste of time and money.

3.Under what circumstances should discovery disputes be subject to mediation?

- a. When the parties' efforts to meet and confer regarding discovery issues has failed due to a lack of communication and/or understanding of the issues.
- b. All discovery disputes should be subject to mediation before a party is permitted to file a discovery motion.
- c. Never, mediation is limited to working with parties to resolve their underlying claims.
- d. Only in a small number of particularly complex or high value cases.
- e. When a third-party neutral's experience might be of value to developing a mutually agreeable discovery plan.

Answers at the bottom of pages 18 and 19

Comments from
Hon. Bridget McCormack
Chief Justice of the Michigan Supreme Court

This past term, the U.S. Supreme Court conducted its first-ever remote oral argument. Audio of the argument was also broadcast in real time, something the Court has never done. The Court usually releases recordings publicly at the end of each argument week.

While the pandemic-induced broadcast was well received, it also drew attention to the Court's long-standing policy of prohibiting cameras in the courtroom–a policy that the Court continued to follow, in spirit at least, with its telephone-only argument. Maybe live audio broadcasts will continue once the Court resumes in-person arguments, but for now it seems unlikely that the Court will revise its policy against cameras.

That is too bad. Public trust is the currency of government, and the judiciary is no exception. Access to judicial proceedings helps maintain that trust. Allowing the public to observe how courts operate both fosters a sense of accountability in our judicial system and helps demystify processes that may seem impenetrable or arcane to non-attorneys.

The Supreme Court has even recognized a right of public access to court proceedings, albeit a limited right. As Chief Justice Burger wrote in *Richmond Newspapers, Inc. v. Virginia*, "[t]he right to attend criminal trials is implicit in the guarantees of the First Amendment, without the freedom to attend such trials, which people have exercised for centuries, important aspects of freedom of speech and of the press could be eviscerated."

But, of course, the number of people who can attend oral arguments before the Court is very small. Typically, only 50 seats are reserved for the general public.

Supporters of the Court's no-cameras policy have long argued that the presence of camera would change the behavior of justices and advocates, and not for the better. That has not been our experience in Michigan, where since 1989 appellate courts have operated under rules that presumptively favor the allowance of film or electronic media coverage of proceedings. Even more recently, our state supreme court has broadcast live video of oral arguments and other public hearings. And we are not unique. Even before the COVID-19 pandemic, a majority of state supreme courts successfully used video livestreaming to make their proceedings more accessible and transparent.

Currently, court systems around the country are going through rapid, pandemic-induced changes. At the appellate level, the transition to remote proceedings has been swift and relatively painless. The challenges have been far greater for our trial courts. Courthouses are high-density places, often located in buildings where social-distancing measures are difficult, if not impossible, to maintain. To conduct operations safely, especially jury trials, many courts have refigured their spaces, some placing jurors in the gallery section of the courtroom.

Safely maintaining public access during these times requires allowing cameras in our courtrooms. In Michigan, we have facilitated such access by equipping every courtroom in our state with a videoconferencing system. Court proceedings are broadcast live on YouTube.

To make access even easier, we have created an online directory where members of the public can quickly and easily find each of these "virtual courtrooms." While the proceedings may not command the public's attention like those of our nation's highest court, anyone with an internet connection can watch, in real time, any court in the state of Michigan.

We are discovering that virtual courtrooms not only protect public health during a pandemic but also help remove traditional barriers to access. They allow litigants to participate without requiring them to find transportation, arrange for child care, or take a day off from work for a hearing that might require only a few minutes of their time. For attorneys, the ability to "appear" in any court in our state without leaving their homes or offices can be a tremendous time-saver.

It is difficult to look beyond the current moment, but as courts formulate plans for an eventual return to normalcy, we cannot limit ourselves to simply "reopening" our old ways of doing business. Virtual courtrooms are not a panacea, and figuring out how they best interact with our understanding of the judicial processes and constitutional rights will undoubtedly be a learning process. But these are changes and lessons that, while accelerated by the pandemic, were likely inevitable.

