Minerva26

Case of the Week: Five Years In—What the Last 179 Episodes Are Telling Litigators Now

Hi, and welcome to a special edition of the Case of the Week segment on the Meet and Confer podcast. Today, we are celebrating five years and 179 episodes of bringing you the Case of the Week. I'm Kelly Twigger, your host. Thanks so much for joining me here today.

For more than 28 years, I've served as merits and discovery counsel in a wide range of civil litigation, from $7,000 insurance disputes to $100 million bet-the-company class actions and everything in between. I love the complex engineering design cases, the IP cases, and those are incredibly heavy with discovery. But today, every case, large and small, has electronic evidence.

As paper evidence gave way to electronically stored information in the early 2000s and our Federal Rules of Civil Procedure were amended in 2006 to specifically provide for the discovery of ESI, my focus really turned to leveraging the opportunity of ESI to tell a story in litigation. And I say opportunity, because that's what I believe it is. We have more of an opportunity than we ever did with paper to piece together the facts of what happened in a matter.

Think about it. Everything you do in a day is somehow documented as ESI. You've likely emailed, texted, slacked, messaged, googled, chatted, traveled to, written in your calendar, or somehow otherwise communicated almost every one of your actions and the actions of people around you, whether for work or personal purposes. And all of that can be evidence in the right context.

By thinking about how people communicate and their actions in creating, storing, sending, and receiving ESI, we can find the puzzle pieces that we need to tell a story in litigation. The big difference is that no one hands us a box with the puzzle pieces in it, the way our clients used to with paper. Instead, we have to go and find them in the sea of ESI and pull them all together.

ESI presents another tremendous challenge because of its volume and the complexity of finding and collecting all of the various sources of ESI. Each one of those sources that I just mentioned: email, text messages, Slack messages, WhatsApp, Signal, cookies, GPS data, etc., etc. All of those require different methods for identifying, collecting, and producing them. And that handling of the volumes of data can be overwhelming. And when it becomes overwhelming, we think of discovery more as compliance — meeting our obligations under the rules to provide ESI — instead of focusing on finding the puzzle pieces to tell our story. And that's where we've gone wrong. We have to comply, of course, but the focus needs to be on what we need to tell our client’s story.

Another layer on top of the volume and complexity challenge has been the constantly evolving technology that we use to create ESI. During COVID, as an example, businesses and industry flocked to using Microsoft Teams and Slack for remote

teams to communicate. The release of ChatGPT in March of 2023 opened up the floodgates of AI tools that are at our fingertips. Senior government officials communicate on encrypted chat platforms like Signal and WhatsApp. All of that means that our courts are being asked to determine parties' obligations to provide ESI within the scope of a subset of rules on discovery and rely on parties to teach judges how the technology at issue works to help judges solve the dispute in front of them. Some are better than others, no question. Some judges are better, some lawyers are better.

But that process has produced a constantly evolving body of case law on discovery issues that has given us more than 5,000 decisions a year for the past several years. The quality of the decisions is, in most cases, directly correlated to the quality of the information that is given to the court to make a decision.

Keeping up with the discovery issues and technology is a full-time job, and it's not an easy one at that. I started Case of the Week during the pandemic in 2020 as a way to help litigators and legal professionals focus on *one* decision at a time and what you can learn from it. Now, in recognition of our fifth-year anniversary, I've gone back through all 178 episodes we've covered and identified five key issues that have evolved over those five years — and are facing us now — that are currently challenging litigators and require some real strategic thought for each matter.

Let's dive in.

Possession, Custody or Control

Our first issue is one that has divided courts across the country and will only continue to be a key topic in discovery: Whether an employer has the required possession, custody, or control over the data on an employee's mobile device under Rule 34 of the Federal Rules of Civil Procedure such that an employer is required to produce data from that employee's device.

I recently did an entire episode on this topic on our podcast with United States District Judge Xavier Rodriguez. So we'll link to that here and you can go and review that in more depth. Judge Rodriguez and I are also writing a law review article on the topic that will be published in April with some potential alternative ways to address the problem that courts have not yet taken up.

The long and short of this issue is this. The traditional analysis of whether possession, custody, or control exists under Rule 34 has been governed by two common law tests: either the legal right or the practical ability test. But in today's reality, neither of those tests actually fit for the analysis of whether an employer has possession, custody, or control over an employee's mobile device. They were created under common law, again, before we had this technology explosion, before COVID, before remote work, before the use of phones became what we do on a daily basis.

