



Effectively Managing eDiscovery in a Globalized Marketplace

A roundtable discussion with Epiq Systems



**DAILY
REPORT**
An incisivemedia publication

2008 SPONSORED ROUNDTABLE SECTION

SPONSORED SECTION

The Panelists:**Jon Neiditz**

*Partner, Nelson Mullins
Riley & Scarborough*

**Jonathan Soll**

Georgia-Pacific

**Hope Haslam**

Epiq Systems

**Michael J. Kline**

The Coca-Cola Co.

**Jim Jordan**

Moderator

About The Sponsor:

EPIQ SYSTEMS is a leading provider of integrated technology products and services for the legal profession. Its software applications and Web-based platforms offer case management and document management solutions for electronic discovery, legal notification, claims administration and controlled disbursement.

SPONSORED SECTION



ZACHARY D. PORTER/DAILY REPORT

The roundtable was comprised of legal privacy experts. Pictured from the left: Moderator Jim Jordan, Jon Neiditz, Jonathan Soll, Michael Kline and Hope Haslam.

Panel parses hypothetical international privacy quagmire

What if you opened your morning newspaper to a story that reported adverse—not to mention supernatural and destructive—side effects as the result of consuming a food product manufactured by a foreign subsidiary of a locally based international conglomerate? And what if several weeks later, that same international company were served with a product liability lawsuit along with lengthy and extreme discovery demands? And what if the privacy laws in the country of manufacture were strict, making it nearly impossible to obtain some of the discovery requested?

And what if you were that company's general counsel?

That's the scenario deliberated by a panel of privacy experts convened by Epiq Systems for a roundtable discussion on managing e-discovery across borders.

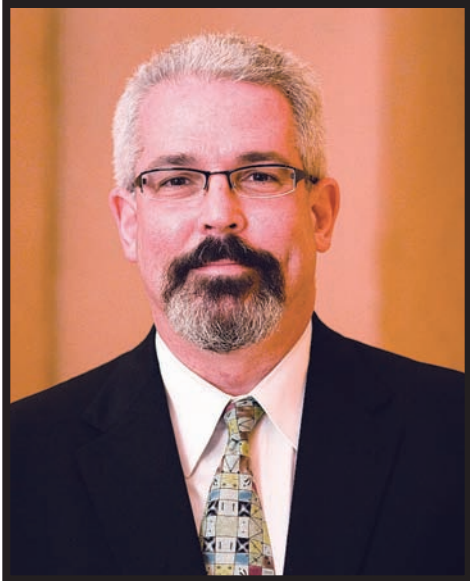
The discussion was moderated by Jim Jordan, chief privacy officer for Brookfield, Wisc.-based Fiserv.

Also on the panel were Michael J. Kline, senior litigation counsel—intellectual property for The Coca-Cola Co.; Jonathan Soll, chief privacy officer and chief counsel for information technology for Georgia-Pacific; Jon Neiditz, co-leader of Nelson Mullins Riley & Scarborough's information management practice; and Hope Haslam, director of consulting services for sponsoring company Epiq Systems.

Among the topics discussed: the differences between U.S. and EU discovery requirements, the reasons for the differences and the subsequent consequences.

The views expressed in the following transcript do not necessarily reflect the opinions of the companies or firms the experts represent. Rather, they are personal opinions. In some cases, the transcript was edited for clarity and brevity.

SPONSORED SECTION



Jon Neiditz

Partner, Nelson Mullins
Riley & Scarborough

Jon Neiditz is co-leader of Nelson Mullins Riley & Scarborough's information management practice. He is a partner in the firm's Atlanta office where he focuses on the legal and technological challenges of electronically stored information—including managing risks and costs of e-discovery, developing and implementing records management programs, and preventing information leakage and privacy issues. He has represented many clients in connection with breaches of information security and across a very wide range of other privacy matters. He also has assisted those clients in transitioning the role of in-house counsel to include control of electronic information, combining legal with organizational consulting services and drawing on his background as a national consulting practice leader for a Big 4 firm.

JORDAN: The market place for U.S. businesses has become increasingly globalized and many companies are now operating both in the U.S. and other countries. Many of your clients probably are as well. These companies can encounter significant challenges where there are conflicts between the laws and the different jurisdictions in which they operate. One example is the conflict between the discovery rules in the U.S. and laws in other countries, particularly privacy laws, labor laws and blocking statutes, particularly in the European Union.

