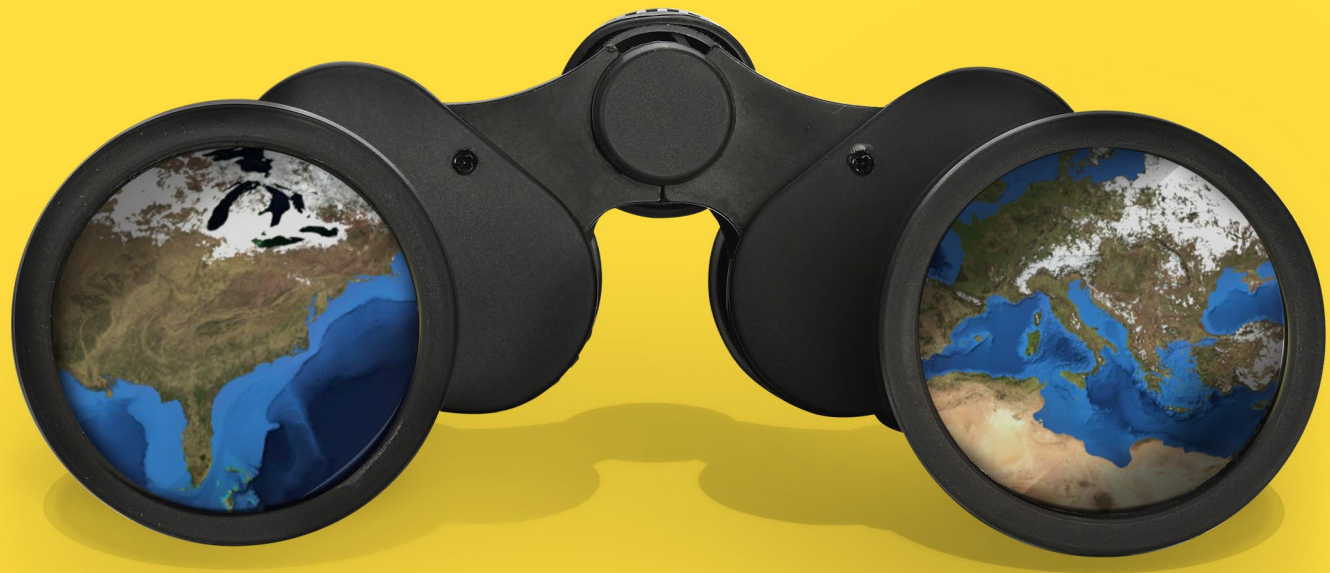
CROSS-BORDER INVESTIGATIONS:

When Your Company Is In Hot Water Overseas



MODERATOR:

Tom Best
Partner
Steptoe & Johnson

PARTICIPANTS:

Eugene I. Goldman
Partner
McDermott, Will & Emery LLP

Veeral Gosalia
Senior Managing Director
Technology
FTI Consulting

Steven P. Solow
Partner
Katten Muchin Rosenman

George J. Terwilliger III
Partner
Morgan, Lewis & Bockius LLP

FTI CONSULTING™

At the 2014 American Bar Association's National Institute on Internal Corporate Investigations and In-House Counsel, co-sponsored by FTI Consulting, the panel discussion "Trends in Cross-Border Investigations" featured Veeral Gosalia, Senior Managing Director in FTI Consulting's Technology segment. Gosalia is an expert in computer forensics and European Union (EU) data privacy issues regarding computer acquisitions and tape restorations. The panel, moderated by Tom Best, a partner at Steptoe & Johnson, included Steve Solow, Co-chair of Katten Muchin Rosenman's White Collar and Complex Litigation group; George Terwilliger, Partner and Head of Morgan Lewis Bockius' White Collar Litigation and Government Investigations group, who also served as U.S. acting Attorney General under President George H.W. Bush; and Eugene Goldman, Partner at McDermott, Will & Emery LLP, who represents clients on Foreign Corrupt Practices Act litigation and other matters.

TOM BEST: Five years ago, we were in a world where the United States, the U.S. Department of Justice [DoJ], the U.S. Securities and Exchange Commission [SEC] and maybe one or two other of the major trading nations around the world drove the enforcement agenda and, thereby, the compliance agenda.

I think we've moved on from that to a more unipolar, if you will, environment.

So I thought we'd introduce a hypothetical: A multinational corporation, let's call it USMNC, has its corporate headquarters in the United States, but a lot of its regional folks are based in European jurisdictions. Much of the company's growth is coming from some difficult regions.