This issue is, as with all discovery issues, entirely fact-dependent. Is the phone company-issued? Does the company have a policy governing the use of specific applications on the phone? There are a number of factual questions that courts will ask in trying to fit the analysis into either the legal right or the practical ability test. Courts that engage in that kind of factual analysis, as in In re Pork Antitrust Litig., which was Episode 72 on Case of the Week, and Allergan, Inc. v. Revance Therapeutics, Inc., which was Episode 171, and more recent. They have both used policy and IT practices to find that the employer did not have possession, custody, or control. Allergan really looked back and relied on the reasoning in In re Pork. But, interestingly, multiple other courts have ruled on motions for sanctions for loss of data on employees' personal

devices without ever considering the question of possession, custody, or control. It simply just isn't even raised in the court's analysis. The Hunters Capital decision, which we covered here on Episode 98 of Case of the Week, and the In re Skanska case, Episode 107, are examples.

United States District Judge Jane Boyle captured my view on the subject in her decision in Miramontes v. Peraton, Inc., which was captured on Episode 117 of Case of the Week. This is a quote from Judge Boyle in the Miramontes case: "Today, many, if not most, employees use cell phones for work. And while some companies issue work devices, others, including Peraton, do not. Under Peraton's view, a company could effectively shield a significant amount of its employees' business communications from discovery simply by allowing its employees to conduct business on their personal phones."

Following that, we're still looking at the analysis of whether or not companies have issued their own phones versus allowing employees to use their own personal phones. We've gone away from the BYOD policies of the past, and we need to revisit those as organizations. But there really is no simple clear-cut analysis, no settled body of law across the country on this issue for you to use to advise your clients. But as the trends move towards production of data from employees' personal devices, preparing your client to have to produce mobile device data and having a plan in place for it will be to your advantage, even if you successfully argue the In re Pork view of the issue.

Hyperlinked Files

All right, our second issue, hyperlinked files, is one that is so confounding to all that I've done three webinars already in the last two years, and we're doing another one on collaboration data for E-Discovery Day on December 7th. I'll add the link to the show notes to register, or if you're signed up for our newsletter, you'll get it when you receive the Minerva Edge.

We now have more than 40 decisions ranging from 2021 forward on hyperlinked files in the Minerva26 case law database, and the crux of the issue is this: if your client uses technology that shares files via a hyperlink, you may be required to produce those files. Courts have held that the data that is responsive should be produced if it's technologically feasible.

Hyperlinked files raise several issues:

- Whether they can be collected from the custodian the parties have agreed to — and that takes us back to the possession, custody, or control argument;
- What version is available at the time of collection, and whether you want the one created when the message link was sent, or whether you want the contemporaneous version, meaning the one that exists as of the date you're collecting it; and
- Other considerations include how to actually preserve hyperlinked files and whether you can provide some kind of relational metadata that links the file to the original message, the way that we have parent-child relationships with physical attachments.

All of those are part of the hyperlinked files debate. As always, the answers to those questions really depend on the facts of the case.

In the *In re Uber Techs., Inc. Passenger Sexual Assault Litig.*, covered on Episodes 141 and 169 on Case of the Week, Magistrate Judge Lisa Cisneros wrangled with whether and how to require production of contemporaneous versions of Google Drive files hyperlinked in emails and Google Chats. There, the Court ordered preservation of linked metadata and production of contemporaneous versions "to the extent feasible", with a 200-link manual carve out where Google Vault blocked automation. So, a very specific ruling tied to the technology's capabilities and what parties asserted before her that could be done. All of that happened through a lot of expert testimony.

In *In re StubHub Refund Litig.* covered on Episode 144, that case taught us not to agree to an ESI protocol on producing hyperlinked files until you know you can actually collect the data. StubHub agreed to produce hyperlinked files and later found out they couldn't do it. The Court initially required production, but later let StubHub off the hook through the good cause language in the parties' ESI protocol, stating that if you can't do what you agreed to, that's good cause to modify and avoid sanctions. Note that StubHub probably spent several hundred thousand dollars getting to that result.