By embracing innovation and refiguring processes that were once viewed as sacrosanct, we embrace the opportunity to create a system that is more accessible and transparent and that ultimately does a better job of delivering justice to the public.

Reprinted with permission, *ABA Litigation Journal* (Spring 2021).

The author is chief justice of the Michigan Supreme Court, and an associate author of *Litigation*.

The difference between routine document destruction and spoliation

By: Steven A. Neeley

This article was originally published April 26, 2021, on Husch Blackwell's The Contractor's Perspective blog.

In today's world, there is a tendency to believe that everything must be preserved forever. The common belief is that documents, emails, text messages, etc. cannot be deleted because doing so may be viewed as spoliation (*i.e.*, intentionally destroying relevant evidence). A party guilty of spoliation can be sanctioned, which can include an adverse inference that the lost information would have helped the other side. But that does not mean that contractors have to preserve every conceivable piece of information or data under all circumstances. There are key differences between routine document destruction (when done before receiving notice of potential claims or litigation) and spoliation.

The Armed Services Board of Contract Appeals decision in *Appeal of Sungjee Constr. Co., Ltd.*, ASBCA Nos. 62002 and 62170 (Mar. 23, 2021) provides a good reminder. There, Sungjee challenged its default termination under a construction contract at Osan Air Base in South Korea. Sungjee argued that the government denied it access to the site for 352 days (out of a 450-day performance period) by refusing to issue passes that were needed to access the base. The government argued that it had issued the passes, but it could not produce them to Sungjee in discovery because they had been destroyed as part of a routine document destruction policy. The base security force issued hard copy passes and entered the information in a biometric system. The government was able to produce the biometric system data but not the hard copy passes because they were destroyed each year.

Sungjee argued the government was guilty of spoliation and moved for sanctions. It asked the Board to draw an adverse inference that the passes would have shown that the government had not issued proper passes on a timely basis, which delayed Sungjee's performance. The Board denied Sungjee's motion for several reasons.

First, when the passes were destroyed, the government was not under a duty to preserve them so their destruction could not be spoliation. There are two ways the duty to preserve arises: (i) a statutory, regulatory, or contractual obligation to preserve documents for a specific period of time (*e.g.*, FAR Subpart 4.7 and Subpart 4.8); or (ii) litigation is "reasonably foreseeable" and the party should know that the documents may be relevant to the litigation. In the *Sungjee* case, the hard copy base passes were not "contract files" (which agencies must preserve) because the base security force was not a contracting party. Moreover, when the passes were destroyed, there was no reason to think that Sungjee would appeal its termination, so litigation was not "reasonably foreseeable." Sungjee had not previously asserted an excusable or government delay and had even admitted fault for the delays on several occasions.

Second, even if the government did have a duty to preserve, the destruction of the passes did not warrant sanctions because the government did not destroy the documents in bad faith or with a "culpable state of mind." In other words, the passes were destroyed "as a matter of routine policy," not out of a desire to conceal evidence. The Board also found that Sungjee was not prejudiced because Sungjee could not offer any other evidence to support its argument that the destroyed passes would have supported its position: "If the government's failure to issue needed passes was indeed the reason Sungjee could not timely perform, it seems highly unlikely that Sungjee would not carefully document this fact, so that at trial it could support its defense against the eventual termination for default with its own contemporaneous records."

Although the *Sungjee* decision absolved the government from potential sanctions, its rationale applies with equal force to contractors. Spoliation is not a "gotcha" and sanctions should not be imposed just because data is deleted. The key is whether there was a duty to preserve and whether the documents or data were destroyed out of a desire to conceal the information. If they were, sanctions may be appropriate. But that does not mean contractors must preserve everything forever. Routine document deletion when there is no duty to preserve is appropriate and permissible.