The company is doing a lot of business in one jurisdiction in particular — Country A. That country requires USMNC to follow a joint venture [JV] structure. So it has a JV partner, Partner Co., whose shares are 100 percent owned by a citizen of that country.

USMNC owns 49 percent of the JV; Partner Co. has 51 percent. USMNC, however, is operating the venture on a day-to-day basis. USMNC holds the checkbook, and it has appointed a chief financial officer and staff.

The immediate thing one needs to do if a company is in legal jeopardy is to bring it to an end.

Five years ago, Country A privatized its telecommunications industry, including wireless telephony. Partner Co. was a successful bidder for a license. It was developing the infrastructure and the ability to service that license but ran out of capital. Partner Co. had to find a partner — thus USMNC.

It turns out that Partner Co. may have made some improper payments when it acquired its license. While Partner Co. was the sole entity in the license auction process, it also was working closely with USMNC's European management with the expectation that Partner Co. eventually would have to form a joint venture.

Now USMNC's legal department is hearing that the license may have been procured through improper payments and that USMNC might have known about them and might have been involved. The legal department is trying to decide whether to launch an investigation.

Those are the facts. What are the pros and cons to launching an investigation?

GEORGE TERWILLIGER: Let's start at a fundamental level. Why would either in-house or outside counsel recommend an internal investigation at this point?

I think because knowledge is preferable to ignorance.

Largely, an internal investigation is for defensive purposes. Most corporations value their reputation. One of the reasons to commence an investigation in a forensically sound manner is because there are reputational interests pertaining to USMNC that deserve to be protected.

When you see a red flag — at least from the position of the directors (and especially the independent directors) of a public company — you have an obligation to act to protect shareholder interests by looking into the matter.

The SEC will take the position that a public company with this kind of information has a duty to look into the facts and not ignore them. And if you're going to do that, you might as well do it in a forensically sound manner so you get the biggest bang for the buck.

There's also the issue of remedial steps. The immediate thing one needs to do if a company is in legal jeopardy is to bring it to an end. You can do that only if you have a thorough understanding of the underlying conduct that caused the liability.

You will find a wide variety of responses to a situation like this. Companies that have been through this process will act fast and know exactly what they need to do. Then there are those that will have a tendency to say, "Geez, do we really need to conduct an internal investigation? It's expensive." After much discussion, company leaders will ask, "Can't we just go talk with a few people and see what happened?"

The answer is, yes, you could do that. But if it turns out there is a problem, you're going to have to go back and do it over again, repeating a lot of the work you've already done.

I am sympathetic to the costs. Even a relatively simple investigation can be expensive because of the amount of document discovery that needs to be done. An internal investigation involves outside consultants, forensic accountants, forensic technology experts, a detailed document review and a protocol of some kind using search terms or predictive coding to search documents because the world in which we live has become much more transparent, as well as complex.

The structure of an investigation in this kind of circumstance might be a little different. In essence, we have a JV that we don't own, but it's a JV that we operate and whose problems we, therefore, *do* own.

TOM BEST: So we have a joint venture. But our company doesn't own it so perhaps you need to secure the cooperation of the local partner. How do you go about doing that? Do you have any specific tips?

GEORGE TERWILLIGER: Yes. The initial step is to review the JV agreement itself. Most JV agreements where you have this type of major investment and management role by one company typically would contain some kind of right of audit or inspection.

In this particular hypothetical, you could assert that an audit or inspection be conducted as part of the management responsibility. And you could even appoint people internally within the JV to facilitate that exercise.

TOM BEST: Let's assume we've decided to kick off an investigation and that USMNC's legal department in the United States is on board. What do you do when there is evidence or conduct in a third country and yet there are folks who physically are located in the EU? How do you approach data protection and privacy issues, and how would you view those issues in your overall structuring of an investigation?

GEORGE TERWILLIGER: Well, you've pinpointed a number of issues that have to be taken into account. In the EU countries, each of which has some version of the EU Data Protection Protocol as part of its law, how strict the law is varies from country to country.

There's no playbook to which you can turn.

We conducted an interview in a western European country not long ago. The person wanted a human resources representative present. And he wanted a representative of his management chain and a lawyer of his choice in the room for the interview. I guarantee you that no employee in the United States would ever assert that.

It actually is quite amazing. The United States professes to be concerned about civil liberties, but we're behind the European countries when it comes to protecting people's personal data.

At least up until now (although I think this may be changing), one of the reasons for that is because people in Europe use their work email for all aspects of their life. We've come across everything from medical information to social media and entertainment to personal relationships in our reviews.

