



# Effective Document Collection and Legal Hold Protocols

## Effective Document Collection and Legal Hold Protocols

MARNI CENTOR: Hello, everyone. The Association of Corporate Counsel and SmartPros Legal & Ethics welcome you to today's webcast, "Effective Document Collection and Legal Hold Protocols."

*[The instructions provided here were intended for attendees of the live webcast when it was originally broadcast.]*

Our presentation today will be moderated by Amar Sarwal, who is general litigation counsel for the United States Chamber of Commerce. And now, I'll turn it over to Amar.

AMAR SARWAL: Thanks, Marni. Welcome to today's webcast on effective document protection and legal hold protocols. As Marni mentioned, my name is Amar Sarwal, and I am general litigation counsel at the United States Chamber of Commerce and a member of the Association of Corporate Counsel's Litigation Committee.

As the Supreme Court has recognized in recent years, corporate defendants are faced with staggering costs due to the burdens of discovery. With the advent of electronic discovery, these burdens have only multiplied, with the companies increasingly focused on document retention and management practices that make sense for their bottom line while also meeting the strict protocols being developed by trial courts. Given the importance of these issues to the health of their companies, these issues should be front and center for all in-house counsel. I am pleased to be joined by three experts who will educate us on the most effective and cutting-edge approaches.

Craig Carpenter is a vice president and general counsel at Recommind. Mr. Carpenter has extensive experience in the e-discovery, enterprise, software and information security industries, is a frequent writer and speaker at industry events, and a leading advocate with key industry groups like The Sedona Conference and the EDRM project.

Next, Wendy Curtis is special counsel for e-discovery and is chair of Orrick's e-discovery working group. Ms. Curtis consults on e-discovery strategy and litigation matters. She has been engaged by Fortune 100 companies and major financial institutions to create and deploy e-discovery and records management programs. Wendy has generously offered a complimentary case alert. We will provide details about that case alert at the tail end of this webcast.

Last, but not least, Julia Peixoto-Peters is an IT and e-discovery counsel for DHL, working from the DHL Data Center for the Americas region in Scottsdale, Arizona. Julia leads the e-discovery and data retention practice group for DHL Legal and advises the various DHL business units on complex issues related to e-discovery readiness, data preservation and collection efforts in the context of litigation and data retention.

*[The CLE code and instructions provided here were for use only by attendees of the live webcast.]*

OK, with that, I'll turn the program over to Craig.

CRAIG CARPENTER: Great, thanks, Amar. Good morning everyone—or afternoon—wherever you may be. I quickly wanted to walk everyone through the agenda before we get into the meat of the program. We have a very good panel here, and an exceptional moderator. We thought it would be very helpful to have a nice cross-section of the industry with someone on the in-house side, in the form of Julia, someone as outside counsel, in the form of Wendy, and then Amar, and myself, for that matter, in terms of other attorneys who really see a good cross-section of what's going on.

The topic for today is in my opinion very apropos with a lot of the issues that we're all dealing with. I think what you'll hear each of us talk about as we go through the program is the number of issues that can arise when preservation—or backing up further than that, identification and preservation and collection are not done correctly. There has actually been some recent case law that we're going to delve into a bit here that highlights the downside for parties when collection and preservation are not undertaken in a way that they should have been in terms of defensibility and consistency, etc.

So, quickly, just to walk through the agenda, Amar has taken us through the introductions. So what we're going to spend our time doing is focusing on these seven kind of distinct steps or areas that we want to analyze today.

The first that we added in here, although it wasn't in the title, relates to early case assessment. Early case assessment has been getting obviously a lot of attention these days. We want to kind of deconstruct it and start from the perspective that we don't all share a common definition of what early case assessment is, or what it should be, let alone the dependent factors that dictate the success or failure of an ECA effort. So we want to delve into that a bit, which we'll do shortly here.

The next step in the process deals with implementing a defensible legal hold process. Oftentimes on the vendor side, we talk a lot about technology, and on the outside counsel side they talk a lot about the substantive law. Eight or nine times out of 10, in my experience, when problems arise or when problems are avoided it's because there is good solid process and work flow on the in-house side, and that's where Julia spends her time dealing with. And so, we're going to walk through that next, because that's a critical kind of piece of the puzzle.

Then we're going to get into the collection stage, first looking at the defensibility from kind of a substantive legal angle, and then getting into the different schools of thought. Traditionally, over the last many decades, self-collection—having individual custodians deal with collection themselves—has been the “accepted” approach. More recently there has been an approach that deals with taking images of drives, and that's what we refer to here as forensic imaging, which we'll get into. And then last, but not least, deals with something that has been gaining in popularity quite a bit, and that is selective collection.

We're going to walk through those three schools of thought and why one or the others may make sense in certain situations and what might work for you. Obviously we all work for different size entities, so there is no-one-size fits-all for any of this, but there are certainly some best practices that we want to delve into today.

The next step is getting a little bit more kind of future looking, although many of us are already dealing with this today, and that is dealing with data or ESI that is outside our “custody and control.” So we’ll have Wendy walk us through the substantive angles of that, in terms of where do you draw the line between custody and control. And we’re going to touch on all sorts of great buzzwords that we’re hearing about: cloud computing, Web 2.0 tools, software as a service, etc.

And then the last two areas: We’re going to focus on technology, which is something that is near and dear to my heart, in terms of which parts of the preservation, collection, early case assessment process or spectrum lends itself best to automation, and how exactly do we do that. And then Julia is going to offer some tips in terms of how she deals with this sort of thing and what works for her and what doesn’t.

And then last, but not least we’re going to talk about releasing a hold, something that probably gets short shrift, although it’s something that, if not done right, can also cause some headaches further down the road for any number of reasons.

We do have a question-and-answer session dedicated at the end here, although we would encourage you to [ask] questions early and often, kind of like voting in Chicago, because we will actually interrupt or answer the questions as we go through the presentation, because we’re covering a lot of territory here and we feel that’s the best way to do it. So please, we encourage you to ask questions whenever something arises in your head.