Steven A. Neeley is a partner with Husch Blackwell LLP. He focuses his litigation and arbitration practice on government contracts, renewable energy and construction projects. Based in Washington, Steven can be reached at steve.neeley@huschblackwell.com.

FORTZ Legal

The Trial Bubble is About to Burst

by Owner and CEO, Shaun Fitzpatrick

In late March of 2020, the litigation community, like many other businesses, came to a screeching halt. As a service provider for both trial support and court reporting services, we spent these first few months campaigning that remote depositions were a great option to counteract the restrictions of the pandemic. We embraced the inevitable change and put our creative minds together to come up with an amazing solution for conducting remote depositions. It did not take long for the legal community to see remote depositions as a viable option to keep their cases moving forward and now our court reporting services are as busy as ever.

Yet, even though our world has become increasingly more remote, not all legal proceedings seem quite as tangible in a remote setting. Trial dockets in civil cases have been continually pushed back, prompting many cases to settle. However, there are always cases that cannot reach resolution without a trial!

While some Judges across the country have participated in remote bench trials, there has been much reluctancy to host a jury trial that is completely remote. We can certainly understand the hesitation to conduct a jury trial in this fashion. Yet, our creativity and preparedness in this new remote environment gives us confidence that we will be ready for the day – in the not-so-distant future – when remote jury trials are the new normal. At Fortz Legal, we know that the show must go on and, when it does, will you be ready?

Blowing Things Out of Proportion:

S.D.N.Y. Finds Hyperlinked Documents Are Not Necessarily Attachments and Rejects a Revamping of Production Protocols

By: Kevin H. Gilmore

The Southern District of New York recently held that hyperlinked documents should not necessarily be considered "attachments" and declined to require a responding party to utilize a collection tool proposed by the requesting party, which would have collected all hyperlinked documents and maintained their familial relationship with the parent document. This is a novel and important issue that has not received such thorough treatment by other courts. With the COVID-19 pandemic forcing many employees to work from home and increasing the use of cloud-storage apps for documents, the issues related to the treatment of hyperlinked documents and litigants' obligations in collecting and producing these documents are unlikely to disappear anytime soon.

In *Nichols v. Noom Inc.*, the plaintiffs initiated a class action suit against Noom for a litany of allegations centered around false advertising. Prior to commencing discovery, Noom agreed to collect and search relevant data from multiple Google App sources (*i.e.*, Gmail, G-chat, Google Drive). The parties agreed to utilize Google Vault to collect the relevant documents from Google Drive, despite the fact that Google Vault would not be able to collect file path metadata for each document. Additionally, the parties never agreed to the method of collection for emails stored on Gmail. While Noom wanted to use Google Vault to collect the relevant emails, the plaintiffs were concerned by the fact that Noom's collection method would not pull documents hyperlinked within emails. The plaintiffs asked Noom to use instead an e-discovery forensic tool, Forensic Evidence Collector (FEC), which would allow Noom to collect the hyperlinked documents, so as to retain the familial relationship with the emails in which the hyperlinks were contained. Noom refused, and the parties sought guidance from the court. Noom balked, claiming that the process would cost in excess of $180,000 and was not necessary given Noom's agreement to produce any linked documents requested. The plaintiffs pushed back with their own expert's much lower estimate, but failed to include enough detail in their counterproposal for the court to fully evaluate their claimed cost estimate.

The court initially resolved this issue by allowing Noom to utilize its requested method, Google Vault, citing the oft-invoked Sedona Conference Principle 6, which states that the producing party is best situated to determine its search and collection methods. The court also noted the relative costs and delays that would occur should the parties utilize FEC and set forth a framework to guide the parties in the event of future disputes concerning these hyperlinked documents. The court provided, where certain hyperlinked documents could not be located or identified within Noom's productions, the plaintiffs should raise the issue with Noom and Noom would be required to either identify the bates range of the hyperlinked document or produce the hyperlinked document in question. While the parties had negotiated an ESI protocol, they did not define "hyperlinked documents" as part of a "family group"; nor did they define the term "attachment."