This does not prevent us from doing our job, but it's a hurdle that usually involves using search terms to screen so you're getting only relevant nonpersonal information. There's a lot of exposure if you get the data privacy piece of it wrong.

TOM BEST: Veeral, we're talking about collecting information. Tell us about some of your experiences in managing these data protection issues. How do you actually do this investigation?

VEERAL GOSALIA: There's a ton of information out there about what you can't do in these circumstances but not very much about what you can or should do, especially put in the context of our hypothetical scenario. There's no playbook to which you can turn.

That's not to say there aren't frameworks. Some of you may have heard of terms like model contracts and binding corporate rules. There are some logistical issues to using those guidelines in this context. Importantly, they have to be in place prior to the review and it's difficult to implement a new framework during a fast-moving investigation.

More specifically, I think the bigger problem is that many of these options don't have a clear path for the onward transfer of the information. You may have used it to conduct your investigation but then discovered the SEC or the DoJ has requested certain data. Generally, it's not possible to forward such documents.

Consent is the other thing people immediately think about when they hear the topic of data privacy. I'm not saying not to do consents — or not to use them as a way of addressing this issue — but it's important to point out that the EU data privacy regulators repeatedly have said that consent is unworkable most of the time and is not a permissible basis upon which to transfer protected data to the United States, for example. That's because consent has to be given freely, and it cannot be granted prospectively. And what do you do when you have a custodian who refuses to sign the consent form? On balance, I do think you should have the consent form in place. You should use that as a key ingredient because, at the end of the day, you want to be able to point to actions that you've taken to try to comply with local laws. Consent is a good way of doing that as long as you include certain aspects in the agreement as described below.

Some elements I recommend including in the consent form would be details of the data being collected and processed. For example, what are you collecting? What are you processing? The EU considers data collection to be a form of processing. So even though you're merely doing preservation, that's still considered processing. You have to provide the reason for the collection taking place, how long the data will be held and where the data will be stored. You need to specify the jurisdictions where the data potentially will be transferred and detail how to exercise rights to inspect or correct that data.

I've had a number of instances where custodians have asked to look at the data being collected or that eventually may get transferred. Be prepared to do that. Then you want to ensure that the consent form is in the local language vs. just English. That's an important fact since you don't want people to come back and say they didn't understand the consent form.

That said, what it basically boils down to is a catch-22 where you have a need to conduct a thorough and forensically sound[1] investigation and meet the requirement to comply with local laws. The two don't necessarily work together. The approach I normally take when I have this situation is to advocate for one of data minimization. That involves doing a lot of in-country data culling and review. The idea is to limit how much data will leave the country. That's all easier said than done, of course.

For example, in places like Germany, France, or China, the local e-discovery market doesn't really exist. So you must have some kind of a mobile process to do this type of work.

One process is to go on-site; conduct the data collection, leaving the data in-country; process[2] the data there; apply strong keywords; and then fight technology with technology. You don't have to do that sort of document-by-

document review. Nowadays, there's technology that will let you do data visualization, data clustering, and predictive coding. There are ways in which you can attack the data population much more rapidly than by conducting a page-by-page review as you would in a traditional manner.

Another element is state secrecy, which pertains more to China than to the EU. I typically treat data protection and state secrecy in the same manner. The big difference is that China has rules that essentially prohibit the transfer of information that the Chinese government considers being important to its economic interests vs. protecting the interests of someone's privacy, as is the case in the EU.

Where the challenge begins is that the Chinese government hasn't conclusively defined what it considers a state secret. Government officials also have said they can decide retroactively what is or is not a state secret.

EUGENE GOLDMAN: They don't want you to know.

VEERAL GOSALIA: So that's another reason for having a consistent approach that you follow throughout an investigation. The initial step I frequently take when we decide to conduct an investigation — and I'm called in to handle, say, data collection — is to build a data map to identify issues pertaining to data protection and state secrecy.

Outsourcing data and IT [information technology] infrastructure to third parties in the United States is not common, but in the EU and especially in Asia, it's very common. Companies might store their data in places where you could come across these types of issues, and it's important to recognize that so you can plan ahead and know exactly where to go.

Consider doing drills. Walk through a scenario in which you might have to collect and review data in situations where the data might fall under one of these data protection/state secrecy issues. Seek outside help to do that. You'll often find that firms are more than willing to help you think through these issues on a proactive rather than on a reactive basis. The best vehicle for cost-containment is efficiency. So have a plan in place before you get into one of these investigations.

The cardinal rule of conducting a forensically sound investigation is not to edit the data you're capturing.