And then we’ll just have some parting thoughts, and as Amar mentioned, Wendy has been kind enough to offer up a case note, or a case alert, that she has done for Orrick on the recent *Pension Committee* case that we’re going to delve into a bit here that I think you’ll all find of a great deal of value. So please stick around for that, and we’ll give you Wendy’s contact information that will allow you to get that.

So, real quickly here I want to just walk through what we call ECA, which is short for early case assessment, that many of you have probably heard of, whether or not you’re familiar with it. And what we find in the industry, and I think on the speaker side we’re all kind of in the same boat here, is that ECA is a little bit like art. It means many different things to many different people. Although this is one area that we should really have a more consistent approach to it. So we thought we would—or I thought I would—start out by looking at Wikipedia, because it’s certainly not the final word on anything, but it’s a good place to kind of get a consensus in terms of what people think of a particular topic.

So, in Wikipedia, at least, the definition, which I think works pretty well for early case assessment is: a process that allows a party, in many cases a defendant, but not always, to estimate the risk, which is comprised of time and money, to prosecute or defend a legal case. I would also argue that that would include regulatory investigations as well, because it’s really the same process or function, although obviously there are different elements to it.

The cost aspect of it really comes in a couple different flavors, and the risk aspect does as well. Obviously time costs people money, but there is also the cost of disrupting the normal work flow of people trying to do their daily jobs—what we, in the legal space refer to as custodians. And then the risk aspect really deals with a couple different things. What’s it going to cost for time

and money to defend this case? And then, ultimately, what are the odds that we are going to prevail during this case? And then arguably the most important thing these days is: What is it going to cost us to prosecute or defend a case? What we're finding a lot these days, and what The Sedona Conference is spending a lot of time dealing with, is what is called proportionality. Oftentimes you'll have the amount at issue being dwarfed by the collective cost of the parties to get to the ultimate fact in terms of who was right and who was wrong, and who should ultimately pay or remit some sort of damages.

And early case assessment really seeks to get at that. How do we figure out if we're going to win, how much it's going to cost us to get to that stage, and that may dictate that it's worth settling or not filing a suit from the beginning.

So what does early case assessment require? And by the way, and this might sound counterintuitive for me to say this on the vendor side, but early case assessment is really a process. Technology can help facilitate it, but early case assessment is not in and of itself a technology, nor is collection, nor is anything else. The workflow behind it is arguably the most important aspect to it. So you'll see here, in terms of the requirements of early case assessment, two of them, or actually maybe even most of all three of them, don't involve technology.

The first thing is identification of key people, locations, timelines and documents. And actually technology can very much help in this regard, but again, you need someone who knows what they're doing, and that's where we get into the kind of educated analysis step. But you need to be able to wrap your arms around: Who are the key people or custodians that are involved in any given proceeding? Who has ownership or custodianship of the particular content that will be the most relevant and/or responsive to the case at hand? Where are they? Where is the ESI that's relevant to this particular proceeding? What are the timeframes in which we should be looking? Because obviously you don't want it to be grabbing all the data from the company's inception unless you absolutely have to because it's relevant to a particular proceeding.

And then, what types of data? If this particular action had to do with phone calls being made between certain people, then perhaps e-mail or instant messaging is not particularly relevant. These are all the things that you need to kind of identify from the very, very outset of a case, at the time of the legal hold and preservation and collection, as we'll talk about as we go.

Educated analysis: You need to have someone, typically internal, but oftentimes internal working in conjunction with someone on the outside like Wendy, to go in and conduct some sort of educated analysis. OK, we have documents in front of us that are relevant. They tell us something. What does this tell us? And how can we extrapolate that into some sort of strategy with respect to this particular proceeding?

And then last but not least, is speed, and this is something that I think a lot of people miss. Oftentimes we see early case assessment conducted after documents have been preserved, after the legal hold notice has been sent out, after documents have then been collected and then they've been sent to some external third party to be processed, to be culled and to be filtered, and then early case assessment is conducted. That is simply too late. Early case assessment needs to be done from the very outset, because you need to know what you're getting into before you start incurring costs. And that's where we get to the last bullet here, which is: What should early case

assessment deliver? And ultimately, it's insight into a proceeding, ideally before you've spent any money, but in most cases before you've spent any appreciable amount of money, or before you've started to make strategic decisions. So, get a good feel for where things are headed before they go there, which will obviously put you in a good position from there on out.

So, the next step in the process, that I am going to go ahead and turn over to Wendy, is: How do you implement a defensible legal hold process? What are the very steps, and what are the things that you want to be aware of in going through this?

WENDY CURTIS: Thanks, Craig. And thank you to everyone for participating today. And I just want to emphasize that what Craig said: Please stop us with questions. We want this to be as practical as it can.

On the ECA point, before we jump into preservation letters, I just want to pick up on two things that you said, Craig, and that is that timing and the strategy. There are protections available in the law, in the rules, to manage costs, but you have to take advantage of them, in essence before you incur the costs. So as you think about ECA, I would think about it in the context e-discovery and not what are the strengths of my defenses or the competency of my opposing party, but rather what are my risks, what do I think this is going to cost me, and how am I going to manage those costs? And so if you can plan, including what you do here with preservation and collection, and start those discussions with the opposing party sooner rather than later, you will have more protections available to you: anything from the proportionality that Craig alluded to—the arguments under Federal Rule [of Civil Procedure] 26—to cost-shifting to just structuring your scheduling order and your discovery plan to account for tiered discovery.

Judges hate to see this in the motion practice, and they really want you to be focusing either at the meet and confer or in your scheduling your discovery order. I was on a panel with Judge Peck at LegalTech, and I talked about this—contemplating proportionality, tiered discovery—and he echoed: If you include in your scheduling order that you are going to take a first stab at a limited number of custodians of information, allow the receiving party to look at it, and then meet and confer again to decide how much deeper you have to go, he will consider expanding the discovery timeline to allow for that. But if instead you wait until discovery is about to close and then start asking for relief, then start asking for additional discovery, he's going to be much less sympathetic.