Following the original order, Noom utilized Google Vault to collect the documents from Google Drive and Gmail and produced these documents to the plaintiffs. As it turned out, the prevalence of hyperlinks in the produced documents was much greater than the plaintiffs had anticipated; there were thousands of documents that contained hyperlinks, with the plaintiffs having little to no ability to link these documents to their families. Therefore, in a letter to the court, the plaintiffs sought reconsideration of the court's prior order. Further, the plaintiffs requested the court to reconsider: (1) Noom's utilization of Google Vault to collect its Google Drive and Gmail documents, and (2) the court's proposed method for resolving disputes concerning hyperlinked documents.

In its opinion denying the plaintiffs' motion for reconsideration, the court first noted that it was clear there was "no meeting of the minds" in the ESI protocol as to whether hyperlinked documents were considered attachments and, as such, the ESI protocol could not be interpreted to treat hyperlinked documents as attachments. The court further reiterated that it did not consider hyperlinked documents to be equivalent to email or document attachments because they may not be "necessary" to the communication, whereas an email attachment is generally integral to the email correspondence. The court cited multiple examples of irrelevant hyperlinks to support its reasoning, such as hyperlinks that refer to another portion of the same document, hyperlinks that lead to a SharePoint folder, or hyperlinks in an email to a phone number, Facebook page, or a legal disclaimer.

In denying the motion, the court further relied on the principles of Fed. R. Civ. P. 1, 26, and 34. Attempting to foster efficiency in litigation, Fed. R. Civ. P. 1 mandates the court to ensure a "just, speedy, and inexpensive" trial, while Fed. R. Civ. P. 26(b)(1) works to limit discovery expense by requiring a party's discovery requests to be *proportional* to the needs of the case. Fed. R. Civ. P. 34 requires a producing party to produce documents in "reasonably usable form" to prevent a requesting party from unreasonable difficulty or burden in utilizing the documents efficiently in the litigation.

Here, the court expressed proportionality concerns with the plaintiffs' requests, because they failed to show any need for the hyperlinked documents or that these documents were relevant or material to the case. Further, citing Fed. R. Civ. P. 1, the court noted the unnecessary costs and delay that would result from the use of FEC to impose a redundant collection and review of the same Google Drive documents and emails already collected and reviewed by Noom. For example, the court hypothesized that email chains may contain multiple hyperlinks to the same document, resulting in that document being produced hundreds of times.

As the court stated, "[t]he issues raised by Plaintiffs raise complex questions about what constitutes reasonable search and collection methods in 2021." *Nichols* highlights the ever-evolving challenge for litigants, the courts, and the Federal Rules of Civil Procedure to keep up with technological advancements affecting e-discovery. While the court dismissed hyperlinked documents as not necessarily vital to a communication under the specific circumstances (especially in the context of the specific ESI Protocol entered by the court), it seems very likely that another court faced with a different set of circumstances could just as easily find that hyperlinks do in fact relate to relevant documents. We believe this is especially likely as collaborative apps such as Google Apps and Microsoft Teams become more popular. Without a cost-effective solution to collect hyperlinked documents that also provides for metadata, the information gap between the requesting party and responding party will continue to grow in contravention to the purpose of the Federal Rules of Civil Procedure to create a level playing field between the litigants.

The key takeaway here is that, in a case that may involve significant hyperlinked references in the production set, parties must include a discussion of how these specific data sources will be treated in their Rule 26 meet and confer and address these issues in their discovery protocols. Parties need to keep in mind that courts are not prescient on all of the cutting-edge issues involved in modern discovery and will accept (and, as here, likely stand by) the parties' initial agreements and recommendations regarding production protocols, particularly if costly changes are suggested after an initial production has occurred. That said, not every issue can be foreseen, so when new information is learned, proportionality considerations may shift. The parties and the court should be able to adapt to the changing needs of the case by modifying or amending the discovery plan and ESI protocol.

