The Metropolitan
Corporate Counsel®

www.metrocorpcounsel.com

Volume 19, No. 8 August 2011

Controlling Data In A Social Media World

The Editor interviews ***Jason Ray****, Director in the Technology Practice, FTI Consulting, Inc*.

Editor: Tell us about your background.

Ray: My background is a combination of legal services and technology. I've been a senior executive in operations and software development for a number of litigation support companies, the most memorable being COMPEX Legal Services in California and Fios, one of the first electronic discovery companies.

Editor: What is social media? What role does it play in e-discovery?

Ray: Social media is the area of technology used for people to connect directly to other people within a personal network. LinkedIn is your personal business network, Facebook is your personal family and friends network – all is about person to person connection. What role does that play in e-discovery? Like other forms of communication, it is potentially discoverable and potentially relevant.

Editor: Is it possible to completely control social media?

Ray: It cannot be totally controlled: for one, the number of social media systems and the speed with which those systems are changing is significantly faster than the ability for anyone to even understand them all, let alone control them.

Editor: Do policies help?

Ray: Since you can't control it, you can only contain it as best you can. Policies are very important. When you are setting a policy and putting it in a practice that you can manage, you are effectively articulating that you have identified an issue and that you have taken steps to contain that issue. If employees violate your policy, you are in the position of stating that you had put in place a policy to control this issue, so that any violation falls directly on the head of the violator. It is critical that if you do have a policy, you must also have some management system in place to ensure that that policy is being enforced. If you just set the policy but do not try to manage it, you actually put yourself in a worse position.

If you have an enforcement system, even if it's as simple as having employees sign off on having read and understood their employee hand book and periodically attend mandatory review sessions, then an employer has taken the correct steps. You can't ever control all that seeps out, but you can at least show that you were doing everything that was prudent and reasonable.

Editor: Notwithstanding all the steps you might take to control this, what if it treads upon privacy?

Ray: This is particularly interesting in Asia and Europe – Europe, especially because of the more well developed electronic data privacy laws so there is an overlap between an employee's individual rights to privacy and an employer's need to manage information. But if you're the general counsel, your job is to make the company's position as clear as it can be, and if there is a risk to the company, you have to act. If the employee thinks that is an invasion of his privacy, there are mechanisms for dealing with that. Some companies tell their employees up front that everything they do on the web and every email that they send is being monitored. If you try to bend over backwards to give people their own definition of their rights to privacy, you put your company in jeopardy and are not being the steward of the company. In our European consultancy we instruct employers as to their need for the types of systems that make it clear to employees what is and is not private, what is and is not controlled, and that they understand that by using company email systems and telephones they do so in accordance with the policy that they are not to make personal communications through these mechanisms.

Editor: What measures should be considered for controlling the scope of discovery?

Ray: This is the biggest question about social media and the one that is the least discussed. At one time everything was on paper in filing cabinets, but no one would have ever suggested that every piece of paper in every filing cabinet should be copied for discovery. But in technology people think everything has to be looked at. Again social media systems are primarily peer to peer communications in networks set up by persons in the network. Unless there is a reason to believe that a given system is being used for some purpose that is material to the issues in a particular matter, there is no reason to extend discovery to this medium. In most cases and in most matters social media systems are irrelevant.

Editor: How is preservation possible if a company doesn't control the data?

Ray: If the company is not in control of the systems, the only way that the company can ensure preservation on an ongoing basis is to contract with providers that offer ongoing preservation services. If you are not going to be able to, or do not need to, do ongoing preservation, a "Moment in Time" collection is a sufficient preservation act. You just have to ensure that the preservation act happens as quickly as possible by issuing litigation-hold instructions to the employee and provider – Facebook, Twitter or LinkedIn – issuing the message to make sure the information is locked down, once you know that there is an issue. Make a "Moment in Time"

Please email the interviewee at jray@fticonsulting.com with questions about his interview.

preservation as quickly as possible.

For instance, you can't control Facebook – Facebook doesn't let you decide what gets preserved and what doesn't get preserved. The good news is that Facebook keeps almost everything except for messages users can delete.

Editor: How do you make the request for preservation?

Ray: So welcome to the world of social media and cloud technology! There are no universally published standards on how to run a social media communication system. Every provider is doing preservation in a different way. Twitter is different from Facebook, Facebook is different from LinkedIn and LinkedIn is different from the Google+ project that just launched.