And on the cost-shifting issue, if you take nothing else away from today's seminar, remember that you have to ask for cost-shifting before you have incurred the cost. So I understand some folks are having a hard time hearing me. I am one of the folks in the snow, so I'll try to speak up here. But again, for cost shifting, just remember that you have to ask for that relief before you incur the cost.

So shifting then to the point on how do you implement a defensible hold. If you haven't seen the *Pension Committee* decision, this is Judge Scheindlin's most recent decision and it is the next iteration in the trilogy of *Zubulake*. So, in that opinion she says a series of things, one of which is it's gross negligence if you fail to issue a written hold. And she talks about, in that decision, the importance, as she did in *Zubulake*, of issuing that hold. And I think when you think about this, and it's important to step back and evaluate where you are. Are you the plaintiff or the

defendant? What is the date that you're using to, in terms of when you issue the hold, and how does that relate against the date that you used to argue the trigger of the work product privilege? You want to make sure that those two dates reconcile and that you don't say that you were anticipating litigation for the purpose of work product, but then you weren't anticipating litigation in terms of issuing the preservation notice.

On the distribution of your notice, again, it's important here if you think of e-discovery like a funnel. You want the preservation to be the broadest point and then ultimately the production to be much more narrow. The better story that you have to tell in your meet and confer, and also in your motions practice with the court, the more likely you are to get protection. So that if you can show that you took a reasonable approach and a broader approach on preservation, you will be much more effective in arguing a lesser scope on collection in tiered discovery.

Again, you can expand and contract the distribution of your preservation notice as you learn more. So when your duty to preserve first triggers, get that notice out as quickly as you can to the folks who you know are involved, and then in an iterative process you can expand and contract the distribution list as you learn more, conduct custodian interviews, or claims are added or dismissed.

We see a lot of discussion about the gold standard and confirming receipt of a preservation notice. My practical tip to you is: Do not confirm receipt or require your custodians to confirm receipt of a preservation notice unless you have the resources to follow up on that audit trail. It's really important that if you create a record that six custodians didn't confirm receipt of the preservation notice that somebody followed up with them. And again, these are pros and cons of the automation that we'll talk about when we get closer to technology, but you need to have the manpower and the resources behind the technology, so if there is an audit trail in terms of folks who haven't responded, or from folks you haven't collected, you need to make sure that you have somebody monitoring all of this audit material that the technology is generating.

Just in terms of practical tips on reminders and instructions, I think quarterly is best for reminders, but at a minimum you should shoot to get a reminder of your preservation notice out every six months. And then the process and documentation, another practical tip: Compare your preservation notice or your litigation hold—we use those terms interchangeably—but that distribution list against the folks from whom you collect. And you want to make sure that everybody that you went and collected from also received the preservation notice. It's not necessary for the reverse to be true. Again, thinking of that funnel, you may have a broader distribution or preservation notice and decide only to collect from a subset of the folks who are truly the key players.

But as you make those decisions, whether it's to collect from some and not to collect from others, or to take somebody off the preservation notice distribution list, to the extent that you can, it's very helpful to document that. Generally our conduct is not willful—we don't have bad intent—but often, 24 months later, when we're trying to explain to the court or an opposing party why we did or didn't do something, we just don't recall. And so, if you can keep that record, then it's also much easier to have somebody find that declaration to explain why, if there was an honest mistake, again, it was an honest mistake, but that your process was defensible and reasonable.

The other tip that I just ask folks, too, is that more and more, we see preservation notices be distributed by e-mail, and so if you are trying to send it to John Smith, and you've also got Joseph Smith and Jared Smith, just to really double check those e-mail lists and make sure that you sent it to the right folks.

Coming back to the distribution, the *Pension Committee*—Judge Scheindlin issued an original order on the 11<sup>th</sup> of January, and then she issued an amended order on the 15<sup>th</sup>, which clarified some of the points that I think caused a lot of us—especially, often, corporate defendants—for their blood pressure to rise. Two things that she didn't change in the amended order: One was the quote where she said “The failure to collect records, either paper or electronic from key players constitutes gross negligence or willfulness, as does the destruction of e-mail or certain backup tapes after the duty to preserve has attached.” And then this is the next sentence that I think causes me concern. “By contrast, the failure to obtain records from all employees, some of whom may have only had a passing encounter with the issues in the litigation, as opposed to key players, likely constitutes negligence.”

And I think this is a concerning statement because she doesn't provide context and she doesn't apply proportionality. There is lots of case law, including *Zubulake*, where she talks about the need to preserve and collect from key players and not all employees. But I would caution you from folks misusing this quote, if you see folks starting to argue the *Pension Committee* case for over-collection and over-preservation, because I think the law is strong that you do not, especially if you are a large corporation, need to send that preservation notice to everybody, and in fact that would be overly burdensome, and then, again, it needs to be the folks who had a some kind of reasonable role related to the facts of the litigation.

So with that, those are my comments on preservation notice. Julia, did you want to add anything on this slide?

JULIA PEIXOTO-PETERS: Thanks, Wendy. I do, actually. I would like to go back to the previous slide, just because I had a few comments on the ECA process from an in-house perspective. And my thoughts are that in order to do true ECA in the context of e-discovery, there are two critical things that you are going to need. One is visibility into the entire e-discovery process from end to end. And because e-discovery is a process that typically involves a blend of in-house and external processes, tools and resources, it's not always easy to gain such visibility.

For instance, if you are doing preservation and collection in-house, but then you're processing and reviewing data externally, you may be getting different metrics from external vendors and you may not be getting any metrics at all for your internal processes. So what you need is a very solid process for reporting that will give you visibility to all data preserved, collected, processed, reviewed, and ultimately produced and the associated costs and time. Without having this visibility, it will be very difficult to do case assessment, not to mention early case assessment.