For example, let's consider the following hypothetical. You are the in-house litigation counsel for Hulk Foods Inc. a U.S. corporation headquartered in Atlanta that sells ground beef prepared in a meat packing plant in Germany by a subsidiary corporation established there, Hulk Foods GmbH. One day a story appears in an Atlanta newspaper reporting that Stan Lee, a local Atlanta resident, ate some ground beef believed to be sold by Hulk Foods Inc. and within minutes transformed into a green, 20-foot-tall bodybuilder and rampaged in that condition for several hours across the Atlanta area, stealing a pair of size 52 purple shorts from the Falcons' locker room, taking a swim in the Georgia Aquarium and just generally being rude and using bad grammar. He returned to normal only after consuming several kegs of beer at Turner Field.

Several weeks later Hulk Foods is served with a product liability lawsuit that has been filed in the Northern District of Georgia Federal Court in which attorneys representing Mr. Lee and his wife allege that his condition was, in fact, caused by ground beef from Hulk Foods and has caused substantial emotional distress to both Mr. and Mrs. Lee in addition to a large bill for property damage.

The complaint further alleges that the plaintiffs have laboratory results showing that the ground beef contained a radioactive virus that upon information and belief may have come from the cattle, or even one of the meat packing plant workers. The complaint is accompanied by discovery requests, including a request that the personnel working in the meat packing plant all be subjected to radiological and DNA testing to determine if they carry the virus.

The plaintiffs also want all e-mail messages sent by or to the employees in the plant for the last two years in addition to extensive information from personnel files.

Your local counsel in Germany tells you that the German privacy laws are quite strict and obtaining all this personal data lawfully will be nearly impossible. The human resources representative in Germany tells you that the employees in the plant have never been given notice that information of this breadth might be collected and have also never been given notice that their e-mails and information already in their personnel file would be used for litigation purposes.

To make matters even more challenging, the workers are represented by a works council and there is a shop agreement in place with the works council that strictly limits how employee information will be used and that is even more restrictive than the German privacy laws. The works council is also hostile to the company right now due to recent downsizings at the plant.

Let's start with Michael. Given this set of circumstances and this extensive discovery request, what are you, as the in-house counsel for Hulk Foods, going to be faced with in the terms of challenges and difficulties?

KLINE: For starters, as in-house counsel for Hulk Foods there's a reason why I have all this gray hair. It sounds like I'm about to get quite a few more gray hairs.

As an in-house litigation counsel, I've got a million things already on my plate to worry about. It may surprise you to learn that German privacy law is not high on my list. I probably manage a half dozen cases, maybe more. I've got a million other things to do, separate and apart from being a lawyer for a large multinational company. I

am a lawyer with no associates. So in many ways it's just me to solve all these legal problems.

So what do I worry about? Well, the scenario that you just heard for a company like mine is an absolute public relations nightmare. What we have is a food company that has sold contaminated food presumably that has caused some very unusual symptoms in an individual and worst of all it's happened in my hometown where my company is headquartered. It really doesn't get any worse than that.

So one of the first things I need to do is draft an appropriate media response. But before I can even do that, I need to develop an action plan, because when I talk to the media they're going to want to know what do you plan to do to fix this problem.

JORDAN: Michael, let me interrupt you for just a second. The way the hypo is set up there is first a newspaper article that reports that this event has occurred, and then later there is a lawsuit filed that you're served with. During that period in between would you do some sort of internal document freeze or document hold order or would you wait until you actually got the lawsuit?

KLINE: You know that's a great question. It really depends on the circumstances of the case. The way this one is playing out a document retention notice is probably one of the last things on my list because things are going to be happening fast and furious. I've got media calling. I've got business people calling. I probably have the CEO calling at this point. And so it's really a matter of all hands on deck, start bailing.

Unfortunately the document retention notice is probably going to have to wait. In other cases, though, where the facts are not quite as severe as they are here, and things are a little bit more relaxed, I would always tend to err on the side of issuing that document retention notice earlier rather than later because I'd rather not get into a situation where I'm second guessed at some point by a judge in response to a motion to compel or a motion for sanctions that I was not sufficiently proactive in preserving documents.

So back to my action plan. First of all I'm going to sit down and I'm going to do something that we refer to as early case assessment. I've heard it referred to as other things but really it's just taking a very quick snapshot of what happened, where we are, what we need to do, what's our likely exposure, what's our likely risk. I determine the scope of the problem. I might possibly implement a product recall. And it sounds like in this case that's probably going to be an issue. And I'm certainly going to want to give the public notice if this is not an isolated problem that they need to be careful about what they're consuming.