Other courts, including the *In re Insulin Pricing Litig.*, Episode 145, have discussed the technological ability to create metadata to create context for the receiving party. The issue really comes down to the technology that has been used to create hyperlinked files and the existence of tools to go and find those files. Parties need to be very informed about the technical issues here and whether, where it's crucial to the facts of your case to have the files and potentially the contemporaneous files, you'll want to get help. I just did a podcast episode on this issue with Arman Gungor, who is the CEO of Metaspike. Arman and his team at Metaspike have created a tool specifically designed to identify and collect hyperlinked files. So you can get down to the nitty-gritty in that podcast, and we'll link that in the show notes as well.

Discoverability and Context Required for Collaboration Platform Data

On to our third issue. And this is one that I identified as only going to continue to grow through the use of these types of platforms. And that is the discoverability and the context required when we are providing data from chat applications like Slack, Teams, or other IM tools.

Let's start with the context issue where there's no dispute about whether or not the data can be produced. In the Lubrizol Corp. v. IBM Corp., which was Episode 108 of Case of the Week, the Court held that Slack is analogous to text messages and ordered production of full threads of less than 20 messages (these are responsive to search term hits), and 10 messages before and after for longer threads, as well as parity for Teams messages — one party had Slack, one party had Teams.

That decision is a key for litigators that you need to review the data and really understand how much context you need to provide around search term hits for chat applications. Context is key for using the evidence. Think about how you'll use it at a deposition or in a motion if you don't have the right of context. Here's a hint: you won't be able to do it very effectively if the messages are cut off. You'll just have a search term hit and nothing above and below it in order for the court to provide context. The arguments to negate that information are going to come fast and furious.

As the use of AI tools expand to these applications, I expect that we'll see the case law evolve as well. You'll be able to use the AI to create reasoning around what is the proper context that you need for various messages. It may not even be the same for each search term hit. It may depend on the string, and the AI may be able to detect that.

The Two Canoes LLC v. Addian Inc. case, which we covered on Episode 148, expanded a party's duty to preserve WeChat messages on a mobile device over years and over multiple devices, and the failure to preserve those messages resulted in sanctions. That case involved the significant factual analysis of the timing around the messages at issue — another reminder of one of our key themes on Case of the Week, which is that the timeline of what happens with the information is critical in discovery. You need to be able to recreate that timeline in order to be able to make an effective argument to the court, whether you're arguing to compel production of the information or arguing that the information was deleted before your duty to preserve arose.

Now, setting that part aside, let's talk about the ability to get to the chat data even when it is responsive. Vaughn v. Solera Holdings, LLC, which was a case covered on Episode 174, is one of a few rulings on this issue that you may be able to leverage. And if you want to, you better do it fast because I don't think that'll hold up for long. In Vaughan, an employee sought Slack communications in a discrimination case, and the defendant argued its Slack plan did not allow for export for production. The Court, hearing that information about the export, denied the plaintiff's motion to compel, effectively precluding the plaintiff from all of the evidence for its case and held that there was no possession, custody, or control where the defendant had a license that lacked export capabilities.

Given this line of cases, and there are at least three that I can think of, you'll absolutely want to proactively address any planned limits at the meet and confer and possibly get an agreement to production in your protocol, or not, depending on which side your client is on. So that knowledge alone is going to save you something if you're talking about producing data from Slack.

There's no question that every type of data on messaging apps is discoverable if it's relevant. The question now is the technology piece and how to provide context. Again, as AI gets applied to these use cases, some of the technological constraints will be lifted and parties' obligations will start to crystallize. The question will be cost and access to these tools. Today, courts have not ordered parties to engage with tools that they are not currently using. Parties will have to do the ROI on providing the information themselves and calculate in non-monetary factors, like being able to get what you want from the other side, keeping the court in your good graces, and other things that I refer to as the 98% in my 98% rule.

Courts' Tolerance for Failure to Preserve and Discovery Shenanigans

All right, our next issue is one that I refer to as the court's tolerance for failure to preserve and other discovery shenanigans.

On this issue, there is really one definitive statement that I can make for you. Over the past five years, courts have grown increasingly, and I do mean increasingly, with multiple exclamation points, less tolerant of counsel and parties not understanding or not following their obligations to preserve and produce ESI. Sanctions are more readily granted — albeit more on the adverse inference side than terminating sanctions — for cases with demonstrated intent under Rule 37(e)(2), even when I think those terminating sanctions are warranted.