The second thing that I think is helpful in the context of ECA—I think you touched on this briefly, Wendy—is an early agreement on the scope of the e-discovery efforts required for your litigation, preferably at the meet and confer stage. What I see in my practice is that—and no offense to outside counsel—is that outside counsels are not always using the meet and confer to

agree on the terms of the collection and production, or not always making the best use of the meet and confer. A lot of times outside counsel leaves the meet and confer without a clear agreement on what should be preserved, what should be collected, what should be ultimately produced. And without this early agreement on this scope, I find it very hard to practice early case assessment, as you won't know the true cost and the true scope of your litigation until you incur that. And like Wendy said, you have to argue cost-shifting before you incur expenses, and by the time that you get to that it may be too late.

Then my next comments are on the litigation hold process. Once the litigation hold notice is sent out, that's when the real work begins, at least from an in-house perspective. A lot of people think that the litigation hold notice is that's that—it will give you a break and you can focus on some other things—but from my experience, that's when you have to start getting people together in the same room when discussing their involvement in your lawsuit. So that's why you have to understand what data you'll be dealing with as part of your obligation to produce records.

So one of the things that I find very helpful in my practice are, one, follow-up interviews. And I know a lot of us just don't have the time to sit down with each of the custodians and understand where they have data, and that's when automation of the process can be helpful. There are tools out there that will allow you to run surveys and understand exactly what each custodian's involvement is in the lawsuit [and] where data resides. There are questions that you can formulate, and this has to be customized in a case by case basis. But you can ask questions related to your lawsuit and understand exactly where you are storing your data. I know that a lot of companies are following records retention policies, but there may be places or sources of data that you just don't know based on your data map or your records retention policies.

But most importantly, you have to document your process. The process is only as good as your documentation. You have to document your key decision points and steps that were undertaken to identify and collect from the data universe that you have identified. Wendy mentioned the *Pension Committee* decision and the distinction that the judge made between key players and other employees who may have only had a passing encounter with the issues. I think one important thing that people probably are not taking into consideration is that you can divide your universe of witnesses into two categories. You can have your key witnesses, and for those preserve data with a litigation hold right away and collect their data—at least some of their data—at that stage.

And then, for secondary witnesses, what you can do is: Issue the litigation hold to make sure that you're preserving everything and follow up with a few other staff. You can dive in and try to understand to what extent they have data that is potentially relevant to your case through interviews, through follow-up surveys. They can view a good record trail of your effort to understand their involvement. And you can also review data collected from key witnesses to try to find the connection to the secondary witnesses.

If you find a strong connection, then I would say collect, when in doubt, just because if you don't find anything that is relevant, you won't have to worry about processing the data, hosting the data, and ultimately reviewing and producing it. But it's important to go through those steps.

As far as former employees, I know that when the judge left the door open to require companies

to collect from all employees, potentially, the first question that comes to mind is: What do we do about former employees? So my thinking is that if the obligation to preserve has been triggered before the employee is terminated, then there is no question you have to preserve and suspend deletion of accounts, network data, prevent computers from being reassigned and re-imaged. If the duty was triggered after, then you're going to have to look at your policies. What do your policies say? If your policy requires or states that employees' computers are going to be re-imaged after 30 days, and if that employee has been terminated for longer than 30 days, then let's hope that your policy has been enforced. So it's very important to have enforcement at that point. And those are my thoughts on the preservation process.

CRAIG CARPENTER: Great. Thanks, Julia. We really appreciate those. So a quick question here—we actually have two questions that come immediately to mind as we go to the next slide—but the first, for Wendy, it has to do with—the question is: Can a *pro se* plaintiff request a preservation hold to a defendant?

WENDY CURTIS: Can a *pro se*? So here's the interesting trend, and hopefully a concise answer. The plaintiff does not set the parameters for the duty to preserve. Rather, the allegations of the case do. So can the plaintiff send a preservation notice to the defendant? No. Can the plaintiff, *pro se* or not, dictate the scope of that preservation? No. Do we see more and more opposing parties sending preservation letters to each other that say, "We expect you to be preserving all the following things"? Yes. But a *pro se* plaintiff has no control over the defendant. Rather, the party has to issue the preservation notice to its employees.

On the reverse, I recommend for defendants who are in a case against a *pro se* plaintiff, or if you are a corporate entity and again your opposing party is an individual rather than another entity, I do recommend that you send a preservation letter to them, which is not a notice, because you have no control, but rather you're saying, "I am reminding you, individual, that you have an obligation to preserve things, and that means your home computer, that means your personal cell phone, that means your Yahoo! e-mail account." So that if they don't do that you've put them on notice and you can then quickly get to what is now being called "metadiscovery"—discovery about discovery. Because we all know the entity's obligation but often individual plaintiffs are not meeting their responsibility. And if you can show that they deleted their home e-mail, then you may be able to get an adverse inference even against the individual.

So, Craig, do you think I answered the question?

CRAIG CARPENTER: Yes, I think that hit the ball out of the park, definitely. And so, why don't we—we can—Julia and Wendy both already talked about the collection process to varying degrees. Why don't we kind of hit the rest of this slide in the context of a question, which I think—it comes from what I think is a midsized enterprise, but my guess is this problem faces enterprises of all sizes. And essentially what the question is, is that the backup process for this particular enterprise applies to all computers and, in all likelihood, all relevant data sources, so that essentially there is an all-or-nothing when it comes to legal holds. Either everything has to be preserved, or nothing can be preserved, which obviously is not the best way to go. And the question essentially is: How do companies—and I want to start with you, Julia—how do companies get around this kind of all-or-nothing approach with respect to company data and get to a happier place where data can be preserved and collected more selectively?

JULIA PEIXOTO-PETERS: That's a very good question, Craig, and I think that one of the important things to keep in mind here is that when you talk about all-encompassing backups, you have to have a plan on how to deal with that. And backups are only going to be relevant if they contain relevant and unique data. You do not have to preserve backups. They're just a duplicative set of what you have in your live system. So keep that in mind, and obviously that applies to backup tapes as well as any other backup systems.