STEVE SOLOW: One of the issues that comes up — particularly for sophisticated clients that have strong IT departments — is, "We can do a lot of this on our own. Why do we need to bring in vendors?" Part of what needs to be recognized is the risk management side regarding the use of vendors.

VEERAL GOSALIA: The first thing I do is make a company aware that its IT department doesn't necessarily have the right tools, framework or methodology in place to conduct an investigation in a forensically sound way. One of the common comments I hear from clients is, "Well, I can search the material myself. There is a search box in Windows, and I can do a little search and look at my data, right?"

My response is, "Well, that's only searching a small percentage of the information. It's only searching items that are searchable. PDF files, encrypted documents, etc., often won't show up in the results." Often, the search program doesn't search email so people who use Outlook, for example, might store email in a PST file, which is not searched when you use that search window. And the program doesn't tell you what it's not searching. I go through these situations with clients to make them aware. The other thing is, in preservation, the simple act of moving a document from Point A to Point B will change the metadata[3] of that document.

Most IT folks won't be aware of that. They don't even consider metadata as an important element. I explain that in touching these documents, you're altering the data that are part of the investigation. The cardinal rule of conducting a forensically sound investigation is not to alter the data that you're capturing.

GEORGE TERWILLIGER: Let's talk for just a minute about what else we're collecting. I have on this phone, as do many of you, I'm sure, my personal email, my business email, text messaging and maybe some other messaging capabilities.

The government is getting sophisticated about understanding that there could well be a treasure trove of information to be found in messaging that's off the official company email and so forth. In the Deepwater Horizon BP case, an employee was indicted for deleting messages on a personal device. The complications of what needs to be done

in a forensically sound manner when you start asking people about their personal messaging capabilities get a lot more difficult.

TOM BEST: Let's assume that the investigation's gone forward and that a number of improper payments were uncovered, and you think the people at USMNC might be implicated. That puts the question to USMNC of what to do about voluntary disclosure and the respective pros and cons. Eugene, what do you think?

EUGENE GOLDMAN: One of the most important and complex decisions for in-house counsel to make is whether to recommend that the company self-report. We have witnessed a drumbeat of warnings with heavy consequences from the DoJ and the SEC if a company does not self-report.

On the other hand, there is a continuing stream of commentary from practitioners and professors that the potential harm of self-reporting outweighs the benefits, as many self-reporting companies still get hit with heavy penalties, public proceedings, collateral damage from class action suits, etc.

Self-reporting likely would generate SEC influence over the direction and scope of the internal investigation. It could reflect positively for a company. On the other hand, the SEC might say, "Please broaden the investigation and look at not only this joint venture but at all the JVs in this area of the world, or, for that matter, all over the world." So, in a sense, you might lose control if you jump the gun and self-report too early.

GEORGE TERWILLIGER: On the issue of foreign authorities, there's far more cooperation today than ever before between U.S. and foreign authorities. In some of these cases, there's a lot of communication.

I think the possibility of foreign interest in any subject matter of an internal investigation is something that has to be taken into account when you start talking about voluntary disclosure and other pertinent issues.

STEVEN SOLOW: One area we didn't mention, and I throw it out merely for awareness, is that when we talk about data privacy, remember that not all data are personal data. It's important to identify what might be considered business data early on because the data may be easier to access, simpler to use and less complicated to move from one place to another.

GEORGE TERWILLIGER: We're going back to data privacy. I remember the first time I went to the SEC and said, "Look, we can't continue quite this way. We have consents but not from these individuals. So we'll have to give you redacted emails and so forth." The SEC members said, "What? We've never heard of this before."

They really didn't get it. That's changing because the SEC is becoming more educated. I think when you're dealing with enforcement authorities on these kinds of issues, helping to educate officials is a very important part of the process.

TOM BEST: Thank you, all.

REFERENCES

1 — A methodology employed to ensure the process is defensible and maintains the integrity of the data

2 — The processing of data involves converting the original of "native" data into a format that can be searched and more easily reviewed

3 — Metadata can be thought as "data about data" or fields of information that contain data points such as the author of a document, data a file was created, or the last time it was printed.

MODERATOR

Tom Best
Partner
Steptoe & Johnson

PARTICIPANTS

Eugene I. Goldman
Partner
McDermott, Will & Emery LLP

Veeral Gosalia
veeral.gosalia@fticonsulting.com
Senior Managing Director
Technology
FTI Consulting

Steven P. Solow
Partner
Katten Muchin Rosenman

George J. Terwilliger III
Partner
Morgan, Lewis & Bockius LLP

For more information and an online version of this article, visit ftijournal.com.