Kenneth H. Gilmore is an associate in the Commercial & Criminal Litigation practice at Gibbons. He handles a wide range of complex business and commercial litigation matters in both state and federal courts throughout the region. His practice focuses primarily on various aspects of general and complex commercial litigation, including factual investigation, discovery and strategy, briefing and motions practice, and appellate filings in connection with breach of contract, business torts, fraud, and breach of fiduciary duty disputes as well as code-based Federal law, such as ERISA and bankruptcy litigation. Based in New Jersey, Kenneth can be reached at kgilmore@gibbonslaw.com

TYK Answers

Answer 1. The correct answer is e. The duty to supplement discovery responses is set forth in MCR 2.302(E). Under the 2020 rule amendments, the language was updated to correspond to the current version of its federal counterpart, Federal Rule 26(e)(1)(A). Under the previous language of the rule, supplementation was required only if the failure to do so would be a "knowing concealment." The amended rule eliminates the "knowing concealment" language and requires supplementation where "the additional or corrective information has not otherwise been made known to the other parties during the discovery process or in writing. . . ." This is a substantive and important change as sanctions for a failure to supplement were not available unless the court found the failure constituted a "knowing concealment." See Boyer v Home Depot USA, Inc, 2010 WL 1254847, at *4 (ED Mich March 26, 2010) (striking supplemental initial disclosures but declining to impose monetary sanctions for failure to timely supplement); Tucunel v K-Mart Corp, --NW2d--, 1996 WL 33348842 at *2 (Mich App Nov 12, 1996) (finding plaintiffs' argument that defendant willfully and wantonly concealed evidence by failing to supplement was meritless). For a "knowing concealment" there had to be "a conscious decision by a party to prevent disclosure of the information requested." Richardson v Ryder Truck Rental, Inc, 213 Mich App 447, 452 (1995). Although sanctions are now available under a wider array of circumstances for failure to supplement, the severity of the sanctions under MCR 2.313(C), will likely still depend on the degree of culpability of the party failing to supplement and the prejudice suffered by the aggrieved party.

TYK Answers

Answer 2: The correct answers are c and d. MCR 2.401(J)(1) does not require the parties or the court to participate in an ESI conference. The permissive nature of the rule recognizes that not all cases will require a specialized conference solely to address ESI discovery. But, in any case "reasonably likely to include the discovery of ESI," the parties may agree to, the court may order, or a party may request an ESI conference via motion.This provision is new to Michigan law, and it has no counterpart in the Federal Rules. However, many federal district courts have, as part of their local rules, adopted model or standing orders related to ESI discovery. These local orders provide a framework for discussion of ESI-related discovery issues similar to MCR 2.401(J)(1). See, e.g., Eastern District of Michigan's Model Order Relating to the Discovery of Electronically Stored Information (ESI) Checklist for Rule 26(f) Meet and Confer Regarding ESI, which can be found at https://www.mieb.uscourts.gov/courtinfo/local-rules-and-orders. See also Oakland County Case Management Protocol for Business Court Cases, at https://www.oakgov.com/courts/businesscourt/Documents/ocbc-pro-casemanagement.pdf; Macomb County Business Court Discovery Protocols at https://circuitcourt.macombgov.org/CircuitCourt-SpecializedBusinessDocket. Many state court rules provide for ESI conferences. Unlike Michigan's rule, several states, including Arizona, Arkansas and Kansas, require mandatory ESI conferences.