I'm going to notify my insurance carrier. I'm going to start developing safeguards to ensure that this never happens again. I'm going to look for other parties. There might be other parties that either supplied the ground beef, there might be some other suppliers. I might have an indemnity and, if so, I want to verify that.

In this case in particular I'm going to be proactive in seeking out government agencies, whether it be the FDA, whether it be my state attorney general, whether it be several state attorneys general because I want to be in their office before they're in mine. So that's another one of those things that probably keeps me from immediately thinking about a document retention hold notice.

Only after all this is done, and this may take anywhere from a few hours to a few days to a few weeks, do I really have time to sit back and think about how am I going to manage this litigation. Now once I do that—we don't know from the hypothetical exactly how many employees Hulk Foods has, but let's assume they've got thousands. I need to identify the employees who are going to have the most relevant documents and possess the most relevant information. Finally, I'm going to send out my

SPONSORED SECTION

document retention hold notice.

I notice in the hypothetical that we're asked to go back two years for producing documents. I can't speak for Hulk Foods but for many companies two years is unrealistic because of the volume of e-mail and because of the disruptiveness that document retention can have to the business and because of storage space constraints. Many companies are going to a shortened period of time for retaining e-mails. Six months is not unusual. And so if Hulk Foods has a six-month document retention policy for e-mails they're already not in compliance with the document request going back two years. So I want to try and manage that right out of the box.

Somewhere around this time it's going to dawn on me that there is an EU privacy issue. It's not my area of expertise and so I'm really going to be somewhat out of my element on it and I'm going to be relying by necessity on experts, outside counsel, vendors that can help me navigate the choppy waters.

JORDAN: I'd say you make the top 10 percent of in-house counsel by even recognizing that there was a privacy issue.

KLINE: What I really want to do is I want to have it all. I want my company to fully comply with all U.S. laws, all U.S. discovery requirements and I want my company to fully comply with all German privacy laws. Most important, I want to make sure that we produce everything that we must produce and that we not produce anything that we must not produce. I don't want to produce anything that's privileged. I don't want to produce anything that's trade secret and, last of all, I certainly don't want to be sanctioned for having inadvertently destroyed relevant documents.

So your hypothetical creates a conflict between U.S. and German law. And I guess the question is: can I have it all?

JORDAN: Well, Jonathan, can you tell us a bit about what this privacy issue in Germany is all about? Why is there a conflict there?

Sure, Jim. I think the first thing I'd do is sit down with Mike and thank him for coming to me. Many litigators that I know don't know that much about privacy law. I'd want to tell him what personal data means in the context of Germany and most of the EU and ask if he really needs personal data to respond to discovery. In this fact pattern, it appears clear that it's relevant, so I'd walk him through an analysis.

Personal data generally is about an identified individual, personal data, social insurance number, name, personal cell phone, e-mail. Certainly the types of data in this hypothetical—blood, blood test, medical results—that would be absolutely personal data. It could even rise to the level of something different called sensitive data, for which the laws afford very strict rules on collection and transfer. And if you have to collect personal data, I'd ask whether there's any way that it would be acceptable to opposing counsel or the U.S. court if we make the personal data anonymous, such as using Smith and Jones in place of real names. I would want to help him understand that the EU really cares about this stuff because in World War II the Nazis and their allies used people's personal information on religion, political affiliation and other data to get to them. And so throughout the EU the ownership of one's personal data is considered to be a fundamental human right. This is something that the EU and member countries are very serious about.

Once I finished the background, I would do a bit of review into which specific laws might me a problem for us in Germany to collect the data and then to transfer it to the U.S. to produce in a lawsuit. And here there are two different areas of law, privacy law and employment laws. In the privacy realm, the relevant laws come from laws in Germany that may cover sensitive data or medical data. The other area is employment law and I should say I'm not an employment lawyer, but I know enough about those laws to get by and to know when to pull an employment lawyer into the loop. In Germany, the relevant body in the employment law area is called the works counsel, which can act as a labor union.

Works counsels are not the same in every country in the EU and some don't have them. Works counsels may engage in collective bargaining, and in many cases you have to go to them before you do certain things and get their consent. You might simply have to inform them, or you might need their input and consent. In some cases, they may refuse to consent and refer your issue to a higher body called the labor inspector. You might also need the consent of the individual whose data you're going to collect and transfer.

Assuming you can get past the consent issue, and assuming your company already filed documentation and received the works counsel consent, you'd still have to determine if there's an employment contract with the relevant employees and determine whether that prohibits you from collecting the information.