I am not a big fan of sweeping litigation hold notices that put entire systems on hold. I think that by understanding your IT infrastructure and by understanding your data sources, you should be able to implement a hold on specific data sets as opposed to entire systems, and that'll make your life so much easier when you are trying to manage your holds, particularly if you have a very large litigation portfolio. A lot of companies enter into this world of never-ending litigation holds and they can never release anything, and the consequence is just preserving data indefinitely. So I think that it takes a little bit of work, but if you spend time understanding your data sets and understanding the usual suspects—the systems and data sets that are always subject to litigation hold—you will be able to implement holds on specific data sets as opposed to all-encompassing holds that will prevent you from running your IT systems and locating data in the ordinary course of your business.

CRAIG CARPENTER: Great.

WENDY CURTIS: Julia, don't you think that there is an argument in a lot of cases, too, that it is sufficient to preserve in place; that you don't need a backup to achieve preservation? And there are protections in the safe harbor provisions of the federal rules, and generally case law does favor strongly auto-deletion, whether it is auto-deletion of e-mail or an auto-purging of a structured data base. But if your system is so enormous that even suspending that auto-purge would paralyze the business, there is language in the commentary to the safe harbor provisions [and] there is language in the case law about [how] you can't—the preservation obligation can't cripple the business if it is disproportionate to the case. And so, to your point, too, Julia of figuring it out earlier and getting everybody to talk about it is the only way that you're going to protect against it, but I have to echo your point to stay away from back up tapes unless you've got unique backup technology that makes it easy to restore. But it sounds to me like you've got comprehensive backups, which are only going to make restoration from that source more expensive.

CRAIG CARPENTER: To save time, your accessibility argument, I think, gets blown, right, in that process? So, one other thing to add here, and then we have another question about trigger events that we'll throw back to you, Wendy, is that from my perspective, this makes a strong case for where having someone who understands “where the dead bodies are” but also understands the IT systems, etc., coupled with good technology that is able to go in and in a comprehensive fashion grab data, collect it, in that context preserve it, with all the metadata associated with it, etc., so that you take the pressure off of the data backup and recycling systems and let them do their thing. As you pointed out, Wendy, the standard in courts is not preserve everything under all circumstances, in fact, far from it. So the quicker and more accurate action you can take from the outset, the more you'll be able to conduct your business the way you normally do with respect to your data backup and recycling, etc.

Now Wendy, just to throw it back to you, there have been a couple questions with respect to trigger events, so I was going to just move off this slide, but I think there is quite a bit of interest in terms of defining the trigger event. Does it require “threat of litigation”? Is it belief that litigation is likely? I understand this is getting back to that “art is in the eye of the beholder,” but how do you counsel your clients with respect to trigger events?

WENDY CURTIS: So the case law has even now evolved depending on the kind of case, whether it’s an employment action and where you are in the EEOC process, versus on the *Adams* case, an IP [intellectual property] litigation, and where you are in the kind of manufacturing flow and what you should anticipate in terms of your role being part of the litigation. I think that if you are a plaintiff, this is often very challenging. In particular, if you hire outside counsel, you begin to draft the complaint, and then you decide, “You know what? We are not going to pursue this.” You don’t issue a hold, you wait a year, and then you come back a year later and you say, “You know what? We do want to pursue this claim.”

And in those circumstances, again, a lot of this is objects and being able to recall and explain with accuracy and specificity to the opposing party in the court what you did. So if you can show, “Yes, we retained Wendy Curtis on this date. She prepared a draft complaint, but then, you know what? We decided not to pursue it. We, in essence, shut down the matter for a year. We didn’t issue a hold. Eighteen months later, we changed our mind, and as soon as we went back to her, then we issued the hold.” Or, “We issued the hold and then we released the hold.” But you need to show that what you did was reasonable, and also that you’re not doing anything that has the bad-fish smell of, “We prepared a complaint, then we did a huge records management purge, and then we filed the complaint and issued the hold.” I mean, a lot of this is just how it appears.

As the defendant, I mean, obviously, once you receive that complaint or you know the complaint has been filed, the duty to preserve is triggered. But there is an entire body of case law, and often it’s very fact-specific. But I think a lot of this, too, is good faith. If you hired outside counsel, if you’re starting to prepare work product, I don’t think you can argue that you can’t or haven’t anticipated litigation.

Employment matters, I think, are often, especially for companies that have a large number of employees, very tricky, because in a given time you have a fair number of disgruntled employees. In that circumstance, too, you can have a disgruntled employee, but their claim can be very small, and preservation and collection actually is all the same thing—that you go and take a small subset of information in their employment file. And again, all of this has to be proportionate to the value of the matter. So do I recommend that you follow the gold standard for small cases? No. Even medium cases? You, again, have to think this through and decide how far you want to go and what risk you are comfortable with. But you can never get everything.

And so, if you can have a thoughtful process and it’s consistent, then you’re much more likely to be successful. And then, as Julia said, hold your outside counsel accountable. We have clients now who have e-discovery counsel who participate in all their meet and confers. And we have other clients who have outside counsel guidelines that say, “You will cover these things at a meet and confer. And you will not wait.” And it may be search terms, or number of custodians, or date range, or self-collection versus vendor collection. And you have the ability to really you’re your

outside counsel, and I encourage you to do that, because, as Julia said, the sooner you're strategic on this and the sooner you start raising issues, the greater your ability to retain costs and reduce risk.

CRAIG CARPENTER: Great. Thanks, Wendy. And this is great; we're getting questions left, right and center at this point, which is a good thing. One simple thing to point out that hopefully everybody knows, but just realize that these obligations that we're talking about are not just on defendants. We normally think of them in the context of defendants, but—and this is a perfect segue to the *Pension Committee* case—these same obligations apply to plaintiffs as well, which is one of the interesting aspects of the *Pension Committee* case. Wendy and Julia have both talked about it up to this point, so we perhaps don't need to delve down quite as deeply. But Wendy, from your perspective, what are the take-aways, maybe in light of the kind of clarifying commentary made by Judge Scheindlin, but what are your take-aways from the *Pension Committee* case?

WENDY CURTIS: Sure. I think when she clarified this point on self-collection, she, in the amended decision, added a footnote that said, “Look, you can have self-collection. The question just depends on the individual matter.” And so—and this is the bottom quote on this slide here: “The adequacy of each search must be evaluated on a case-by-case basis.” So initially, all the commentary on the *Pension Committee* decision was, “This the death knell of self-collection,” and I disagreed with that even before she added this clarifying point.