In *Lopez v. Apple Inc.*, which we covered on Episode 147, Apple failed to preserve data captured when Siri was falsely triggered, despite a retention policy after the duty attached. The Court ordered sanctions under Rule 37(e)(1), requiring

only prejudice, precluding Apple from weaponizing missing data, but left whether intent actually existed to the jury to determine whether there should be additional sanctions under Rule 37(e)(2).

In *Guardant Health, Inc. v. Natera*, Inc., October 23, 2024 and July 9, 2025, which I covered just recently on Episode 176 — and I highly recommend you read — counsel permitted an expert to self-collect, leading to a failure to produce key documents that led to a host of bad things, including counsel making misrepresentations to the Court about the scope of what was available. The result was sanctions, including evidentiary exclusion of very key data, a credibility instruction risk, and later $3 million in monetary sanctions imposed against the party and counsel.

The Guardant case is one that every head of litigation should be reviewing and circulating to its litigators. If yours hasn't, grab the link here and send it over. The errors there can happen to any litigator. Awareness is very much the key.

There's another case in this section that I think is worth mentioning, and that's the *Safelite Grp., Inc. v. Lockridge* case. I've covered this on multiple presentations. We've covered it here on a Case of the Week in Episode 159. In that particular case, you had an individual defendant named Lockridge who failed to preserve text messages on his phone even after his duty to preserve arose. His lawyer gave him a verbal legal hold — make sure you keep all the evidence — and Lockridge continued to have his deletion settings on his phone set so that they would only retain data for 30 days. He was found to be sanctioned to the tune of an adverse inference as a result of the deletion settings. An individual who was notified by his lawyer to put a legal hold in place was still liable for sanctions.

The court's leniency — those days are gone. You need to know, you need to instruct your clients. If you're handling individual matters, you're at smaller firms, it doesn't matter. The courts are imposing these obligations across the board. It's been 20 years now since the Federal Rules of Civil Procedure have been enacted. I guess 19 years officially — December 1, 2026, will be 20 years. You need to know these obligations. You need to have them down and advise your clients.

Incidentally, in the *Safelite* case, the Court also said that a verbal legal hold was not sufficient, that it should have been in writing. Keep that in mind.

ESI Protocols

All right, our final issue here is one of my favorites, ESI protocols. And whether you're a fan or not of ESI protocols, you'll want to know that now, more than ever, the courts want to see the parties come to an agreement on how they will handle ESI.

Every single case involves ESI. Every single case is not complex. Just because you have a less than complex case, what seems like fairly easy — only a few custodians, only a couple parties, a small breach of contract, a family law dispute — it doesn't mean you don't have ESI issues. You do. Learn what you need to know for your cases. You don't need to know everything. You need to know what you need to know for your cases.

So even if you make the decision to only include the form of production in a protocol, you're still going to want to listen up. Just last night in my law school class we had a guest speaker, Jerry Bui, the VP of Forensics at Purpose Legal. And if you don't know Jerry, you absolutely should and you should follow him on social media. His work in the forensics area on

illuminating what's happening with deep fakes and using AI tools is riveting. It's a little bit scary. But anyway, so follow Jerry. He's listed as the forensics weirdo.

During our class, we discussed how the metadata for every application, for every forensic artifact, as he discussed it, is different. And you need to think about that before you agree to a protocol. You need to think about each data source that you will need and plan for language to revisit the protocol when you identify a new source that you didn't think of, because you will. If you want social media posts, cookie data, audit logs, email, Slack messages, WhatsApp messages, Signal data — all of them have different metadata fields.

Now you don't need to know them off the top of your head. They're all just a click away in Google or ChatGPT or your favorite AI tool. Use the technology to find out the fields that you will want to be able to sort and filter the data. You may not need every metadata field. Just think about when I get this data in, how am I going to want to filter it? How am I going to want to organize it in order to take a deposition or in order to present that data for authentication, in order to create a timeline of social media posts that happened to be able to show a particular fact. What is the data that you're going to be able to want to put forward, to be able to use, to authenticate, and to be able to show that information in a way that's constructive for your case?