JORDAN: Let me just propose this, though. Let's not assume from the hypothetical that we have to produce all this. Wouldn't you want to maybe first file a motion for protective order and try to see if we can get out of having to file some of this and turn the Germany privacy law perhaps in our favor rather than something that works against us?

SOLL: Absolutely. Mike can speak to that.

KLINE: This is not one big company against another big company where you have in discovery potential for mutually assured destruction, that is, where if the other side asks for something unreasonable from me I can turn right around and ask for something unreasonable from them.

This is a hypothetical in which we've got an individual in all likelihood against a huge company and he can ask for the world in terms of documents. There's very little we can ask for in return. So I'm not sure at what point we file for a protective order. I think the first step we would take typically would be to try to negotiate with the other side with their attorneys. I can tell you from experience, the last thing you want to do is bother a federal judge or a state judge for that matter with discovery disputes. They're busy and they don't want to be bothered with it. So the preferred course for us is going to be trying to negotiate something with the other side.

SOLL: You can try to negotiate something with opposing counsel that says we're going to produce this personal data but in the first pass we're going to produce anonymous data. The e-mails or documents will say what happened, what the facts are, but won't have the people's names. Then you're not actually collecting personal data. I'd imagine this may be hard to negotiate unless the personal data is really relevant.

JORDAN: Wasn't there a situation a couple of years ago where the whistle blowing hotline requirements of U.S. law ran afoul of European privacy laws?

That's exactly what happened, and the French government—the CNIL actually—had to introduce new rules to address the problem. Now in France it is possible to have a hotline in certain circumstances if you comply with the rules. So let's assume that you can get over the hurdle of collecting the personal data. Now you still have to transfer it to the U.S.

That represents a whole different set of problems because within the EU you can transfer personal data in some cases fairly freely between EU member countries. But you can't transfer it to countries that don't have adequate data protection laws. And the EU has deemed that the U.S. doesn't have an adequate personal data protection scheme.

So now you have another problem. You have to have a special legal basis to get the data. One is consent of the individual, which sounds great except that people can say no, or they may say yes and withdraw it later on. And if you're an employer asking for consent from the employee under the European labor laws it may be considered coerced and therefore not valid consent.

Another legal basis is called the Safe Harbor. This is a voluntary program that was set up by the Federal Trade Commission and Department of Commerce. It was a negotiated



Jonathan Soll

Georgia-Pacific

Jonathan Soll is chief privacy officer and chief counsel for information technology at Georgia-Pacific. He oversees worldwide privacy compliance and management of the company's IT law group including complex legal matters—those related to software licensing, outsourcing, e-commerce, telecommunications and IT legal aspects of acquisitions and divestitures. Before joining Georgia-Pacific in 1997, he was in-house at WORLDSPAN, and was previously associated with Schnader, Harrison, Segal & Lewis in Atlanta and Davis & Weil in New York. He is a frequent speaker and has published articles on IT legal topics such as software licensing, electronic data risk management, creating e-mail use and retention policies, and electronic monitoring. He graduated from New York's Hofstra University School of Law in 1991.

SPONSORED SECTION



Hope Haslam
Epiq Systems

Hope Haslam is director of consulting services for Epiq Systems, where she focuses on litigation readiness planning and forensic/collection services. Previously, she was director of client services for Merrill Corp., managing a team of consultants in Texas, Colorado and California. She founded Merrill's national CLE program and established its Forensic Services Group. Immediately prior, she was vice president of business development for Engenium Corp., a creator of LSA-based conceptual search engine technology. She received her B.A. in communications from Baylor University in 1987 and graduated from Mississippi College School of Law in 1991. She has written several CLE courses, exploring topics such as drafting electronic discovery response plans and analyzing the 2006 amendments to the Federal Rules of Civil Procedure. She also has led several panel discussions on legal technology.

program between the U.S. and the EU where U.S. companies can join voluntarily and if they agree to follow certain principals of data protection they can then transfer personal data into the U.S. To join, you have to self-certify that you comply with certain data protection principles, which means you have to do quite a bit of due diligence on what personal data you collect from the EU, where it goes, whether and how it's protected, give people notice of any collections and the choice to not participate. For large companies, it can take quite a bit of time to figure it all out.

As far as I know there hasn't been any enforcement of actions by the Department of Commerce against U.S. companies for Safe Harbor violations, but I could be wrong. But because joining the Safe Harbor gives you a legal basis to transfer personal data from the EU, you might consider pre-emptively joining. Again, you have to do internal due diligence to figure out if you can be compliant, so it's not as simple as just joining. Also, it's not a panacea since it doesn't help comply with collection rules in the EU, but it helps show your company's dedication to privacy.