When you run into the need to do a collection or preservation, you need experts who understand those particular systems and can use the correct tools. In collecting from Twitter there are 45 tools to collect – there are dozens to collect from Facebook, no two of which are the same and each of which has different problems. The Facebook internal archiving system, available on any Facebook account, saves messages, not as individual messages but as one gigantic text file of everything that has been sent to you. If you are going to use that information of perhaps a log of 100,000 communications of which two messages are important to a case, are you going to redact all but the two messages? The smart thing to do is use people who have tools that can be verifiably effective in extracting the data.

Editor: Do the regular eDiscovery providers understand all of this? Are they able to help with a Facebook collection of data?

Ray: There is a pretty wide range of expertise and capability between companies that claim to be eDiscovery providers. For social media collections you need companies that are eDiscovery providers who are focused on complex problems, such as FTI. There are certain providers who specialize in this area of collections, preservation consulting and corporate information management, which are either much more likely to know or smart enough to figure out these things. Companies have to be very careful that they hire firms who not only know what they are talking about but have developed tools that they have tested and verified to do the job. And it is that testing and verifying part which is the key because things can change over night. You need to work with vendors that have done diligence in the social media space. Most Facebook collection methods don't get messaging, which from a discovery stand point is often the most important facet of discovery in Facebook.

Editor: What should be considered in planning for data collections?

Ray: The answer is that this is a developing space. It changes all the time so you need companies that are diligent about making sure that what is happening right now has been tested and verified. When you plan for collecting data, first make sure that you actually have to collect it and if so, try to control the scope of collection. Collect it as quickly as possible. If you have a relationship with those firms whom you know have ways of dealing with these problems, contact them.

I am going to use LinkedIn as an example: Many companies now use LinkedIn for recruiting as an internal HR tool. If you are using it as a tool, then make sure that you have a mechanism, a vendor or internal capability that knows how to deal with that specific tool and then you can be prepared to do data collection. The second thing is that social media is uncontrolled, which means that you may not be able to know everything that is involved until you have looked at the actual devices that are used by the those involved in the case. My personal recommendation as a consultant is that you should start with interviews to determine what mechanisms are involved.

Editor: How is social media data being reviewed?

Ray: Just as each system is different requiring different collection methods, each result is different. There are a couple of different challenges. The traditional sort-by-TIFF and date-stamp, putting it into a database rarely works well for social media data. Both because it is not always in a format that is convenient to turn into a TIFF and as with Facebook, what you would get by TIFFing it is not what you want. Typically the way that it is reviewed is either live on the system itself for those systems where that is necessary. For example, there is no way to get messages out of LinkedIn – there is no mechanism for it, and there are no external API tools to let us write software to retrieve it.

When it is possible to take data and turn it into something that lawyers like to see, like turning messages into individual message files that can then be TIFFed if necessary, then that is how they are produced. They are produced like any other electronic document that you would handle. That said, a lot of social media information is produced natively because people don't have the tools to handle it well. Depending again on the specific source and what you are trying to do, the method of production varies. In today's world, documents that are textual that can be turned into paginated, petrified information are typically produced in TIFF form; everything else is typically produced natively. That can create challenges for the person receiving the production because I have produced the documents or information to you natively. If you don't have the systems to read it, then that's unfortunate!

Editor: Do you recommend educational sessions with employees?

Ray: Like any good policy, it needs to be not only articulated but rearticulated periodically. Let's face it, how many people actually read their employee manual? Not many. So the fact that they signed a statement saying they read it doesn't assume it is part of their actual practice.

It is especially a problem with FCPA because what we call a corrupt practice many countries call normal business. If a company has articulated its FCPA policy, if it is reinforcing it, if it is reminding people of their obligations, and if it has established controls, but if one person strays, then at least the problem is contained, and the company can point to the rogue employee. All an employer can say is that I have taken every prudent and reasonable step that I can to contain this process. And the fact that we missed one because somebody built a new system we had never heard of – that is just the way that the world works.

This is actually related to something that I talk about quite a bit now with my clients, which is: If you are proactive and you have taken prudent steps, it changes the control of the conversation. If you sit down with the DOJ, and they say that we want you to restore every back-up tape and get every archive, and do this and that,and you say "well, look here is how we manage this – this is how our disaster recovery strategy works. We ensure that we have these documents that are kept for long-term storage under our preservation policy." If you can articulate this information, then the DOJ virtually all the time will accept your word. If you haven't thought it through and presented it in a way that sounds plausible, then virtually all the time the DOJ will want to get all the data that you have.

And you have to have a system that is enforced by demonstrating that you have control over your data.