One case in particular that has been ripe with disputes over the terms of an ESI protocol, and I've covered it several times on our Case of the Week, is *In re Meta Pixel Healthcare Litig.* In Episode 115 [May 18, 2023], the Court refereed the first wave of disputes over ESI protocol language that included search terms, privilege log, and scope. The Court imposed rigor around testing search terms and protocol specificity to prevent vague, unworkable regimes. Basically, she said, you guys got to do this language better than you have. In Episode 118, the Judge, in resolving whether additional custodians were warranted when they were requested, she stated that there was a factual showing required before expanding the custodians and required the requesting party to tie them to specific claims and defenses, as well as provide evidence of relevance for each custodian before they were entitled to them. And in Episode 172, the Court entertained a motion over browser device cookies as ESI and ordered a targeted meet and confer and workflow to produce cookies with appropriate metadata, treating cookies as discoverable ESI, where relevant and proportional.

So, in each of those different rulings in *one* case, you've got various sources and ways that counsel needed to think about ESI. This is a prime example of why you need to think through all the ESI issues that you have before you draft a protocol so that you can construct the language in a way that's going to measure up with your case. The complexities of drafting an ESI protocol are intense, no question. So the language that you use is going to be very critical in determining whether a court will find in your favor on a dispute or not.

If you're interested, we are putting out a revised edition of our ESI protocol that will include a lot of what we're talking about today. That will be available in a couple of weeks on the Minerva26 website. So if you sign up for the newsletter there, then you'll be able to receive a notice when that protocol is available.

If you are anywhere outside of the Am Law 100, you may be thinking, Kelly, there is no chance that I or my firm will ever get our arms around all of this. I'm going to push back and I'm going to say that instead of being overwhelmed by this big picture, all of these issues that I've just laid out for you, I want you to start small. Think about what the story is that you need to tell for your case, who the people are, who the facts are that are involved, and what ESI they will have created

that will allow you to tell the story you want to tell. Then investigate what you need to do to get at each source of ESI. Throwing up your hands only hurts your clients, and in the long run, it'll hurt you. You can do this.

What's Next on the Discovery Issues Radar

All right, what's coming? So what's on the horizon? What is the next big thing that we're going to have to think about? What's coming is really more of what's already here, unfortunately. And that is the issue of data generated through the use of Generative AI tools. We are having discussions and decisions on the discoverability of data sets used to create AI tools and whether all chats from users of GPT should be preserved for years. That's what's going on in the *N.Y. Times v. OpenAI* litigation. That preservation of all the chats created on the ChatGPT website is a preservation order that came down and that concerns a lot of people. If you've used ChatGPT, your chats are being preserved.

These issues will continue to grow and filter into our case law on discovery issues as soon as I would say this month, next month, definitely in the coming months. We will start to see decisions on requests for prompts from users used to generate AI content and even requests for prompts from within review platforms being created by legal teams to better manage review and documents. Are those going to be privileged? Are they not? Does it depend on who did it? Does it depend on the context? Was there adequate supervision? We don't yet know what those issues are going to be. By the end of 2027, I predict that we'll have more than 50 decisions from across the country on these various issues.

Conclusion

The reality is that the onslaught of discovery issues and case law is *not* slowing down. It is speeding up. It's moving as fast as the releases from AI companies are flying at us. You need a plan in place to stay up to speed on these issues so you know what you need to know for *your* cases. Courts are ready for these disputes, and your arguments are only as good as how well you teach the court about the technologies involved. ESI is an opportunity, but it's also one that will bite you if you aren't paying attention.

All right, that's it for our 5th year anniversary episode. Thanks to every single one of you who's joined me on this journey for the last five years. I'll keep making episodes as long as they are of value to you and we have lessons to learn. So please let me know your thoughts about the issues you want to hear about. Thanks so much and have a great week.

That's our *Case of the Week* for this week. Be sure to follow the Meet and Confer podcast on your favorite platform, or if you prefer, you can follow us on our blog at Minerva26.com/blog. If you're interested in seeing how Minerva26 can help you engage in better discovery strategy, please visit us at Minerva26.com.

As always, if you have suggestions for a case to be covered on the Case of the Week, drop me a line. If you'd like to receive the Case of the Week delivered directly to your inbox via our weekly newsletter, you can sign up on our blog. If you're interested in doing a free trial of our case law and resource database, you can sign up to get started.

Have a great week!