JORDAN: I think somebody in the company has to swear upon penalty of being thrown in jail that they are actually following all the rules.

SOLL: That's right. In our case, it's me. Another basis is called the model contracts. These are pre-negotiated contract forms between European and U.S. legal entities that address the transfer of data. But again, you are agreeing to be bound by a certain set of obligations about personal data, so you have to be fairly certain that you can take on those obligations.

JORDAN: OK. What do we think about the idea of avoiding all this transfer across the border stuff entirely by just producing the data in Germany? Should we go to the court and ask that we be allowed to do that because it's going to be too legally difficult to move the data to the United States?

KLINE: I don't anticipate a very receptive audience from a court in Germany for a number of reasons, not the least of which there is no discovery in Germany.

JORDAN: What I'm saying is to ask the U.S. court whether discovery that's being sought in the U.S. court can be produced to the plaintiff's counsel in Germany.

KLINE: Same issue. I would question whether the U.S. court has the authority to demand production in Germany. And if the U.S. court renders an order that on its face would violate German law I've got problems with that, too.

JORDAN: Well, wouldn't they really just be limiting the responsibility of the defendant under U.S. discovery law by saying that you have to produce it but you don't have to produce it here?

KLINE: If it's being produced contrary to German law it doesn't really matter in my view where that—

JORDAN: Well, no, what I'm saying is that in addition to the production of the data being a problem under the Germany privacy law, the transfer of the data across national borders was a problem under Germany Privacy law. And I was suggesting that maybe we could try to solve that problem by never transferring it across the border, simply produce it locally.

KLINE: To me that's a nifty dodge. Are you going to try the case in Germany? Because somebody is going to have to come back to the U.S. with that information.

SOLL: But I'd also say, if I can chime in here, if you can pull that off if you, the plaintiff and his or her counsel go to Germany and fly back with the personal it may also be considered a transfer. I think the German data privacy authorities might have an issue with that.

JORDAN: Well, Jon, what would you have to add to that? Are there some issues here that we haven't talked about?

NEIDITZ: Well, let me just mention a few that are

worth noting and then what I would like to do is to take these two different worlds that you've heard about from Michael and Jonathan and give you a very concrete protocol that tries to bring them together.

First of all, in addition to privacy issues, there are also country-specific blocking statutes that we are not emphasizing in this discussion.

Second, there are some big sleeper issues. For example, I speak to e-discovery audiences on an almost weekly basis. And I very often ask all the lawyers in the audience, "how many of you have ever lifted a litigation hold?" And very often nobody raises their hands. So we're talking about information stores that are all over the place. Terabytes of data. Do you think anyone is getting unauthorized access to those databases, ever? Are you aware of the 44 state laws that require notification of the people whose personal information was shared when unauthorized access was given, and is anyone thinking about what would happen to a law firm if it had to give that notification? So there's an example of privacy laws in relation to e-discovery right at home that I just want to throw out for your consideration.

But now let me get to an approach to e-discovery in this hypothetical. First I'm going to talk about pre-dispute measures that can be taken. Then I'm going to talk about the very difficult period of when you're in reasonable anticipation of litigation. And finally, I'm going to talk about discovery issues once discovery has been initiated.

Before the dispute there are some things that organizations can do that put them in a better position when dealing with this kind of dispute in Germany. It wouldn't solve the problem with this very sensitive type of personal information that Jim has put in the hypothetical but it would put you in good shape when it comes to the kind of e-mail production disputes that most of us are dealing with all the time from Europe these days. It's important for U.S. organizations to recognize that if they've got EU employees, their obligations as an employer are different in Europe than they are here, and employee policies should be different in some respects.

One respect that they can be different is you can have policies that show deference to the letter and spirit of the data protection laws. So you can have a corporate investigations policy, for example, in Germany, that focuses on proportionality and balance between the needs of the corporation and the needs or rights of the individual under European law.

You can get that investigations policy approved by a works council. Very often you can't get in front of the works council once litigation commences, but you can get that policy approved in advance.

Another idea you might consider is putting personal folders into your EU e-mail systems. Some U.S. information security people really hate that idea. A controversial idea but a useful one to e-discovery. The other thing you can do in advance is you can get contracts ready. Jonathan talked about the model contracts. You can certainly get those in place within your company. You can also get contracts with your major vendor relationships that are involved in running your business.