Answer 3: The correct answers are a and e. MCR 2.411(H) was added in January 2020 because, according to the SBM Committee, some cases are particularly complex or otherwise generate an inordinate number of discovery disputes requiring court attention. "In order to best serve the parties and the interests of justice, the services of a discovery mediator may provide enhanced case management without causing undue expense, delay or burden, and without prejudice to a party's rights to have all discovery disputes adjudicated by the court." MCR 2.401(J) (ESI Conference, Plan and Order) provides a list of issues that you might consider addressing as part of your discovery mediation, including: (a) the scope of reasonably accessible ESI to be preserved and reviewed; (b) the search parameters to be used to locate ESI; (c) the method of review to be employed; (d) the data format (including metadata fields) for production; (e) the time and manner of production (including whether sampling and/or phasing of discovery is appropriate); (f) the procedures for handling privileged information (including whether a privilege log and/or a clawback agreement are appropriate); (g) the procedures for handling confidential and proprietary information (including whether a protective order is appropriate); (h) the methodologies to evaluate compliance with any discovery plan; and (i) the mechanism and protocol to enforce any mediated discovery plan. The outcome of discovery mediation should be reduced to writing and signed by all parties and counsel. See Michigan's Exciting Experiment: Discovery Mediation, The Litigation Journal Winter 2020 Newsletter (State Bar of Michigan Litigation Section).

RESOURCES

Association of Certified eDiscovery Specialists (aceds.org): ACEDS is affiliated with BARBRI and offers free access to a Resource Center which includes on-demand webinars, training materials, articles and blog posts. In addition, ACEDS includes 25 local chapters, each of which offers educational and networking opportunities throughout the year. ACEDS also offers a professional examination and certification program.

The Sedona Conference (thesedonaconference.org): TSC offers free access to hundreds of publications on several topics including eDiscovery, Data Security & Privacy, Complex Litigation and International Discovery. Many of the publications are recommended guidelines and principles developed by working groups composed of judges, attorneys, educators, consultants and other experts. TSC educational institutes and webinars are offered throughout the year for a registration fee.

The Electronic Discovery Reference Model (edrm.net): EDRM creates practical global resources to improve eDiscovery, privacy, security and information governance. EDRM provides articles, webinars, eDiscovery tools and diagrams and the opportunity to propose and participate in eDiscovery research projects. EDRM also offers a Hub which provides you the opportunity to search for jobs, post resumes and post job openings.

Institute of Continuing Legal Education (icle.org): ICLE is cosponsored by the State Bar of Michigan and all of Michigan's law schools and they publish a Michigan Civil Procedure Book which includes a chapter on Discovery of Electronic Evidence. ICLE also provide a broad range of discovery how-to-guides, checklists, forms, publications and webinars. Most of these resources require membership in ICLE or a modest cost to purchase.

State Bar of Michigan (michbar.org/civildiscovery): SBM offers litigation bar journals, seminars, guidelines and other background materials related to discovery in Michigan. In association with our ACEDS Detroit Chapter, ICLE published and offers a Guidebook to the New Civil Discovery Rules.

To become a member or find out more, contact Alma Sobo at asobo@dickinson-wright.com

To get information on previous and future events, recorded links and educational information, contact Cindy MacBean at CMacBean@Honigman.com

ACEDS DETROIT CHAPTER SPONSORS

Sponsor	Webpage	Contact Person
Acorn Legal Solutions	www.Acornls.com	Zef Deda Zef.deda@acornls.com
Cobra Legal Solutions	www.corbralegalsolutions.com	Doug Kaminski doug@cobrals.com
Conduent	www.conduent.com	Abby Melling Abby.melling@conduent.com
Consilio	www.consilio.com	Paul Ramsey paul.ramsey@consilio.com
Elijah	www.elijaht.com	Andy Reisman Andy.reisman@elijaht.com
Exterro	www.exterro.com	Chris Erickson chris.erickson@exterro.com
FTI Consulting	www.fticonsulting.com	John Winkler John.winkler@fticonsulting.com
Trustpoint One	www.trustpoint.one	Suzanne Alfastsen Suzanne.alfastsen@trustpoint.one
Warner Norcross + Judd	www.wnj.com	Jay Yelton Jyelton@wnj.com