But the theme, I think, from *Pension Committee*, and hopefully what you're hearing from the three panelists today, is: You've got to be able to explain what you did with specificity. And so that includes: What was your process for employee self-collection? What instructions did you give them? What IT interviews did you do in advance to have an informed protocol? What technical support did you offer them? And what sampling did you do of the collection to make sure that they were doing it properly? And how did you track this process?

So I think that there is still absolutely a case for self-collection, and a lot of clients do it and do it very, very well. There is even an entire—we could spend an hour on “What does self collection really mean?” Does that mean the individual finding the information and putting it in a folder and then someone coming behind to get it? Does it mean you have an enterprise license at your company that enables the company to self-collect versus the custodian? Regardless of what your situation is, I caution you not to rely on one approach. If you have an enterprise license—a forensic tool—and you've got one of the best self-collection policies and procedures in place, there are still cases where that may not work. It may either be an ITC action and the deadlines are too aggressive; you just don't have the resources. Or it may be [the Department of] Justice knocking on your door and they say, “We don't trust you to self-collect.”

And so, if you have the time and resource to be strategic before a case even hits, consider evaluating collection vendors and going ahead and negotiating discounts and having all of that in place, so when that worst-case scenario hits you're not doing the mass scramble.

We'll probably get to this in another slide, but I also think that the other take-away from the *Pension Committee* [decision] is the benefit of having an outside vendor. If you have an outside vendor assist in your collection, they can be the ones who provides the declaration on your

process, and if they're a good vendor they have a very standard and industry-leading practice that they follow. And they can also be your 30(b)(6) witness, so that you're not struggling to find somebody who has the technical understanding to be able to articulate well what was done, why it was reasonable, and how it compares to industry standards. So if you can't have your vendor serve as your 30(b)(6) witness or help prepare and sign the declaration, make sure that you spend time identifying the right person to do that and that they have the requisite knowledge. Because I think we got this opinion because Judge Scheindlin was so frustrated with the testimony and declarations that were offered in the case that now we have this decision. And often that's what happens.

CRAIG CARPENTER: OK, great. Well, why don't we let that take us into the—in fact, why don't we just go straight to the various approaches we can take to collection, from self-collection, forensic imaging, targeted collection. We've been talking about that a fair amount. Julia, do you want to talk about, perhaps, self-collection, and how you have done things, and what's worked and what hasn't?

JULIA PEIXOTO-PETERS: Yes. I want to echo Wendy's comments on self-collection. There is absolutely a place for it in the discovery world. I like to call it "attorney-guided custodian self-collection," and please note the "attorney-guided" portion of this nomenclature. I think that that's the court-friendly nomenclature. As the name states, it requires very close monitoring by attorneys. And that's why I think this approach has a place but it's not always used. I am not a big fan of it just because attorneys do not always have the time to be supervising custodians closely when it comes to document collection. And frankly, you know the realities of today's workplace does not always allow attorneys, and employees in general, for the required level of supervision. Employees work remotely and people are just in different places all the time, so it would be hard to have someone to sit by the custodian while they do the search and collection of files within their computers.

It can be appropriate on a case-by-case basis when you have a finite number of custodians, when you have sophisticated custodians that understand what you are trying to accomplish with your collection, when you have a limited number of issues in your matters. For example, a real estate matter with very defined issues, or a small employment matter, where custodians do not have a stake in the game. And it usually requires detailed instructions, technical practices and close attorney supervision, like I stated.

I think that if you are doing a attorney-guided custodian self-collection, you ought to provide very specific instructions. And this is not a one-size-fits-all. You can't only use attorney-guided custodian self collection. I think you have to have a mix of different processes, and to the extent that you can standardize your processes in a way that the only thing that you're leaving open to be decided on a case-by-case basis is your search criteria and date range, you're strengthening the defensibility of your process.

Again, I want you to understand that I am not saying that a one-size-fits-all approach is appropriate, but a few flavors that you can pick and choose from when collecting data can be very helpful. For instance, you can have a process for remote collection that defines exactly when you should use it, the tools that you have available to you when using this approach, how to deal with certain types of data. For instance when you collect compound files, do you collect

entire files and then process them after collection, or do you process them before? Do you eliminate system files? Do you collect entire TSPs and apply search terms later? It's very helpful if you can define that criteria from the knowledge and the expertise if you have a reason to do so. Then you can have a process for attorney-guided self-collection, like I described, that would say once you use it, the tools that you make available to your custodians to collect data, how to deal with specific data encountered, standard instructions for the custodians, and the supervision level required depending on the custodians involved as well as the issues of your litigation.

And lastly but not least, a process for forensic imaging. What vendors do you use, or what tools do you have in-house that they can make available [for] actual forensic collection, and how to deal with specific data. Are you going to collect deleted files or not? Are you going to collect systems files or not? So to the extent that you can put all of that in writing and just follow the steps for each type of collection, I think you're in good shape.

CRAIG CARPENTER: Great. Thanks, Julia. A couple comments that I'll make before we go to the next slide, and then Wendy, just a heads-up that there have been a number of questions with respect to ESI in the U.S. that is owned by foreign companies, and then vice-versa, U.S. companies with U.S. litigation that may involve data in foreign locales, and how we deal with that. So in the Q&A period we'll address that because, like I said, there have been a number of questions on that front.

But just to round out this slide, what we've seen—and I completely agree with everything Julia said, specifically with respect to forensic imaging—is that there have been a number of enterprises that have been applying forensic imaging approaches in a way that it wasn't originally meant to be applied. So the whole area of forensics is—it's a scientific body that is meant to recreate events, right? We've all seen CSI, etc. And oftentimes, for run-of-the-mill civil litigation, there are no allegations that anyone did anything fraudulent or anything like that. It's simply what happened when by whom and what can we show? In that context, a lot of these forensic imaging tools that they are being used are really kind of big hammers and clubs that really should give way to the scalpel, in the sense that all sorts of data is being collected, as Julia mentioned—system files, etc.,—that may not be relevant. And ultimately what that requires is (a) supervision by someone like Julia or someone on her team, (b) someone to actually go through and parse out the relevant data and then the data that should be kept and ultimately reviewed and potentially produced from the rest of the stuff that's garbage.