SOLL: Especially the vendors who may be assisting you in the e-discovery where the consultants and data collectors those are critical.

NEIDITZ: And in those agreements you establish whether the vendor or corporate entity is in a processor or controller role. You have data protection provisions, you have security provisions and you have indemnification wherever you can get it because there's no perfect answer here. This is the kind of legal conflict that will have to be worked out between governments as the Safe Harbor was but for now we've just got to do the best we can. Of course, you can also deal with Safe Harbor certification before the dispute. Now let's get to the most sensitive period in terms of this interaction between the two legal

SPONSORED SECTION

systems.

HASLAM: Talking a little bit about the service provider selection process, there are several questions that you need to ask yourself and your outside counsel in terms of identifying that service provider. One is, of course, do they have knowledge sufficient knowledge in the data privacy laws and blocking statutes of that particular country? Secondly, if they have that skill set are they located in the EU or in the foreign jurisdiction? Having your service provider located in that country can save you a lot of time and a lot of expense in travel costs. If you can't find a provider in Germany, say, consider one in a neighboring country like Switzerland or even London that also has the ability to store the data and allow you to review it from servers located there.

Having that skill set and having the knowledge is an important first step. Thirdly, ask if they have collected and processed data in that country as well. This is important because having an understanding of the laws of that country, some effect what kind of hardware can be carried in and out of that country, knowing these laws can play a big part in the success and the cost of this phase of the project. I am thinking of France where you have to be very, very careful in staying within the confines of their criminal statutes because there are certain things they will not let you bring in or take out. Making sure that they understand how broadly the processing statutes are construed in Germany, and they're very broad. What does that constitute, you know, how to say within the confines of these individual state laws. Are they Safe Harbor certified? We are one of the few service providers who is certified. To their point it's a nice step to have. Having that Safe Harbor certification is important and very helpful.

The other thing is being sure that you hire a service provider who has testimony experience, who has written affidavits in that country, can help you with inaccessibility designations, and cost estimates to support of inaccessibility designations.

NEIDITZ: Great points, Hope. Back on the pre-litigation period, the reason that the period when you're in reasonable anticipation of litigation is the most difficult when dealing with EU is because that's an area of U.S. law that really hasn't made it there yet. Therefore, the idea of the importance of responding to U.S. discovery is tough enough but the idea of preservation in connection with a reasonably anticipated but not pending dispute is particularly challenging in Europe.

SOLL: And we should say we're talking about the preservation of personal data. If it doesn't involve personal data we don't have to worry about it from a data privacy perspective.

NEIDITZ: Right, if we're talking about data that's not personal data then we're in the clear. But the data that we're talking about is very personal, so we need to come up with some legal basis for processing and we can anticipate that basis in these two weeks that we have after the things hit the paper. And in this the particular case we actually have a clear basis that we're going to try, which is the public necessity, public health basis found in the EU Directive and German law; you've got some real possibility that other people are going to turn green and grow, so you've got a compelling case.

At this point you want to make a decision though. Are you going to go to the data protection authorities and begin to talk with them about this during this period or are you going to try to do everything right so you've got a good story to tell, including everything that you've done beforehand and then be ready to tell that story if and when things come to their attention?

For most companies, it's going to be the latter approach, just because when you're dealing with works councils you really don't know what the outcome will be.

SOLL: And you wouldn't necessarily ask for a special meeting of the works counsel. They usually meet about monthly. We should also add that you may have to go to

one or more German regional works councils for each of the regions where your company does business in a country and a central one as well.

NEIDITZ: Right. So are you going to commence the investigation at this point? Are you going to commence preservation? Typically, you figure out your best basis and you begin to preserve at this point.

Now the litigation is commenced. There are certain things you always have to do. One is you never hide anything once the litigation has commenced. I mean you don't want to bother federal judges with discovery disputes but on the other hand there's a large group of federal magistrate judges who love talking about discovery disputes, and if you happen to have one of those you're certainly going to be very transparent.

KLINE: Absolutely. The last thing I ever want to do whether it's an Article III judge or a magistrate judge is lose any measure of credibility with them or with the process. I want to present my company as a company that wants to do the right thing, wants to comply with all the rules, all the regulations, all the local rules of the court and all the discovery rules.

NEIDITZ: And the other thing you always want to do is aim for narrowly tailored e-discovery, particularly when it involves the EU. The big problem that everybody with e-discovery systems is facing is over-collection. You want to be able to refine your search criteria as much as you can.

So you need to determine the legal basis and we've talked about consent. In this case with sensitive data it needs to be very explicit consent. Of course, if you can present things in an anonymized way then have you no issue.

JORDAN: Let's clarify what "anonymize" means. What would you have to do to the data?

NEIDITZ: You have to render data such that no one is identifiable.

JORDAN: For example, if they were asking for some of the illness records you could maybe identify Employee 1, Employee 2, Employee 3.

NEIDITZ: Right. There are also some mixed models here. So perhaps you have anonymization in open court combined with in camera review by the judge. Protective orders have been mentioned a number of times.

Fundamentally, you look for what they call in Europe a derogation. In this case public necessity is the one that you're going to push on. And then after you determine the legal basis for processing you have to develop the legal basis for transfer, although you've also got the option of in-country review and processing as a possibility. The processing still needs to have a legal basis but you can deal with the transfer issue that way. You can use Safe Harbor. It works well in this hypothetical because we're not talking about moving the data to India from the U.S. afterwards. It's in the U.S. And at that point it can come out in open court. Clearly when your basis for transfer is model contracts use of the document in local court is more problematic because you don't have the ability to share the information forward without some kind of agreement with the other side or a protective order. So a protective order in combination with model contracts, again, is workable.

And while you're doing all this, you need to protect yourself in the U.S. court. I don't know if anyone has been using the new Section 26(b)(2)(B), which is the section of the Amended Rules of Civil Procedure that allows you to resist producing if electronically stored information is not reasonably accessible due to undue burden or cost. Very often we could be seeing situations of this sort. I just worked with the Sedona Conference on an article on interpreting that clause. But there is also 26(b)(2)(C) and 26(b)(2)(C) is what 26(b)(2)(B) returns to once it's challenged by the other side. 26(b)(2)(C) limits discovery when the burden or expense of the proposed discovery outweighs it's likely benefit considering the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake and the importance of the discovery resolving the issue.



Michael J. Kline

The Coca-Cola Co.

Michael J. Kline is senior litigation counsel—intellectual property for The Coca-Cola Co., managing worldwide IP litigation matters including pre-litigation analysis, ongoing litigation and mediation, negotiating dispute settlements and performing strategic IP business analysis. Prior to joining the company in 1999, he founded and chaired the IP department at Thorp, Reed & Armstrong in Pittsburgh, Pa. In private practice, he served as chief outside IP counsel for Sunbeam Corp. and litigated patent and trademark matters in federal district and appellate courts. He earned his J.D., cum laude, from The University of Pittsburgh School of Law and his B.S. in chemical engineering from The Pennsylvania State University. Some may recall him as a lawyer on hidden camera in a national television commercial for Coca-Cola Zero.

SPONSORED SECTION



Jim Jordan

Chief Privacy Officer, Fiserv

Jim Jordan earned his B.S. and law degrees from the University of Georgia and served seven years active duty as a Navy nuclear submarine officer. He practiced 11 years in law firms, including six years at Alston & Bird where he was among the first Internet law practitioners in the early 1990s. He worked an additional nine years as in-house counsel, including six years with the General Electric Co. where he was among the first chief privacy officers in the nation. He was a drafter of the original certification examination for privacy professionals seeing CIPP certification from the International Association of Privacy Professionals. He is chief privacy officer of Fiserv Inc., a Fortune 500 company and the world's largest provider of e-commerce and information technology services to the financial services industry.

I am not suggesting for a second that these provisions would work in this hypothetical, but the broader question is whether courts will establish some reasonableness-based precedents in this context.

SOLL: I want to bolster something Hope said earlier. One of the questions I would ask Mike if he came to me is, "do you already have a vendor and is the vendor going to help you with the collection?" And, "who is going to move the information from Germany to the U.S.?" And does the vendor have has experience in Germany, with German privacy laws, do they know data protection authorities, do they understands how the works council works? And then, are they a member of the Safe Harbor. I want to stress that it's important for them to be a member of the Safe Harbor if vendor is the one transferring the data. This helps you if you're questioned later by the data protection authorities because it becomes part of your whole compliance story. You would then at least be able to tell the German authorities, here are all of the things we did.

NEIDITZ: There are big differences in vendors in the minds of regulators. Regulators are likely to think that there are good-guy technologies and good-guy vendors and bad-guy vendors. Those judgments are made based on experience, not necessarily on comprehensive surveys.

SOLL: in the vendor bidding process, you want to ask about the technologies the vendor has, and whether they're in the Safe Harbor.