And then, third, additional cost and time with respect to going in and processing the data, because you have all sorts of files, oftentimes, like system files, etc., that really didn't need to be collected at all. But now they've been collected. There's going to be additional cost and time required to get them out of the collection, not to mention the fact that someone's going to have to spend their time and actually go through and do that. And now they're also on hold, so if perhaps an unrelated litigation may come up, stuff that may have been recycled otherwise, defensibly, has now been preserved, which is not a situation those who are in kind of serial litigation want to encounter. And that's, I think, the reason that we're seeing a lot of interest in the whole approach of targeted collection. Rather than imaging entire drives or entire PSTs, let's go into data both in the archive and perhaps on the exchange server, live data, and find surgically the stuff we need and the stuff that is of interest and relevant to a particular proceeding. Oftentimes that—well, it's almost always quicker, in terms of actually getting through the ECA process, but the costs can

oftentimes be lower, and actually ultimately result in better early case assessment because you're not going in and trying to analyze hundreds of gigabytes or terabytes of data. You have a smaller sample set, which obviously reduces the cost and timelines downstream from there.

So there's a whole—and apologies in advance; I think we're being overwhelmed by the number of questions we're getting, which is good, but we definitely want to hit this particular aspect of it, and I'll throw it over to Wendy first, and then we can move on to Julia.

With respect to “off-site data”— we won't deal with international data at this step, but we'll get to that in the Q&A—but data that's being hosted by a third party provider for any number of reasons, or e-mail that's being hosted, how do we handle this data and what advice do you give your clients in terms of approaching this whole area?

WENDY CURTIS: Sure. So let me just quickly give first a couple of tools I think would be helpful. Last year Judge Illston in the Northern District of California issued an order in the *Nursing Home Pension v. Oracle* case, and this is particularly helpful on two points. One, it gives a great insight along with the *Pension Committee* discussions, in the footnote about Rule 34, if you've read that decision, about the scope of how far your obligations for information that is not in your custody but arguably under your control. And I would look to those two cases.

I would also look to the *Nursing Home* case because of this—what I expect to see folks arguing—this broad obligation based on what was said in the *Pension Committee* [decision] about all employees. The *Nursing Home Pension* case has a great discussion that parties are asking for relief and sanctions argued that the distribution of the hold notice and the collection was not broad enough and that they didn't go to enough key players, and the court said that the moving party did not meet their evidentiary requirements to make a showing of why they needed more. So if you've got somebody pushing you on these points, I think there's some great language in that case to counter that.

And then—I am just going to try to talk fast here—we could talk for hours about the privacy point in international data, but there is a terrific decision that just came out of federal court in Utah—it's *Access Data Corporation v. Alste Technology*—and, again, that's out of Utah. It was issued on January 21<sup>st</sup> [2010], and again, it's the *Access Data Corp.* case. And that gives some interesting guidelines and insights as to the tension between the jurisdiction of U.S. courts versus the data privacy protections in the E.U. There is a lot of controversy about this decision as to whether the judge got it right, but it's a great case to read if you're trying to see the issues.

And then, to your question, Craig—and let me see how fast I can talk in our final minutes—is you think about custody and control. Again, this is a really broad interpretation that the courts are taking. If you can get it—if you could ask for it, from a third party and they would likely give it to you—then many courts are going to interpret that as having control over the data. As we move to more and more outsourcing models, to the cloud, to software as a service, as in-house counsel I really encourage you to work with your procurement folks and look at those contracts, in particular if you are a small company and you are outsourcing your e-mail, because that's where you have to preserve and that's where you have to collect. And so often we're under so many time pressures that if you can include in the terms of your contract how they are going to manage their information, how they're going to respond to your preservation requests, and how they're

going to respond to your collection, you're going to be better prepared for when litigation hits.

And then, again, as you think of all these, these are the pros and cons of moving your information outside from under the one roof. And so, you want to understand how that third party handles your information. Maybe they don't keep it permanently in the underlying system, but do they keep backups for years? If so, you need to address that in your contract as well, because if you think that you've got great records management and you're not keeping anything over the seven years, but come to find out the third party that manages your e-mail archives keeps all their back up for 10 years, what you thought you achieved has now been completely undermined.

So those are some high-level thoughts, Craig, how are we doing on time?

CRAIG CARPENTER: That's great, and I know we're under a time crunch here. So why don't—Julia, why don't you have any comments you have on this slide, and then we'll—we're going to skip the automation slide and just go to the release slide, because I think that's an important thing to want to cover. Obviously, with respect to any of this case law, or the technology or workflow of this, our contact information will be on the last slide, so feel free to contact any of us after the presentation is over, just because we're on a bit of a time crunch.

So, Julia, why don't you take any commentary you have here, and then we'll go to the release slide.

JULIA PEIXOTO-PETERS: Yes, I'll make one quick comment on this slide, and I think we touched a few relevant points here. Just following up on what Wendy stated earlier, that it's better to try to define roles and responsibilities in the contract with the third-party vendors, I have some experience with this in the context of outsourced IT operations. That's becoming more and more common. And I think one very helpful thing: You should define service level agreements with the vendor, including the criteria for compliance, based on acceptable levels of services. And you have generic language in the contract, but that's always something you can update on a yearly basis as you work with your vendor and you define what's working and what's not working, and revise those SLAs. And you're going to need to document the chain of custody very, very well, so when you have a third party managing your data, that's a requirement. As far as releases, you want me to talk about this now, Craig?

CRAIG CARPENTER: Yeah, exactly.

JULIA PEIXOTO-PETERS: OK, as far as release, particularly in my practice, in-house legal will give the green light for the release with outside counsel's consent. Obviously outside counsel is in the trenches doing the day-to-day work, so you need to understand whether litigation has reached the point where you can release the hold. And typically what will happen to the data is that the data collected [and] produced, has to be archived for a specific period of time, and preserved data can be released and can resume its ordinary life cycle based on the records retention policy. That's how we typically deal with the release of holds.

CRAIG CARPENTER: OK, great. Thanks. We'll just have some wrap up comments from each of us in the context of the Q&A.

[The CLE code and instructions provided here were for use only by attendees of the live webcast.]

CRAIG CARPENTER: So why don't we do this? We will do the question-and-answer session, but in the interest of those who might have a call at the top of the hour or a meeting of some sort, we'll put our contact information up here. First, I just want to remind everybody that Wendy has been kind enough to offer the case alert that she has authored on the *Pension Committee* case. So all you need to do is send her a quick e-mail. Her email address is here, as is the contact information for Julia and myself.

So why don't we—we'll start with you, Wendy, closing comments, and then, as I mentioned before, there were a number of questions with respect to data domiciled in the U.S. but owned by foreign corporations, and then U.S. corporations who are sued in the U.S. or investigated in the U.S. with data outside the U.S., in terms of how to deal with that. Obviously that's a huge, thorny field that we could spend a day or days talking about. But what are some high-level things or advice you might want to give clients?

WENDY CURTIS: Sure. On closing comments, on Julia's point about releasing the hold, don't forget data that's hosted by your vendor and your outside law firm, if they're hosting your review platform. Once the matter is closed, you want to get rid of all of that data so that it doesn't pose a risk in future litigation, assuming that it's not relevant and subject to preservation obligations in other cases.

On the, in particular, E.U. data privacy issues that, as you said [is] a topic in and of itself, but some practical tips. The first scenario that you described, Craig, was a non-U.S. corporation with data resident in the U.S., and that could be, I guess because they have a subsidiary here, they've outsourced here, or they've gone to the cloud and the cloud server is actually here in the United States. I think your average judge is going to say that he has jurisdiction over that data; it's here.

The second scenario now is when you have a company, U.S. or not, who is subject to U.S. litigation and some of the relevant data is in the E.U., and how do you reconcile your collection and production obligations against the E.U. data privacy requirements? And that's something that everybody struggles with, but one practical tip that I encourage folks to do is to reach out to your privacy officer if you have one. In particular, if you have a privacy officer for Europe or, in particular, some of the countries that even have tighter regulations within the E.U., they can be invaluable in helping you navigate this. And also to the extent that you decide to reach out to the regulator within the country within the E.U., they can help you manage that, also as you're evaluating vendors, depending on which—because it's not even once you're in the E.U., but then some of the countries within the E.U. have even more stringent requirements.

You're going to need to look at whether the vendor is going to move the data as part of the preservation and collection practice, or whether they can do the hosting and keep it within that country, because if it's through the Web and attorneys outside of that country are accessing the data through the Web, that's considered in essence a violation of the data privacy issues, and so that you want to be very cognizant of the movement of the data and who and how people are looking at things. Sedona also has a working group on data privacy, but I think the practical tips—unfortunately those guidelines aren't quite there yet. But those are some of the high-level

comments and tips I would give folks.

CRAIG CARPENTER: Great, thanks, Wendy. And Julia, any parting comments from you?

JULIA PEIXOTO-PETERS: Yes, I just want to comment briefly on this topic because, like you said, it's a topic on its own. I'm sure we could spend an hour here talking about data privacy, but one of the things that I find helpful is that there is really no way to reconcile e-discovery obligations with European data privacy obligations at this point. So to the extent that you can ask earlier and try to be proactive when your business decisions are being made as to whether to allocate data in the U.S. or the European Union, then I would encourage you to act swiftly when those decisions are being made. Just to try to avoid the issue altogether until more clear guidelines have been issued.

And just a final comment. It has now been three years since the amendment to the Federal Rules of Civil Procedure, and I think that companies did not have much time to plan and prep their internal processes when this amendment came out. Most companies have been going through the motions in answering requests for production to the best of their abilities without taking the time to strategize. So what I see is a trend, and it's a good one, in companies taking a step back and looking at the big picture. And ECA is a big part of that trend. The goal is really to assess your overall e-discovery process, identify gaps, and take the time to close those gaps. I think that an assessment of the entire process—the entire e-discovery process—is a very worthwhile investment.

CRAIG CARPENTER: Great. Thanks, Julia. So apologies in advance. There are a number of questions we weren't able to get to. We are more than happy to follow up with each of you as appropriate. Our contact information is still on the screen. Feel free to just drop any or all of us, actually, a message and we'd be happy to kind of follow up with you offline.

The only thing I would add before I turn it over to Amar is just to be aware that the technology is there in certain situations to help you. As Julia and Wendy have talked about, understanding the workflow and the processes and the IT systems are the most important aspects of it. Once you have a handle on that and how that works, using technology to really do the heavy lifting in a quick, cost-effective fashion can help you find the relevant data you're looking for and the relevant custodians and where things are, and work through early case assessment before you've really spent any money, and then maybe even doing your processing in-house and things like that can really save you a lot of money and actually can corroborate the consistency and replicability of your systems. But obviously you need to understand your systems first; that's the most important aspect.

So let me turn it over to Amar, and in the process I'd like to thank all of you for coming, and thank our speakers for today's webinar.

AMAR SARWAL: Wow. What an incredibly informative program. I really hope all the listeners benefited as much as I did from Craig, Wendy and Julia's excellent presentation. We look forward to hearing back from them again as these issues develop.

To all the listeners, we would love if you could fill out the evaluation form as we really value your feedback. And on behalf of the Association of Corporate Counsel and its Litigation

Committee, we wish you the best of luck. Thanks, and I'll turn this over to Marni.

MARNI CENTOR: Thanks, Amar. On behalf of the Association of Corporate Counsel and SmartPros Legal & Ethics, thank you again for listening to today's program.

*[The CLE code and instructions provided here were for use only by attendees of the live webcast.]*

Thank you again, and have a great day.