HASLAM: Exactly.

SOLL: How sophisticated it is and how automated it is and how much personal interaction you need with the technology to use it. And I think the less the people have to do the filtering and key words, the better. If the computer looks at personal data instead of a person, to render the data anonymous or to avoid personal data collections if possible, there may be no conflict with data protection laws. It's if the people look at the personal data then it becomes a problem.

JORDAN: Well, Michael, you've heard all of this advice. Is it now clear what you need to do?

KLINE: One thing that occurs to me because this is just part of my world is that I'm going to need witnesses because I'm going to be served with deposition notices. And in all likelihood I'm going to get, as litigators well know, a 30(b)(6) deposition notice for someone who is able to testify on the category of my document retention and production policies and procedures. And I know I'm not going to be that witness. The question I have is would my vendor be that witness and what are the pros and cons of doing that.

KLINE: And for those of you who don't know what a 30(b)(6) witness is, that's a witness that is designated by my company to speak on behalf of my company. So whatever they say binds my company.

HASLAM: I hate to give this answer but it depends really on the litigation and the amount in controversy. For example, if the key issue is about the collection of the data or its about the process by which a cost estimate was created for an inaccessibility designation then the service provider's expert should be more than capable of testifying on behalf of the company.

NEIDITZ: I've had the opposite experience with a lot of companies. My role is often to try to get in and help the company avoid excessive discovery costs. So I work with a lot of companies where they see these 30(b)(6) witnesses having to get completely up to speed all over again, if they're coming from outside, because the information systems are always changing.

KLINE: Yeah, there are a lot of risks. I mean there are practical limitations though on a 30 (b)(6) witness. It's a given that this person is not a walking encyclopedia. But you have to do the best you can. And so maybe a good middle ground would be for a company employee that at least knows something about document retention

procedures to be trained and brought to speed by people like yourselves who are truly the experts.

Another question that I have relates to just a fact witness. In the hypothetical that we have we've got employees that presumably carry this virus. And if I'm plaintiff's counsel I'm going to want to depose one or more of these people. Now we talked about anonymizing the data. Now the question I have is can you anonymize the witness? And one of the ways that you could do that is with the screen or voice disguising techniques. Have you experienced that sort of thing?

JORDAN: If they were to agree to do a telephone deposition, other than doing some sort of voice print I'm not sure how they would know who they were questioning.

SOLL: If the person is going to testify in a way that's adverse to the company then you worry about other things like whistleblower laws in Germany, so you're adding layers of complexity.

JORDAN: Once you get to the point, though, where you have a potential public health problem in Germany you may be able to go and get compulsory testimony under German law. It adds another layer of complication to it, but that's another way of going about it.

SOLL: And your best bet there may be if it's really a public health issue asking for help from a U.S. regulator. Maybe they can step in with the German data protection authorities and enter into some kind of agreement.

I want to raise one more thing. I think in our hypothetical the German operation is a German subsidiary of the Atlanta-based company; is that correct?

JORDAN: Yes.

SOLL: OK. Let's say the same meat packing operation was actually your vendor. They produce meat for you but they're not you. Then I think the analysis on the privacy laws doesn't become a whole lot different. But one of the things you can do in advance is when you're entering into the contract with that company to produce meat for you in that contract you try to put in place language that encourages or requires cooperation in the event of litigation. They'd be hard pressed to agree to give you personal data because it would be potentially in violation of European data protection laws for which they can be fined But I think you can at least get their reasonable cooperation. I mean you can identify somebody there that becomes your privacy point person if this comes up. You can also try to require them to join the Safe Harbor or enter into model contracts between their EU subs and your US entity.

JORDAN: There is always an issue that comes up when you have someone who is processing data on your behalf who is the controller and the processor under European law because those are loaded terms. And the controller is the entity that has the primary legal liability and who gets to make the discretionary decisions about what happens to the data.

Most vendors would like to be a processor. They like to have it very clear in the contract that they're just doing what you tell them to do and you're the one with the liability.

One thing I would like to point out from real life is that there actually has been at least one case in Texas in 1995 in which the defendant was asked to produce the corporate phone book of all the employees, which included German employees. And they raised the defense of German privacy law. They brought in an expert to testify that this would violate German privacy law and, in fact, they got a protective order. Based on the intervention and the expert testimony about the scope and burden of German privacy laws, the Texas Supreme Court concluded that the corporate phonebook should not be produced in contravention of German law. So you do have a bit of precedent in using this type of issue to try to limit the discovery.